Final Project Report

Introduction to p-adic numbers

Prepared in fulfilment of the course

MATH F266

submitted to

Dr. Divyum Sharma

Assistant Professor

Department of Mathematics

Birla Institute of Technology and Science, Pilani

Rajasthan (India) -- 333 031

By

Raghav Khanna

2018B4A40914P

DEPARTMENT OF MATHEMATICS

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI

CERTIFICATE

This is to certify that the project report **“Introduction to p-adic numbers”** being submitted by

Raghav Khanna – 2018B4A40914P

in fulfilment of Course Number MATH F266 is a bonafide work carried out under my supervision.

Dr. Divyum Sharma

Assistant Professor

Department of Mathematics

Birla Institute of Technology and Science, Pilani

Rajasthan (India) -- 333 031

ACKNOWLEDGEMENT

A lot of effort has gone in to make this project a success. It would not have been possible without the kind support and help of my mentor, Ms. Divyum Sharma who has given her valuable time and energy for this project. I would also like to thank Maths Department, BITS Pilani for giving the students a chance at conducting such project type courses and Dr. Divyum Sharma for accepting me and providing me with a chance to learn more in-depth and apply what I had learnt in my previous 2 years in college.

ABSTRACT

In mathematics, the *p*-adic number system for any prime number *p* extends the ordinary arithmetic of the rational numbers in a different way from the extension of the rational number system to the real and complex number systems. The extension is achieved by an alternative interpretation of the concept of "closeness" or absolute value. Till now, we have considered the concept of closeness to be a measure of distance, but two *p*-adic numbers are considered to be close when their difference is divisible by a high power of *p*: the higher the power, the closer they are. This allows us to study the concept of congruences in more detail and in a completely different manner than we did in the earlier Number Theory course. We also define the concept of fields for p-adic numbers. For a given prime *p*, the field $\mathbf{Q}_p$ of *p*-adic numbers is a completion of the rational numbers. The field $\mathbf{Q}_p$ is also given a topology derived from a metric. This metric space is complete (every Cauchy sequence converges to a point in $\mathbf{Q}_p$*)*. We further learnt about 2 of the most important results in the p-adic universe- Hensel's Lemma and Strassman's Theorem and learnt to perform arithmetic and various other mathematical operations on p-adic numbers. Limits, Continuity, Differentiability, Integration, Power Series' etc all which had been covered earlier on the set of real or rational numbers was now covered for the set of p-adic numbers, which gives a different approach to solving different mathematical problems.

Table of Contents

Definition of a field:

*A **field** is a set F, containing at least two elements, on which two operations + and * (addition and multiplication) are defined so that for each pair of elements x, y in F there are unique elements x + y and x * y (or xy) in F for which the following conditions hold for all elements x, y, z in F:*

(i) $x + y = y + x$ (commutativity of addition)

(ii) $(x + y) + z = x + (y + z)$ (associativity of addition)

(iii) There is an element $0 \in F$, called zero, such that $x+0 = x$. (existence of an additive identity)

(iv) For each x, there is an element $-x \in F$ such that $x + (-x) = 0$. (Existence of additive inverses)

(v) $x*y = y*x$ (commutativity of multiplication)

(vi) $(x * y) * z = x * (y * z)$ (associativity of multiplication)

(vii) $(x + y) * z = x * z + y * z$ and $x * (y + z) = x * y + x * z$ (distributivity)

(viii) There is an element $1 \in F$, such that $1 \neq 0$ and $x*1 = x$. (existence of a multiplicative identity)

(ix) If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $x * x^{-1} = 1$. (existence of multiplicative inverses)

Section 1: Absolute Value on a Field

Notation : ***k*** is a field

$R_+ = \{x \in R: \ x \geq 0\}$

Definition 1.1: *An absolute value on k is a function $|\ | : k \rightarrow R+$; that satisfies the following conditions:*

i) $|x| = 0$ if and only if $x = 0$;

ii) $|xy| = |x||y|$ for all $x, y \in k$;

iii) $|x + y| \leq |x| + |y|$ for all $x, y \in k$.

Non Archimedean Absolute Value: Aside from the standard properties of an absolute value, an absolute value is non-Archimedean if it satisfies the additional condition:

iv) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in k$;

Absolute Value at Infinity

The usual absolute value that we have defined till now is defined by taking k = Q, then | | is defined as:

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

We see that this Absolute Value is Archimedean – How?

Taking x = y = 1, we get |x + y| = |1+1| = 2 > max{|x|,|y|} = 1 → non Archimedean condition is not followed. Therefore, the absolute value is Archimedean.

This absolute value is now termed as the "*Absolute Value at Infinity*". $| |_\infty$

Trivial Absolute Value

The trivial absolute value is defined on any field k and is the first non-Archimedean Absolute Value we encounter

$$|x|_0 = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

Proof: Trivial Absolute Value is non-Archimedean

Case 1: x+y ≠ 0 => $|x+y|_0$ =1.

Since x+y is not zero, at least one of x and y must not be equal to 0. Without loss of generality, let x≠0.

So, $|x|_0$ = 1, $|y|_0$ = 0 => max{|x|,|y|} = 1 = $|x+y|_0$.

If both are non-zero, we can clearly see that both $|x|_0$ and $|y|_0$ will be 1.

Case 2: x+y = 0 => $|x+y|_0$ = 0

Since x+y is zero, either both x and y are zero, or both x and y are non zero.

If both x,y = 0; max{|x|,|y|} = 0 = $|x+y|_0$

If both x,y $\neq$0, max{|x|,|y|} = 1 > $|x+y|_0$ => non Archimedean Condition is Satisfied.

Definition 2.1.2: P-adic Valuation

Fix a prime number p $\in$ Z. The p-adic valuation on Z is the function v_p : Z - {0} → R defined as follows:

For each integer n $\in$ Z, n ≠ 0, let $v_p(n)$ be the unique positive integer satisfying:

$$n = p^{vp(n)}n' \text{ with } p \nmid n'.$$

We extend v_p to the field of rational numbers as follows: if x = a/b $\in$ Q×, then

$$v_p(x) = v_p(a) - v_p(b).$$

Proof for extension of v_p to rational numbers:

Let x = a/b where,

a = $p^{a0}p_1^{a1}p_2^{a2}p_3^{a3}....p_n^{an}$ and

b = $p^{b0}p_1^{b1}p_2^{b2}p_3^{b3}..p_n^{bn}$ where ai,bi >= 0 and pi are prime numbers (prime factorization method)

$v_p(a) = a_0$ and $v_p(b) = b_0$ (from the definition of p-adic valuation)

Now, x= a/b = $p^{a0-b0}p_1^{a1-b1}p_2^{a2-b2}p_3^{a3-b3}....p_n^{an-bn}$

$v_p(x) = a_0 - b_0 = v_p(a) - v_p(b)$

Lemma 1.2: For all x,y ∈ Q, we have

1. **$v_p(xy) = v_p(x) + v_p(y)$ and**
2. **$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$**

Proof:

1. Once again using prime factorization method,
   Let $p^{x0},p_1^{x1},p_2^{x2}p_3^{x3}....p_n^{xn}$ and $p^{y0},p_1^{y1},p_2^{y2}p_3^{y3}....p_n^{yn}$ to be the prime factorization of x and y
   $v_p(x) = x_0$ and $v_p(y) = y_0$
   Then, xy = $p^{x0+y0},p_1^{x1+y1},p_2^{x2+y2}p_3^{x3+y3}....p_n^{xn+yn}$
   Therefore, $v_p(xy) = x_0 + y_0 = v_p(x) + v_p(y)$
   If x and y are rationals, let x = t/q and y = r/s;

Then,

$$v_p(xy) = v_p\left(\frac{tr}{qs}\right) = v_p(tr) - v_p(qs)$$

$$= v_p(t) + v_p(r) - v_p(q) - v_p(s)$$

$$= v_p\left(\frac{t}{q}\right) + v_p\left(\frac{r}{s}\right).$$

2. Let $p^{x0}p_1^{x1}p_2^{x2}p_3^{x3}....p_n^{xn}$ and $p^{y0}p_1^{y1}p_2^{y2}p_3^{y3}....p_n^{yn}$ be the prime factorization of x and y respectively.

   Now, $x+y = p^{x0}p_1^{x1}p_2^{x2}p_3^{x3}....p_n^{xn}(1+ p^{y0-x0}p_1^{y1-x1}p_2^{y2-x2}p_3^{y3-x3}....p_n^{yn-xn})$

   Taking the p-adic valuation, we get $v_p(x + y) \geq v_p(x)$

   We can also write $x + y = p^{y0}p_1^{y1}p_2^{y2}p_3^{y3}....p_n^{yn}(1+ p^{x0-y0}p_1^{x1-y1}p_2^{x2-y2}p_3^{x3-y3}....p_n^{xn-yn})$

   Taking the p-adic valuation, we get $v_p(x + y) \geq v_p(y)$

   So, from the 2 conditions we get $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

   For the case of rationals, If x and y are rationals, let x = t/q and y = r/s;

   Then, let $t = p^{t0}p_1^{t1}p_2^{t2}p_3^{t3}....p_n^{tn}$

   $q = p^{q0}p_1^{q1}p_2^{q2}p_3^{t3}....p_n^{qn}$

   $r = p^{r0}p_1^{r1}p_2^{r2}p_3^{r3}....p_n^{rn}$

   $s = p^{s0}p_1^{s1}p_2^{s2}p_3^{s3}....p_n^{sn}$

   Then $t/q = p^{t0-q0}p_1^{t1-q1}p_2^{t2-q2}p_3^{t3-q3}....p_n^{tn-qn}$

   $r/s = p^{r0-s0}p_1p_2^{r2-s2}p_3^{r3-s3}....p_n^{rn-sn}$

   We then proceed similar to how we did in the case of integers and replace x and y by the prime factorised form of x and y so we get $v_p(x + y) \geq v_p(x)$ and $v_p(x + y) \geq v_p(y)$

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

Definition 1.3: P-adic Absolute Value

For any nonzero $x \in Q$, we define the p-adic absolute value of x by

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

We extend this to all of Q by defining $|0|_p = 0$.

Theorem: p-adic absolute value is non-archimedean

Proof: To prove that p-adic absolute value is non-Archimdean, we need to show that the non-Archimdean condition: $|x + y| \leq \max\{|x|, |y|\}$ for all x, y ∈ k holds.

$|x+y|_p = p^{-vp(x+y)} \leq \max\{ p^{-vp(x)}, p^{-vp(y)}\}$

We know that, $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

Hence, without loss of generality, let $v_p(x) > v_p(y)$

Then, $v_p(x + y) \geq v_p(y) \Rightarrow -v_p(y) \geq -v_p(x+y) \Rightarrow \mathbf{p^{-vp(y)} \geq p^{-vp(x+y)}}$ **------------- (1)**

Now, we also know that $v_p(x) > v_p(y) \Rightarrow \mathbf{p^{-vp(y)} \geq p^{-vp(x)}}$ **-------------------------(2)**

So, $\max\{ p^{-vp(x)}, p^{-vp(y)}\}= p^{-vp(y)}$

Using 1 and 2, $|x+y|_p = p^{-vp(x+y)} \leq \max\{ p^{-vp(x)}, p^{-vp(y)}\}$

Section 2: Basic Properties

Theorem 2.1 : For any absolute value | | on any field k, we have:

i) |1| = 1.

ii) If x ∈ k and x^n = 1, then |x| = 1.

iii) | - 1| = 1.

iv) For any x ∈ k, | - x| = |x|.

v) If k is a finite field, then | | is trivial.

Proof: |x| is a positive real number.

i) $|1| = |1^2| = |1|^2 = 1$ since the only non-zero positive real number α for which $\alpha^2 = \alpha$ is $\alpha = 1$

ii) Since |x| is a positive real number and x^n = 1(positive) => |x| = 1

iii) $|-1| = |(-1)^{2*1/2}| = |1|^{1/2} = 1$ (from (i)) and using the non-negativity of the absolute value

iv) |-x| = |-1||x| => |-x| = |x| since |-1| = 1 from (iii)

v) Since k is a finite field, $x^{q-1} = 1$, where q is the order(number of elements) of the finite field when $x \neq 0$ (property of field); so from (ii), the absolute value must be trivial

----

Theorem 2.2: Let k be a field and let | | be an absolute value on k. The following are equivalent:

(i) For all x, y ∈ k, |x + y| ≤ max{|x|, |y|}.

(ii) For all $z \in k$, $|z + 1| \leq \max\{|z|, 1\}$.

Proof: Let us assume (i) is true, then; by putting $x = z$, $y = 1$ we get (ii). So it is clear that (i) implies (ii).

Now assume (ii). If $y = 0$ then (i) holds automatically so we can assume $y \neq 0$

Let $z = x/y$. Then we have

$$\left|\frac{x}{y}+1\right| \leq \max\left\{\frac{|x|}{|y|}, 1\right\}.$$

Multiplying both sides by $|y|$ now gives (i).

Theorem 2.3: Let k be a field and let $| \; | : k \longrightarrow R+$ satisfy

i) $|x| = 0$ if and only if $x = 0$,

ii) $|xy| = |x||y|$ for all $x, y \in k$, and

iii) $|x| \leq 1 \Rightarrow |x - 1| \leq 1$.

Then $| \; |$ is a non-archimedean absolute value on K.

Proof: We need to show that these 3 conditions imply the non – Archimedean Condition $|x+1| \leq \max\{|x|,1\}$ for all x belonging to the field k

$x+1 = -(-x-1)$

Now, From (iii), $|x| = |-x| \leq 1 \Rightarrow |-x - 1| \leq 1 \Rightarrow |x+1| \leq 1$

Therefore, $|x| \leq 1 \Rightarrow |x-1| \leq 1$

Now we take 2 cases,

Case 1: $|x| \leq 1 \Rightarrow \max\{|x|,1| = 1$ and so $|x+1| \leq 1$

Case 2: $|x| >1 \Rightarrow |1/x| < 1$ and so $| 1+1/x| \leq 1$ from (iii)

So, we now have

$$\left|\frac{x+1}{x}\right| = \left|1+\frac{1}{x}\right| \leq 1,$$

And hence, $|x + 1| \leq |x| = \max\{|x|, 1\}$

Theorem 2.4: Let $A \subset k$ be the image of Z in k. An absolute value $| \; |$ on k is non-archimedean if and only if $|a| \leq 1$ for all $a \in A$. In particular, an absolute value on Q is non-archimedean if and only if $|n| \leq 1$ for every $n \in Z$.

Proof:

Part 1

We have | ± 1| = 1 always; hence, if | | is non Archimedean, we get that

$$|a \pm 1| \leq \max\{|a|, 1\}.$$

By induction, if follows that $|a| \leq 1$ for every a ∈ A.

Part 2

We need to show that if $|a| \leq 1$ for all a ∈ A, then | | is non-Archimedean.

To show that the absolute value is non-Archimedean, we need to show that for all x belonging to k, we have $|x+1| \leq \max\{|x|,1\}$

If m is a positive integer, then

$$|x+1|^m = \left|\sum_{k=0}^{m}\binom{m}{k}x^k\right| \leq \sum_{k=0}^{m}\left|\binom{m}{k}\right||x^k|.$$

Now since ${}^{m}C_{k}$ is an integer, we have $|\,{}^{m}C_{k|} \leq 1$. This implies that:

$$|x+1|^m \leq \sum_{k=0}^{m}\left|\binom{m}{k}\right||x^k| \leq \sum_{k=0}^{m}|x^k| = \sum_{k=0}^{m}|x|^k.$$

The largest value of $|x|^k$ will be at k = m and will be equal to $|x|^m$ if $|x|>1$ else it will be $x^0 =1$ if $|x|\leq 1$

So, $|x + 1|^m \leq (m+1)\max\{1,|x|^m\}$

Taking the m^th root, we get $|x+1| \leq (m+1)^{1/m} \max\{1,|x|\}$

We also know that for very large values of m, $(m+1)^{1/m}$, tends to 1[limit m tending to infinity]

Therefore,

$|x+1| \leq \max\{1,|x|\}$, which is the required statement.

Archimedean Property: *Given x, y ∈ k, x ≠ 0, there exists a positive integer n such that |nx| > |y|.*

<u>Section 3: Topology</u>

Definition 3.1 Let k be a field and | | an absolute value on k. We define the distance d(x, y) between two elements x, y ∈ k by

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

The function d(x, y) is called the metric induced by the absolute value.

Definition 3.2

Continuous function: Let k and F both be fields with absolute values, and let f : k -⟶ F be a function. We say f is continuous at $x_0 \in k$ if given any $\varepsilon > 0$ we can find $\delta > 0$ (possibly depending on both x_0 and ε) so that $d(x, x_0) < \delta \Rightarrow d(f(x), f(x_0)) < \varepsilon$.

Uniformly Continuous Function: We say f is uniformly continuous on k if δ does not depend on x_0, i.e., if given any $\varepsilon > 0$ we can find $\delta > 0$ so that for any $x, y \in k$ we have $d(x, y) < \delta \Rightarrow d(f(x), f(y)) < \varepsilon$

Lemma 3.3 (Ultrametric Inequality): Let | | be an absolute value on a field k, and define a metric by $d(x, y) = |x - y|$. Then | | is non-archimedean if and only if for any $x, y, z \in k$, we have

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

Proof:

Part 1

We know that $x-y = x-z + z-y$.

If we apply non Archimedean property on this equation, we get

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

Part 2

Given, $d(x, y) \leq \max\{d(x, z), d(z, y)\}$, we want to prove that the absolute value is non-Archimedean

$|x - y| \leq \max\ \{|x - z|, |z - y|\}$

Taking $y = -y_1$ and $z = 0$,

$|x + y_1| \leq \max\ \{|x|, |y_1|\}$ which satisfies the condition for a non-Archimedean Field [for any 2 positive real numbers, $a+b \leq \max(a,b)$]

Proposition 3.4 Let k be a field and let | | be a non-Archimedean absolute value on k. If $x, y \in k$ and $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.

Proof: Without loss of generality, we may suppose that $|x| > |y|$.

Then we know that

$$|x + y| \leq |x| = \max\{|x|, |y|\}\text{--------(a).}$$

On the other hand, $x = (x + y) - y$, so that

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

Since we know that $|x| > |y|$, this inequality can hold only if

$$\max\{|x + y|, |y|\} = |x + y|.$$

This gives that $|x| \leq |x + y|$, and from it (using (a)) we can conclude that $|x| = |x + y|$.

Corollary 3.5 In an ultrametric space, all “triangles” are isosceles.

Proof: Let x, y and z be three elements of our space (the vertices of our “triangle”).
The lengths of the sides of the “triangle”are the three distances $d(x, y) = |x - y|$, $d(y, z) = |y - z|$, and $d(x, z) = |x - z|$.
Now, $(x - y) + (y - z) = (x - z)$,
So,
Case 1: $|x-y| = |y -z|$, then the triangle is obviously isosceles since 2 sides have the same length
Case 2: $|x-y| \neq |y-z|$, then using Proposition 2.3.4, we have $|x-z| = \max\{||x-y|,|z-y|\}$
In either case, the triangle is isosceles

Definition 3.6: Let k be a field with an absolute value | |. Let $a \in k$ be an element and $r \in R^+$ be a real number.
The open ball of radius r and centre a, is the set:
$B(a, r) = \{x \in k : d(x, a) < r\} = \{x \in k : |x - a| < r\}$.
The closed ball of radius r and centre a, is the set: [represented by $\underline{B}$]
$\underline{B}(a, r) = \{x \in k : d(x, a) \leq r\} = \{x \in k : |x - a| \leq r\}$.

Proposition 3.7 Let k be a field with a non-archimedean absolute value.
i) If $b \in B(a, r)$, then $B(a, r) = B(b, r)$; in other words, every point that is contained in an open ball is a center of that ball.
ii) If $b \in \underline{B}(a, r)$, then $\underline{B}(a, r) = \underline{B}(b, r)$; in other words, every point that is contained in a closed ball is a center of that ball.
iii) The set $B(a, r)$ is both open and closed if $B(a, r)$ has empty boundary.
iv) If $r \neq 0$, the set $\underline{B}(a, r)$ is both open and closed and has empty boundary.

v) If $a, b \in k$ and $r, s \in R^{\times}_{+}$, we have $B(a, r) \cap B(b, s) \neq \phi$ if and only if $B(a, r) \subset B(b, s)$ or $B(a, r) \supset B(b, s)$; in other words, any two open balls are either disjoint or contained in one another.

vi) If $a, b \in k$ and $r, s \in R^{\times}_{+}$, we have $\underline{B}(a, r) \cap \underline{B}(b, s) \neq \phi$ if and only if $\underline{B}(a, r) \subset \underline{B}(b, s)$ or $\underline{B}(a, r) \supset \underline{B}(b, s)$; in other words, any two closed balls are either disjoint or contained in one another.

Proof

(i) By the definition, $b \in B(a, r)$ if and only if $|b - a| < r$. Now, taking any x for which $|x - a| < r$, the non-Archimedean property tells us that

$$|x - b| \leq \max\{|x - a|, |b - a|\} < r,$$

$x \in B(b, r)$; this shows that $B(a, r) \subset B(b, r)$.

Switching a and b, we get the opposite inclusion, so that the two balls are equal

We can show ii by replacing $<$ by $\leq$ in the prof for (i)

(iii) The open ball $B(a, r)$ is always an open set in any metric space. But in an ultrametric space it follows at once from (i), that the open ball of radius r around any point in the open ball is the same as $B(a, r)$

Now we need to show is that in our non-archimedean case, it is also closed. This is equivalent to saying its complement $C = \{x \in k : d(x, a) \geq r\}$ is open.

Choose any $y \in C$, so that $|y - a| \geq r$, and let $s < r$. We show that the open ball $B(y, s)$ is contained in C.

We have $|z - y| < s < r \leq |y - a|$, so by "all triangles are isosceles" we get $|z - a| = \max\{|z - y|, |y - a|\} = |y - a| \geq r$, so $z \in C$. So there is an open ball around every $y \in C$ that is entirely contained in C, which says C is an open set. Therefore its complement $B(a, r)$ is closed.

We can show (iv) by replacing $<$ by $\leq$ in the Proof for (iii). However, we need to additionally show why the condition r not equal to 0 is necessary. We need the $r \neq 0$ condition as a closed ball with radius 0 is basically a point which is not open.

(v) We can assume that $r \leq s$ without loss of generality. If the intersection is not empty, there exists $c \in B(a, r) \cap B(b, s)$. Then we know, from (i), that $B(a, r) = B(c, r)$ and $B(b, s) = B(c, s)$. Hence, $B(a, r) = B(c, r) \subset B(c, s) = B(b, s)$,

We can show (vi) by using closed balls instead of open in proof for (v) and use condition (ii).

Definition 3.8 Let k be a field with an absolute value | | (or, more generally, any metric space). We say a set S ∈ k is clopen if it is both an open and a closed set.

Disconnected Sets: A set S is called disconnected if one can find two open sets U1 and U2 such that

- S = (S ∩ U1) U (S ∩ U2),
- (S ∩ U1) ∩ (S ∩ U2) = ∅, and
- Neither S ∩ U1 nor S ∩ U2 is empty.

Proposition 3.9: In a field k with a non Archimedean absolute value, the connected component of any point x ∈ k is the set {x} consisting of only that point.

Proof:

We prove the proposition by showing that if a set contains two distinct points then it is disconnected. Suppose a set S contains both points x and y; we will show S cannot be connected.

Let $r = |x - y|$.

To show S is disconnected, we need to find the sets U1 and U2 from the definition of a disconnected set. Balls are clopen. For U1 we take the open ball of radius r/2 around x; this contains x and not y. For U2 we take the complement of U1, which is open because U1 is closed; this contains y but not x. The union of U1 and U2 is the whole space, so we get the desired result.

Section 4: Absolute values on Q

Definition 4.1 Two absolute values $| |_1$ and $| |_2$ on a field k are called equivalent if they define the same topology on k, that is, if every set that is open with respect to one is also open with respect to the other.

Lemma 4.2 Let k be a field with an absolute value | |. The following are equivalent:

i) $\lim_{n\to\infty} x_n = a$.

ii) Any open set containing a also contains all but finitely many of the x_n.

Proof:

Part 1 ii→i

Assume (ii). Since an open ball B(a, ε) centered at a is an open set, all but finitely many x_n will be in the open ball, and so there is an N such that $n \geq N$ implies a ∈ B(a, ε). Therefore for any ε an N such that $n \geq N$ implies $|x - a| < \varepsilon$, i.e., $x_n \to a$.

Part 2 i → ii

Conversely, suppose $x_n \to a$, and let U be an open set containing a. Since U is open there exists an r such that $B(a, r) \subset U$. Therefore there is an N such that $|x - a| < r$ for all $n \geq N$. Hence for all but finitely many n we have $x_n \in B(a, r) \subset U$.

Proposition 4.3 Let $| |_1$ and $| |_2$ be absolute values on a field k. The following statements are equivalent:

i) $| |_1$ and $| |_2$ are equivalent absolute values.

ii) For any sequence (x_n) in k we have $x_n \to a$ with respect to $| |_1$ if and only if $x_n \to a$ with respect to $| |_2$.

iii) For any x ∈ k we have $|x|_1 < 1$ if and only if $|x|_2 < 1$.

iv) There exists a positive real number α such that for every x ∈ k we have $|x|_1 = |x|^{\alpha}{}_2$

.Proof:

i =>ii

$| |_1$ and $| |_2$ are equivalent absolute values. So, by definition of equivalent absolute values, each sequence converging wrt one absolute value converges wrt to the other values. So, $x_n \to a$ with respect to $| |_1$ if and only if $x_n \to a$ with respect to $| |_2$.

ii=>iii

Assuming ii, given any x ∈ k, we see that $\lim_{n\to\infty} x_n = 0$ with respect to the topology induced by an absolute value | | if and only if $|x| < 1$. Therefore, iii holds

*iii=>iv

Choose any $x_0 \in k$, $x_0 \neq 0$, such that $|x_0|_1 < 1$. Then (iii) says that $|x_0|_2$ is also less than 1, so that there exists a positive real number α such that $|x_0|_1 = |x_0|_2{}^{\alpha}$. Taking logs on both sides gives us our α.

Case 1

Now choose any other $x \in k$. If $|x|_1 = |x_0|_1$, then we must also have $|x|_2 = |x_0|_2$, because otherwise either x/x_0 or x_0/x would have $|\ |_2$ less than 1 and (iii) would be violated. So in this case the equation $|x|_1 = |x|_2{}^{\alpha}$ holds.

Case 2:

If $|x|_1 = 1$, then we must have that $|x|_2 = 1$ also, so the equation $|x|_1 = |x|_2{}^{\alpha}$ holds trivially.

Case 3:

$|x|_i \neq 1$ and $|x|_i \neq |x_0|_i$ for $i = 1, 2$. We choose β such that $|x|_1 = |x|_2{}^{\beta}$; again, this means that we also have $|x_n|_1 = |x_n|_2{}^{\beta}$ for all integers n. In particular, we can assume that $|x|_1 < 1$ (otherwise replace it with 1/x), which of course also implies that $|x|_2 < 1$.

We need to show that α and β must be equal.

Let n and m be any two positive integers.

$$|x|_1^n < |x_0|_1^m \iff \left|\frac{x^n}{x_0^m}\right|_1 < 1 \iff \left|\frac{x^n}{x_0^m}\right|_2 < 1 \iff |x|_2^n < |x_0|_2^m.$$

Taking logs on the first and last equation, we get

$$n \log |x|_1 < m \log |x_0|_1 \iff n \log |x|_2 < m \log |x_0|_2,$$

This says that the set of fractions which is smaller than the first quotient of logs is exactly the same as the set of fractions which is smaller than the other; since there are fractions as close as we like to any real number, this means that the two numbers must be equal. Thus, we get

$$\frac{\log |x_0|_1}{\log |x|_1} = \frac{\log |x_0|_2}{\log |x|_2},$$

$$\frac{\log |x_0|_1}{\log |x_0|_2} = \frac{\log |x|_1}{\log |x|_2}.$$

But plugging in $|x_0|_1 = |x_0|_2{}^{\alpha}$ shows that the first quotient equals α, and similarly the second quotient equals β. This shows α = β, and we are done.

iv=>i

$|x - a|1 < r \iff |x - a|_2{}^{\alpha} < r \iff |x - a|_2 < r^{1/\alpha}$, So any open ball with respect to $| |_1$ is also an open ball (of different radius) with respect to $| |_2$. This is the condition to show that the 2 absolute values are equivalent

---

Theorem 4.4 (Ostrowski) Every non-trivial absolute value on Q is equivalent to one of the absolute values $| |_p$, where either p is a prime number or p = ∞.

Case 1 : | | is Archimedean → we will show $| | = | |_\infty$

For a ,b $\in$ Z, we write b^n in base a

$b^n = c_m a^m + c_{m-1} a^{m-1} + ... + c_1 a + c_0$; $0 \le c_i \le a$ and $m \le n\log_a b$; $a^m < b^n$

Let max c_i = B

$|B|^n \le (m+1)$ B $\max(|a|^m,1)$

$\Rightarrow |b| \le (n\log_a b + 1)B)^n \max(|a|^{\log_a b}, 1)$

$\Rightarrow |b| \le \max(|a|^{\log_a b},1)$

Since | | is Archimedean, we can choose $|b| > 1 \Rightarrow |a| > 1$ & $|b| \le |a|^{\log_a b}$ → 1

Since a and b are arbitrary constants, we can interchange a & b

$|a| \le |b|^{\log_b a}$ → 2

Because of symmetry → 1=2

$\log|a|/ \log a = \log|b|/ \log b = c$

$|a| = a^c = |a|^c_\infty = | | \approx | |_\infty$

Case 2:

| | is non-archimedean

n $\in$ Z, n>1 this implies that |n|<1

$n = p_1^{a1} p_2^{a2} ... p_n^{an}$ where each p_i are primes

Since |n|<1, there are some primes for which |p|<1

We need to show that that |p|<1 for some prime p and |q|=1 for other primes q $\neq$p

This will imply that $| | =| |_p$

Proof by Contradiction:

Let us assume we have |q|<1 for some other prime.

Then, For some r,s; we have $|rp+sq| = 1 \le \max\{|rp|,|sq|\} \le \max\{|p|,|q|\} < 1$

This proves that 1<1 which is obviously incorrect.

Therefore, |q| is not less than 1.

We can extend the theorem to Q by setting a = N/D; N,D $\in$ Z^x

----

Proposition 3.1.5 (Product Formula) For any $x \in Q^{\times}$, we have:

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

where $p \leq \infty$ means that we take the product over all of the primes of Q, including the "prime at infinity."

Proof

We write the prime factorization of $x = p_1^{x1}p_2^{x2}p_3^{x3}...p_n^{xn}$

$|x|_q = 1$ if $q \neq p_i$

$|x|_{pi} = p_i^{-xi}$

$|x|_\infty = x = p_1^{x1}p_2^{x2}p_3^{x3}...p_n^{xn}$

Multiplying all the terms, all the terms get cancelled out and we get the product =1.

Section 5: Completions

Definition 5.1

Let k be a field and let | | be an absolute value on k.

i) A sequence of elements $x_n \in k$ is called a ***Cauchy sequence*** *if for every $\varepsilon > 0$ one can find a bound M such that we have $|x_n - x_m| < \varepsilon$ whenever $m, n \geq M$.*

ii) The field k is called ***complete*** *with respect to | | if every Cauchy sequence of elements of k has a limit in k.*

iii) A subset $S \subset k$ is called ***dense*** *in k if every open ball around every element of k contains an element of S; in symbols, if for every $x \in k$ and every $\varepsilon > 0$ we have $B(x, \varepsilon) \cap S \neq \phi$.*

Completion *: There exists an inclusion $Q \to R$ of Q into a field R which is a completion:*

• the absolute value $| |_\infty$ extends to R,

• R is complete with respect to the metric given by this absolute value, and

• Q is dense in R (with respect to the metric given by $| |\infty$).

Lemma 5.2 A sequence (x_n) in a field k with a non-Archimedean absolute value | | is a Cauchy sequence if and only if we have

$$\mathbf{\lim_{n\to\infty} |x_{n+1} - x_n| = 0}$$

Proof: If m = n + r > n, we get

$|x_m - x_n| = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdot\cdot\cdot + x_{n+1} - x_n|$ - adding and subtracting the terms in between.

$|x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdot\cdot\cdot + x_{n+1} - x_n| \leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\}$(Grouping and applying non-Archimedean Condition)

Now, since the Cauchy sequence is convergent, we get the required result.

Lemma 5.3: The field Q of rational numbers is not complete with respect to any of its nontrivial absolute values.

Proof:

To construct the necessary Cauchy sequence, we need only find a sequence of solutions modulo p_n of an equation that has no solution in Q.

Case 1: p=2

Choose an integer a ∈ Z such that:

- a is not a cubic in Q;
- 2 does not divide a;
- a is a cubic residue modulo 2, i.e., the congruence $X^3 \equiv a \pmod 2$ has a solution.

Now how do we prove that such an a exists?

We can take any odd cube in Z and add to it any multiple of 2- this number will be a satisfactory value of a => a = some $n^3 + 2q$ (n is odd)

Now we construct a Cauchy sequence (with respect to $| |_p$) in the following way:

- choose x_0 to be any solution of $x_0^3 \equiv a \pmod 2$;
- choose x_1 so that $x_1 \equiv x_0 \pmod p$ and $x_1^3 \equiv a \pmod 4$;
- in general, choose x_n so that $x_n \equiv x_{n-1} \pmod{2^n}$ and $x_n^3 \equiv a \pmod{2^{n+1}}$

But we need to show that such an x_1 exists.

Given, $x_1 \equiv x_0 \pmod 2$; So $x_1 = x_0 + 2t$

$x_1^3 = x_0^3 + 6x_0t(x_0+2t)+ 8t^3$

Taking mod 4 on both sides, we get that $x_1^3 \pmod 4 = x_0^3 + 6x_0t(x_0+2t)+ 8t^3 \pmod 4$

$= x_0^3+ 2(3x_0t) \pmod 4$ which is exactly same as a(mod 4)

So, such an x_1 exists.

By induction, the series (x_n) will also exist

Checking for Cauchy Sequence:

$|x_{n+1} - x_n| = |\lambda 2^{n+1}| \leq 2^{-(n+1)} \to 0$, so the sequence is Cauchy

On the other hand, we also know that $|x_n^3 - a| = |\mu 2^{n+1}| \leq 2^{-(n+1)} \to 0$, so that the limit would have to be a cube root of a. Since a is not a cube in Q, there can be no limit in Q, which shows Q is not complete with respect to $| |_{2.}$

Case 2: p ≠ 2

Suppose p ≠ 2 is a prime.

Choose an integer a ∈ Z such that:

- a is not a square in Q;
- p does not divide a;
- a is a quadratic residue modulo p, i.e., the congruence $X^2 \equiv a \pmod p$ has a solution.

Now how do we prove that such an a exists?

We can take any square in Z and add to it any multiple of p- this number will be a satisfactory value of a this implies that a is of the form $n^2 + qp$

Now we construct a Cauchy sequence (with respect to $| |_p$) in the following way:

- choose x_0 to be any solution of $x_0^2 \equiv a \pmod p$;
- choose x_1 so that $x_1 \equiv x_0 \pmod p$ and $x_1^2 \equiv a \pmod{p^2}$;
- in general, choose x_n so that $x_n \equiv x_{n-1} \pmod{p^n}$ and $x_n^2 \equiv a \pmod{p^{n+1}}$

But we need to show that such an x_1 exists.

Given, $x_1 \equiv x_0 \pmod p$; So $x_1 = x_0 + tp$

$x_1^2 = x_0^2 + 2x_0tp + t^2p^2$

Taking mod p^2 on both sides, we get that $x_1^2 \pmod{p^2} = x_0^2 + 2x_0tp + t^2p^2 \pmod{p^2}$

$= x_0^2 + 2x_0tp \pmod{p^2}$ which is exactly same as $a \pmod{p^2}$

So, such an x_1 exists.

By induction, the series (x_n) will also exist

Checking for Cauchy Sequence:

$|x_{n+1} - x_n| = |\lambda p^{n+1}| \leq p^{-(n+1)} \to 0$, so the sequence is Cauchy

On the other hand, we also know that $|x_n^2 - a| = |\mu p^{n+1}| \leq p^{-(n+1)} \to 0$, so that the limit would have to be a square root of a. Since a is not a square in Q, there can be no limit in Q, which shows Q is not complete with respect to $| |_p$

Definition 5.4 Let | | = | |$_p$ be a non-Archimedean absolute value on Q. We denote by C, or $C_p(Q)$ if we want to emphasize p and Q, the set of all Cauchy sequences of elements of Q:

$C = C_p(Q) = \{(x_n) : (x_n)$ is a Cauchy sequence with respect to $| |_p\}$.

Proposition 5.5 Defining

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

$(x_n) \cdot (y_n) = (x_ny_n)$ makes C a commutative ring with unity.

Proof:

Sum: By rearranging the terms from LHS of the equation, we get $(x_n + y_n) - (x_m + y_m) = (x_n - x_m) + (y_n - y_m)$. Since the Left hand side of the equation is Cauchy, then the Right Hand side is also a Cauchy Sequence.

Product: $x_ny_n - x_my_m = x_n(y_n - y_m) + y_m(x_n - x_m)$, Now since x_n and y_m are bounded, we get that the sequence on the Right hand side is Cauchy

Other elements of the ring:

Zero Element: 0,0,0,0...

Unit Element: 1,1,1,1,..

Inverse Element: Will exists when the sequence is bounded away from 0, else the sequence will not Cauchy.$(y_n) = (1/x_n)$

x˜ Notation defines the constant sequence x,x,x,x,x,.....

Lemma 5.6: The map x → x˜ is an injective ring homomorphism from Q into C.

Proof

Injective => All every element in x is mapped to a unique value in x˜

Ring Homomorphism: Since all the elements in x are mapped to a unique element in x~, but this unique element = the same constant, so all the properties of homomorphism are satisfied from the definition itself.

Definition 5.7 We define $N \subset C$ to be the ideal

$N = \{(xn) : xn \to 0\} = \{(xn) : \lim_{n\to\infty} |xn|p = 0\}$ of sequences that tend to zero with respect to the absolute value | |$_p$.

Lemma 5.8 N is a maximal ideal of C.

Proof: To prove that N is a maximal ideal we first need to show that N is an ideal of C. (Since it is commutative, left ideal = right ideal)
In any Cauchy sequence (x_n), x_n is bounded. Hence, since $y_n \to 0$(by definition), then $x_ny_n \to 0$, so N is an ideal.

Let $(x_n) \in C$ be a Cauchy sequence that does not tend to zero (i.e., does not belong to N), and let I be the ideal generated by (x_n) and N. What we want to show is that I must be all of C.

We will do that by showing that the unit element $1^{\sim}$ (i.e., the constant sequence corresponding to 1) is in I. This is enough, because any ideal that contains the unit element must be the whole ring.
Now, since (x_n) does not tend to zero but is Cauchy, there must exist a number $c > 0$ and an integer N such that $|x_n| \geq c > 0$ whenever $n \geq N$.
We may define a new sequence (y_n) by setting yn = 0 if $n < N$ and yn = 1/xn if $n \geq N$.
Thus y_n is Cauchy as:

$$|y_{n+1} - y_n| = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1} - x_n|}{c^2} \longrightarrow 0,$$

and y_n belongs to C.
Now, $x_ny_n = 0$ for n<N and $x_ny_n =1$ for n≥N by observation
This sequence x_ny_n will consist of a finite number of 0's followed by an infinite number of 1s.
To make it more usable in out context, if we write the sequence $1^{\sim}$ - x_ny_n; we get a sequence of finite 1s followed by infinite zeroes(sequence tends to 0)
Thus, $1^{\sim} - x_ny_n \in$ N and $1^{\sim}$ can be written as a multiple of (xn) + an element of N and hence it belongs to C.

Definition 5.9 We define the field of p-adic numbers to be the quotient of the ring C by its maximal ideal N: Qp = C/N.

Lemma 5.10: Let (xn) ∈ C, (xn) ⋹ N. The sequence of real numbers $|x_n|_p$ is eventually stationary, that is, there exists an integer N such that $|x_n|_p = |x_m|_p$ whenever m, n ≥ N.

Proof:

Since (x_n) is a Cauchy sequence which does not tend to zero, we can find c and N1 such that $n \geq N1 \Rightarrow |x_n| \geq c > 0$.

On the other hand, there also exists an integer N2 for which

$n, m \geq N2 \Rightarrow |x_n - x_m| < c$.

We want both conditions to be true at once, so set N = max{N1,N2}. Then we have $n, m \geq N \Rightarrow |x_n - x_m| < \min\{|x_n|, |x_m|\}$, which gives $|x_n| = |x_m|$ by the non-archimedean property

---

Definition 5.11 If λ ∈ Qp is an element of Qp, and (xn) is any Cauchy sequence representing λ, we define $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$.

Proposition 5.12 The image of Q under the inclusion Q → Qp is a dense subset of Qp.

Proof: let (x_n) be a Cauchy sequence representing λ, and let ε' > 0 be a number slightly smaller than ε – Why? We need to decrease ε slightly to guarantee that y doesn't end up in the closed ball of radius ε

We need to show that any open ball around an element λ ∈ Qp contains an element of the image of Q, i.e., a constant sequence. So, we fix a radius ε > 0. We need to show that there is exists a constant sequence belonging to the open ball B(λ, ε).

Let (x_n) be a Cauchy sequence representing λ, and let ε' > 0 be a number slightly smaller than ε. By the Cauchy property, there exists a number N such that $|x_n - x_m|_p < \varepsilon'$ whenever n, m ≥ N. Let $y = x_N$ and consider the constant sequence ˜y.

We claim that y ∈ B(λ, ε), i.e., that $|\lambda - \tilde{}y|_p < \varepsilon$.

How?

$|(x_n - y)|_p = \lim_{n\to\infty} |x_n - y|_p$.

But for any n ≥ N we have $|x_n - y|_p = |x_n - x_N|_p < \varepsilon'$ so that, in the limit, we get $\lim_{n\to\infty} |x_n - y|_p \leq \varepsilon$ '< ε, so that (y) does indeed belong to B(λ, ε).

< becomes ≤ in the final step because it's perfectly possible for a sequence to tend to a certain value while remaining consistently smaller than that value.

Theorem 5.13 Q_p is complete with respect to $| |_p$.

Proof:

Let λ_1, λ_2, ..., λ_n,... be a Cauchy sequence of elements of Q_p, so that each λ_i is a Cauchy sequence of elements of Q.

Since the image of Q is dense in Q_p, we can find, for each i, a number $y_i \in Q$ such that the constant sequence $\tilde{}y_i \in Q_p$ tends to λ_i as i tends to infinity.

$|\lambda_i - y\tilde{}_i|_p < 1/i$,

Now, we know that the sequence ($\tilde{}y_n$) (a sequence of constant sequences in Qp) is Cauchy. Therefore, since the absolute value of a constant sequence is the absolute value of the constant, the sequence (y_n) (a sequence of rational numbers) is Cauchy, so defines an element of Qp.

Let λ be the element of Q_p corresponding to (y_n).

The sequence λ is the limit we are looking for.

Let $\varepsilon > 0$. Since $\lambda = (y_n)$ is Cauchy, there exists an N such that n, m ≥ N implies

$|y_m - y_n| < \varepsilon/2$.

Consider the sequence of constant sequences ($\tilde{}y_n$).

The difference $\lambda - y\tilde{}_n$ is represented by $(y_m - y_n)$, where n is fixed and m varies.

So if m ≥ N we have $|\lambda - y\tilde{}_n|_p = \lim_{m\to\infty} |y_m - y_n|_p \leq \varepsilon/2 < \varepsilon$.

Therefore the sequence $\lambda - (\tilde{}y_n)$ converges to 0 in Q_p.

Now, we know that $|\lambda_n - y\tilde{}_n|$ converges to zero, and we know that ($\tilde{}y_n$) converges to λ. Therefore (λ_n) converges to λ. Since (λ_n) was an arbitrary Cauchy sequence in Q_p, any Cauchy sequence in Q_p has a limit.

Section 6: Exploring Q_p

Definition 6.1 The ring of p-adic integers is the valuation ring

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

Valuation Ring: *A valuation ring is an integral domain D such that for every element x of its field of fractions F, at least one of x or x^{-1} belongs to D.*

Proposition 6.2: The ring Z_p of p-adic integers is a local ring whose maximal ideal is the principal ideal $pZ_p = \{x \in Q_p : |x|_p < 1\}$. Furthermore,

i) $Q \cap Z_p = Z_{(p)} = \{a/b \in Q : p \nmid b\}$.

ii) The inclusion $Z \rightarrow Z_p$ has dense image. Specifically, given $x \in Z_p$ and $n \geq 1$, there exists an $\alpha \in Z$, $0 \leq\alpha \leq p^n -1$, such that $|x-\alpha|_p \leq p^{-n}$. The integer α with these properties is unique.

iii) For any $x \in Z_p$, there exists a Cauchy sequence (α_n) converging to x, of the following type:

•$\alpha_n \in Z$ satisfies $0 \leq\alpha_n \leq p^n - 1$

•for every $n \geq 2$ we have $\alpha_n \equiv\alpha_{n-1} \pmod{p^{n-1}}$.

The sequence (αn) with these properties is unique.

Proof:

Z_p is a valuation ring, hence it is a local ring, and so there exists a unique maximal ideal and every element of Z_p not in the maximal ideal is invertible in Z_p.

If $|x|_p < 1$, then $|x|_p \leq 1/p$; since $|p|_p = 1/p$, which implies that $|x/p|_p \leq 1$, and so $x \in pZ_p$. This shows that the valuation ideal is contained in pZ_p and since the valuation ideal is a maximal ideal, and $pZ_p \neq Z_p$.

i) Z(p) is the valuation ring in Q corresponding to the p-adic valuation. Hence using the definition of a valuation ring and intersecting it with Q, we get **$Q \cap Z_p = Z_{(p)} = \{a/b \in Q : p \nmid b\}$.**

ii) We choose an $x \in Zp$ and $n \geq 1$. Since Q is dense in Qp, we find $a/b \in Q$ which is as close as we like to x.

We choose the corresponding a/b, so that:

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

For rational number a/b, we will have

$$\left|\frac{a}{b}\right|_p \leq \max\left\{|x|_p, \left|x-\frac{a}{b}\right|_p\right\} \leq 1$$

which says that a/b ∈ Z(p).

Now, from the elementary theory of congruences, if p∤b, there exists an integer b' ∈ Z such that bb' ≡ 1 (mod p^n), unique mod p^n.

This implies

$$\left|\frac{a}{b}-ab'\right|_p \leq p^{-n},$$

Finally, we need to check whether we can find an integer between zero and $p^n - 1$. We conclude this from the definition of closeness in terms of p-adic numbers: two integers are p^{-n}-close iff they are congruent mod p^n.

Choosing α to be the unique integer such that $0 \leq \alpha \leq p^n - 1$ and α ≡ ab' (mod p^n) gives the desired result: $|x - \alpha|_p \leq p^{-n}$

iii) To prove (iii), we use (ii) for a sequence of integers n = 1, 2, ...

So, there exists an α_n ∈ Z, $0 \leq \alpha_n \leq p^n - 1$, such that $|x-\alpha_n|_p \leq p^{-n}$

Constructing this sequence for n=1,2,3... will give us the desired Cauchy sequence.

Since at each step of the construction in (ii) our choices were unique mod p^n, the constructed sequence is unique.

Corollary 6.3: $Q_p = Z_p[1/p]$, that is, for every x ∈ Q_p there exists an n ≥ 0 such that $p^n x$ ∈ Zp. The map Qp → Qp given by x → px is a homeomorphism.

Proof: If x ∈ Q_p, we can compute its valuation $v_p(x)$.

If $v_p(x) \geq 0$, then x is already an element of Z_p, by the definition of a valuation ring.

Otherwise, if $v_p(x)$ is negative, then we have

$$v_p(p^{-v_p(x)}x) = -v_p(x) + v_p(x) = 0,$$

which means that $p^{-v_p(x)}x \in Z_p$. That multiplication by p is a homeomorphism since the field operations are continuous functions.

Corollary 6.4 Qp is a totally disconnected Hausdorff topological space

Proof: We have already proved that Qp is a totally disconnected in an ultrametric space, so we just need to show that Qp is Hausdorff. Since Qp is a metric space and all metric spaces are Hausdorff, Qp is a totally disconnected Hausdorff Space.

Compactness: *A subset X of a topological space is called compact if any collection of open sets which covers X has a finite subcollection which also covers X.*

Local Compactness*: A space is called locally compact when every point has a neighborhood which is a compact set.*

Corollary 6.5 Z_p is compact, and Q_p is locally compact

Proof

Since Z_p is a neighbourhood of zero, proving that it is compact is enough to prove that Q_p is locally compact, so that the second statement follows from the first.

To prove the first statement, we already know that Z_p is complete since it is a closed set in a complete field. We just need to prove that it is totally bounded.

So we need to show that for any $\varepsilon > 0$ one can cover Z_p with finitely many balls of radius ε. It is enough to check this for every $\varepsilon = p^{-n,}$ $n \geq 0$

Therefore, as a ranges through 0, 1, ..., $p^n - 1$, the p^n balls

$$a + p^n\mathbb{Z}_p = \{a + p^n x : x \in \mathbb{Z}_p\} = \{y \in \mathbb{Z}_p : |y - a| \leq p^{-n}\} = \overline{B}(a, p^{-n})$$

cover Z_p(cosets of p^nZ_p in Z_p are also balls in the p-adic topology) and hence Z_p is totally bounded and hence compact.

---

p-adic units

The p-adic units are the invertible elements of Z_p denoted by Z^x_p . Since $x \in Z_p$ means $|x|_p \leq 1$ and $x^{-1} \in Z_p$ means $|x-1|p = |x|^{-1}_p \leq 1$, we see that

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}. \quad \textit{and} \quad \mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid ab\right\}.$$

We use a concept of Coherent Sequences to prove the next lemma. If we take a p-adic integer x ∈ Zp, then there exists a coherent sequence of integers α_n converging to x such that:

- $\alpha_n \equiv x \pmod{p^n}$
- $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$

- $0 \leq \alpha_n \leq p^n - 1$.

Lemma 6.6: Given any $x \in Z_p$, the series $b_0 + b_1p + b_2p^2 + \ldots + b_np^n + \ldots$ converges to x with $0 \leq bi \leq p - 1$, and this representation is unique.

Proof:

A series will converge iff its partial sums (sum of first n finite terms, taking n=1,2,3..) converge.

$\alpha_1 = b_{0;}\ 0 \leq b_0 \leq p - 1$

$\alpha_2 = b_0 + b_1p;\ 0 \leq b_1 \leq p - 1$

$\alpha_3 = b_0 + b_1p + b_2p^2;\ 0 \leq b_2 \leq p - 1$

$\alpha_4 = b_0 + b_1p + b_2p^2 + b_3p^3;\ 0 \leq b_3 \leq p - 1$

The partial sums of our series are exactly the α_n, which we already know converge to x.

(the b_i can be imagined as digits of x written in base p expansion).

Since the α_n of the coherent sequence are unique this implies that the b_n are too (because they are just the digits in base p).

Corollary 6.7: Every $x \in Qp$ can be written in the form

$x = b_{-m}p^{-m} + \ldots + b_{-1}p^{-1} + b_0 + b_1p + b_2p^2 + \ldots + b_np^n + \ldots$ with $0 \leq b_n \leq p - 1$ and $-m = v_p(x)$. This representation is unique.

Proof: If $x \in Qp$, there exists $m \in Z$ such that $p^m \in Z_p$

$p^m\, x = b_0 + b_1p + b_2p^2 + \ldots + b_np^n + \ldots$

Dividing both sides by p^m, we get $x = b_{-m}p^{-m} + \ldots + b_{-1}p^{-1} + b_0 + b_1p + b_2p^2 + \ldots + b_np^n$.

$|x|_p = p^{-vp(x)} = p^m$ and so $m = -v_p(x)$.

Corollary 6.8 Choose $A \subset Z_p$ to be a set of representatives of Z/pZ. Every $x \in Qp$ can be written in the form:

$x = b_{-m}p^{-m} + \ldots + b_{-1}p^{-1} + b_0 + b_1p + b_2p^2 + \ldots + b_np^n + \ldots$ with $bn \in A$ for each n and $-n_0 = v_p(x)$. This representation is unique.

Proof: Suppose $x \in Z_p$ and look at its image in $Z_p/pZ_p = Z/pZ$.

By our choice of A there is a unique element $b_0 \in A$ such that $x - b_0 \in pZ_p$.

Then $x - b_0 = px_1$ for some $x_1 \in Z_p$. There exists a unique $b_1 \in A$ such that $x_1 - b_1 \in pZ_p$, so that $x = b_0 + b_1p + p_2x2$ for some $x_2 \in Z_p$.

Continuing in this way, we obtain for each n: $x = b_0 + b_1p + b_2p^2 + \cdots + b_np^n + p^{n+1}x_{n+1}$ with $x \in Z_p$, and so $|x - (b_0 + b_1p + b_2p^2 + \cdots + b_np^n)| \leq p-(n+1)$. This shows that the series $b_0 + b_1p + b_2p2 + \cdots + b_np^n + \cdots$ converges to x.

If $x \notin Z_p$, we write $x = p^{-m}x_0$ with $x_0 \in Zp$, expand x_0 as we did with x before and multiply by p^{-m} to get our series.

Theorem 6.9: Z_2 with the 2-adic norm is homeomorphic to the middle thirds Cantor set C with the norm it inherits from R.

Proof:

Any real number $y \in [0, 1]$ can be represented as

$y = a_13 + a_23^2 + \cdots + a_n3^n + \cdots$ with $a_i \in \{0, 1, 2\}$.

On the other hand, any element $z \in Z_2$ has a 2-adic expansion $y = b_0 + b_12 + b_22^2 + \cdots + b_n2^n + \cdots$ with $b_i \in \{0, 1\}$. There is a bijection from $\{0, 1\} \rightarrow \{0, 2\}$: $(f(x) = 2x)$

So we can make a function $f : Z_2 \rightarrow C$ like this $f(b_0 + b_12 + \cdots + b_n2^n + \cdots) = 2b_03 + 2b_13^2 + \cdots + 2b_n3^{n+1} + \cdots$Similarly we construct a bijection from {0,2}->{0,1}.

Hence Z_2 with the 2-adic norm is homeomorphic to the middle thirds Cantor set C with the norm it inherits from R

Section 7: Hensel's Lemma

*Definition 7.1 Let $F(X) = a_0+a_1X+a_2X^2+\cdots+a_nX^n$ be a polynomial with coefficients ai $\in R$, where R is a ring. The **formal derivative** of F(X) is*

$$F'(X) = a1 + 2a2X + \cdots + nanXn-1.$$

Theorem 7.2 (Hensel's Lemma) Let $F(X) = a_0 +a_1X +a_2X^2+\cdots+ a_nX^n$ be a polynomial whose coefficients are in Z_p. Suppose that there exists a p-adic integer $\alpha_1 \in Z_p$ such that

$$\mathbf{F(\alpha_1) \equiv 0 \ (modpZ_p)}$$

and

$$\mathbf{F'(\alpha_1) \ !\equiv 0 \ (modpZ_p),}$$

where F'(X) is the formal derivative of F(X). Then there exists a unique p-adic integer $\alpha \in Z_p$ such that $\alpha \equiv \alpha_1$ (mod pZ_p) and $F(\alpha) = 0$.

Proof: We will show that the root α exists by constructing a Cauchy sequence of integers converging to it. The idea is essentially what is known as "Newton's method" which I have studied in Numerical Analysis.

We construct a Cauchy sequence of integers $\alpha_1, \alpha_2, ..., \alpha_n, ...$ such that, for all $n \geq 1$, we have

i) $F(\alpha_n) \equiv 0$ (mod p^n),

ii) $\alpha_{n+1} \equiv \alpha_n$ (mod p^n).

Its limit α will satisfy $F(\alpha) = 0$ (by continuity) and $\alpha \equiv \alpha_1$ (mod p) (by construction). Conversely, a root α will determine such a sequence α_n. Thus, once we have $\alpha_{n,}$ the theorem will be proved. The main assumption in the theorem is that α_1 exists. To find α_2, we note that condition (ii) requires that

$\alpha_2 = \alpha_1 + b_1p$ for some $b_1 \in Z_p$.

Plugging this expression into the polynomial F(X) and expanding, we get

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1 p) \\ &= F(\alpha_1) + F'(\alpha_1)b_1p + \text{terms in } p^n,\ n \geq 2 \\ &\equiv F(\alpha_1) + F'(\alpha_1)b_1p \pmod{p^2}. \end{aligned}$$

To show that one can find α2, we have to show that one can find b_1 so that

$$F(\alpha_1) + F'(\alpha_1)b_1p \equiv 0 \pmod{p^2}.$$

Now, we know that $F(\alpha_1) \equiv 0$ (mod p), so that $F(\alpha_1) = px$ for some x. The equation then becomes

$$x + F'(\alpha_1)b_1 \equiv 0 \pmod{p}.$$

after we divide by p.

$F'(\alpha_1)$ is not divisible by p, and hence is invertible in Zp, so we can take

$$b_1 \equiv -x(F'(\alpha_1))^{-1} \pmod{p}.$$

We can choose such a b_1 in Z, with $0 \leq b_1 \leq p - 1$, where b_1 is uniquely determined. For this choice of b_1, we set $\alpha_2 = \alpha_1 + b_1p$, which will have the stated properties. This shows that one can take the first step: given α_1, find α_2. Similarly using induction, we get a_{n+1} using a_n. Hence, we can construct the whole sequence, and it is uniquely determined at each step.

Alternate form of Hensel’s Lemma (in the form of Newton Raphson Method):

Let $F(X) = a_0 + a_1X + a_2X2 + \cdot\cdot\cdot + a_nXn$ be a polynomial whose coefficients are in Z_p. Suppose that there exists a p-adic integer $\alpha_1 \in Z_p$ such that $|F(\alpha_1)| < 1$ and $|F'(\alpha_1)| = 1$. Setting, for each $n \geq 1$,

$$\alpha_{n+1} = \alpha_n - F(\alpha_n) / F'(\alpha_n)$$

defines a convergent sequence whose limit $\alpha \in Z_p$ is the unique p-adic integer such that $|\alpha - \alpha_1| < 1$ and $F(\alpha) = 0$.

Proposition 7.3 For any prime p and any positive integer m not divisible by p, there exists a primitive m-th root of unity in Q_p if and only if m divides $p - 1$.

Proof:

For each m dividing p−1, we can find m incongruent roots of $X_{m-1} \equiv 0 \pmod p$. Then using Hensel’s Lemma we see that we have m different roots of X_{m-1}, which are the mth roots of unity.

Now we need to show that there are no other roots of unity.

Specifically, we show that if $\zeta_k = 1$ and $p \nmid k$ then in fact $\zeta_m = 1$ for some m dividing $p - 1$.

Using the uniqueness part of Hensel’s Lemma, suppose $\zeta_k = 1$.

Then $\zeta_k \equiv 1 \pmod p$ and we also we know that there is an m dividing p−1 such that $\zeta_m \equiv 1 \pmod p$.

By Hensel’s Lemma, there is a unique $\zeta_1 \equiv \zeta \pmod p$ such that $\zeta_1^m = 1$. But then, since m divides k, ζ_1 is a root of $X^k - 1$ as well, and it is congruent mod p to ζ. Thus,using the uniqueness part of Hensel’s Lemma, $\zeta_1 = \zeta$.

Proposition 7.4 Let $p \neq 2$ be a prime, and let $b \in Z_p^{\times}$ be a p-adic unit.

If there exists an $\alpha_1 \in Z_p$ such that $\alpha_1^2 \equiv b \pmod{pZ_p}$, then b is the square of an element of $Z_p^{\times}$.

Proof:

$F(X) = X^2 - b$

$F(\alpha_{1)} = \alpha_1^2 - b.$

Therefore, $F(\alpha_1) \equiv 0 \pmod p$ which implies $\alpha_1^2 - b \equiv 0 \pmod p$

Finally, $F'(\alpha_1) = 2\alpha_1 !\equiv 0 (\bmod p)$. Hence b is the square of an element of $Z_p^{\times .}$

Definition 7.5: ***Relatively Prime Polynomials****.*

Let g(X) and h(X) be polynomials in $Z_p[X]$.

Let g¯(X) and h¯(X) ∈ $F_p[X]$ be the polynomials obtained by reducing the coefficients modulo p.

We say g(X) and h(X) are relatively prime modulo p if gcd(g¯, h¯)=1 in $F_p[X]$, or, equivalently, if there exist polynomials a(X), b(X) ∈ Zp[X] such that

$$a(X)g(X) + b(X)h(X) \equiv 1 \ (\mathrm{mod}\ p),$$

where we understand congruence coefficient-by-coefficient, i.e., we say two polynomials are congruent modulo p if each coefficient of one is congruent modulo p to the corresponding coefficient of the other.

Theorem 7.5 (Hensel's Lemma for Polynomials) Let f(X) ∈ $Z_p[X]$ be a polynomial with coefficients in Z_p, and assume that there exist polynomials

$g_1(X)$ and $h_1(X)$ in $Z_p[X]$ such that

i) $g_1(X)$ is monic,

ii) $g_1(X)$ and $h_1(X)$ are relatively prime modulo p, and

iii) $f(X) \equiv g_1(X)h_1(X)$ (mod p) (understood coefficient-by-coefficient).

Then there exist polynomials g(X), h(X) ∈ $Z_p[X]$ such that

i) g(X) is monic,

ii) $g(X) \equiv g_1(X)$ (mod p) and $h(X) \equiv h_1(X)$ (mod p), and

iii) f(X) = g(X)h(X).

Proof:

Let d be the degree of f(X), and m be the degree of $g_1(X)$(monic).

Then we can assume that $\deg(h_1) \leq d - m$ (it could be less, because the top coefficient of f could be divisible by p).

We want to construct two sequences of polynomials gn(X) and hn(X) such that

i) each g_n is monic and of degree m,

ii) $g_{n+1} \equiv g_n$ (mod p^n) and $h_{n+1} \equiv h_n$ (mod p^n), and

iii) $f(X) \equiv g_n(X)h_n(X)$ (mod p^n).

If we can find such sequences, we are done, since going to the limit gives the desired polynomials g(X) and h(X). In other words, the coefficients of g(X) will be the limits of the corresponding coefficients of the $g_n(X)$.

We already have $g_1(X)$ and $h_1(X)$, now we need to get $g_2(X)$ and $h_2(X)$.

Since the g's are to be congruent, we must have $g_2(X) = g_1(X) + p\, r_1(X)$ for some polynomial $r_1(X) \in Z_p[X]$;

Similarly, we must have $h_2(X) = h_1(X) + p\, s_1(X)$. To show that g_2 and h_2 exist, we have to show that it is possible to find r_1 and s_1 such that the above stated conditions are satisfied. For that, we need to solve the equation:

$f(X) \equiv g_2(X)h_2(X) \pmod{p^2}$

So, $f(X) \equiv (g_1(X) + p\, r_1(X))(h_1(X) + p\, s_1(X)) \pmod{p^2}$.

$\equiv g_1(X)h_1(X) + p\, r_1(X)h_1(X) + p\, s_1(X)g_1(X) + p^2\, r_1(X)s_1(X)$

$\equiv g_1(X)h_1(X) + p\, r_1(X)h_1(X) + p\, s_1(X)g_1(X) \pmod{p^2}$.

Now, $f(X) \equiv g_1(X)h_1(X) \pmod{p}$, so that we have $f(X) - g_1(X)h_1(X) = p\, k_1(X)$ for some $k_1(X) \in Z_p[X]$.

Rearranging, we get $p\, k_1(X) \equiv p\, r_1(X)h_1(X) + p\, s_1(X)g_1(X) \pmod{p^2}$.

Dividing through by p, we get

$$k_1(X) \equiv r_1(X)h_1(X) + s_1(X)g_1(X) \pmod{p}.$$

This is the equation we need to solve to determine r1 and s1.

We have assumed that g_1 and h_1 are relatively prime modulo p.

This means that we know that there exist a(X), b(X) ∈ Zp[X] such that

$a(X)g_1(X) + b(X)h_1(X) \equiv 1 \pmod{p}$.

Consider, then, the two polynomials $r_1\tilde{}(X) = b(X)k_1(X)$ and $s_1\tilde{}\,(X) = a(X)k_1(X)$

These will make all the congruence conditions true. The only problem is that we have no control over the degree of $r_1\tilde{}\,(X)$; if that degree is bigger than m, then $g_1(X) + pr_1\tilde{}\,(X)$ will not be monic of degree m.

To remedy that:

We already know that $r_1\tilde{}\,(X)h1(X)+ s_1\tilde{}\,(X)g1(X) \equiv k1(X) \pmod{p}$.

Now divide $\tilde{}r_1(X)$ by $g_1(X)$, and let r1(X) be the remainder: $r_1\tilde{}\,(X) = g_1(X)q(X) + r_1(X)$.

And now we know that deg $r_1(X) <$ deg $g_1(X)$. If we set $s_1(X) = \tilde{s}_1(X) + h_1(X)q(X)$, it all works out:

$r_1(X)h_1(X) + s_1(X)g1(X) \equiv (\tilde{r}_1(X) - g_1(X)q(X))h_1(X) + (\tilde{s}_1(X) + h_1(X)q(X))g_1(X)$
$\equiv \tilde{r}_1(X)h_1(X) - g_1(X)h_1(X)q(X) + \tilde{s}_1(X)g_1(X) + g_1(X)h_1(X)q(X)$
$\equiv \tilde{r}_1(X)h_1(X) + \tilde{s}_1(X)g_1(X) \equiv k_1(X)$ (mod p), so that our congruence conditions are satisfied, and the fact that the degree of $r_1(X)$ is smaller than the degree of $g_1(X)$ is enough to guarantee that $g_1(X) + pr_1(X)$ is monic, and we are done.

This shows that g_2 and h_2 exist. Since they are congruent to g_1 and h_1 modulo p, they are also relatively prime modulo p. We repeat the same method to find g_3 and h_3 and so on.

Section 8: Elementary Analysis in Q_p

Lemma 8.1 A sequence (a_n) in Q_p is a Cauchy sequence, and therefore convergent, if and only if it satisfies lim $_{n\to\infty}$ $|a_{n+1} - a_n| = 0$.

Proof: We have already proved the result for any field K, taking K = Qp gives us the result.

Corollary 8.2 An infinite series $\sum_{n=0}^{\infty} a_n$ with an ∈ Q_p is convergent if and only if $\lim_{n\to\infty} a_n = 0$, in which case we also have

$$\left|\sum_{n=0}^{\infty} a_n\right| \leq \max_n |a_n|.$$

Proof

A series converges when the sequence of partial sums converges.

Now, the n-th term an is exactly the difference between the n-th and the (n − 1)-st partial sums; if it tends to zero, it follows from previous Lemma that the sequence of partial sums is a Cauchy sequence, hence is convergent.

Using Ultrametric Inequality and induction,

|a1+a2| ≤ max{a1,a2}

|a1+a2+a3|≤max{a1,|a2,a3|} ≤ max{a1,a2,a3}

Hence for n terms:

$$\left|\sum_{n=0}^{\infty} a_n\right| \leq \max_n |a_n|.$$

Proposition 8.3 Let $b_{ij} \in Q_p$, and suppose that

i) for every i, $\lim_{j\to\infty} b_{ij} = 0$, and

ii) $\lim_{i\to\infty} b_{ij} = 0$ uniformly in j.

Then both series

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) \qquad \textit{and} \qquad \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

converge, and their sums are equal.

Proof

We know that given ε we can choose N such that if max{i, j} ≥ N then $|b_{ij}| < \varepsilon$. In particular, bij tends to zero for every i when j → ∞ and vice versa, which means that the internal sums

$$\sum_{j=0}^{\infty} b_{ij} \qquad \text{and} \qquad \sum_{i=0}^{\infty} b_{ij}$$

converge (the first for all i, and the second for all j). In addition, for i ≥ N and j≥N we have,

$$\left|\sum_{j=0}^{\infty} b_{ij}\right| \leq \max_j\{|b_{ij}|\} < \varepsilon; \qquad \text{and} \qquad \left|\sum_{i=0}^{\infty} b_{ij}\right| < \varepsilon.$$

we see that

$$\lim_{i\to\infty}\sum_{j=0}^{\infty} b_{ij} = 0 \qquad \text{and} \qquad \lim_{j\to\infty}\sum_{i=0}^{\infty} b_{ij} = 0,$$

so that both double series converge.

Now, we need to show that the double sums are equal.

For that, we continue to use N and ε chosen as above, so that $|b_{ij}| < \varepsilon$ when either i or j is ≥ N, and we use over and over the fact that in a non-Archimedean field a bound on each term in a sum gives a bound on the sum itself; this is just the ultrametric inequality |x + y| ≤ max{|x|, |y|}

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right)\right| = \left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right) + \sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right|$$

Now, if j ≥ N + 1, we have |bij | < ε for every i; by the ultrametric inequality, it follows that

$$\left|\sum_{j=N+1}^{\infty} b_{ij}\right| < \varepsilon$$

and using ultrametric inequality, we get

$$\left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right)\right| < \varepsilon.$$

And Similarly, $$\left|\sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right| < \varepsilon,$$

Using ultrametric inequlity, we finally get

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right)\right| < \varepsilon.$$

Reverising i and j,

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right| < \varepsilon.$$

Since this is true for any ε > 0 it follows that the two sums must be equal

----

Definition 8.4 Let $U \subset Q_p$. A function $f : U \to Q_p$ is said to be ***continuous*** *at $a \in U$ if for every $\varepsilon > 0$ there exists a $\delta > 0$ (possibly depending on a) such that, for every $x \in U$,*

$$|x - a| < \delta \Longrightarrow |f(x) - f(a)| < \varepsilon.$$

Let $U \subset Q_p$. A function $f : U \to Q_p$ is said to be uniformly continuous on U if for every $\varepsilon > 0$ there exists a $\delta > 0$ such that, for all $x, y \in U$,

$|x - y| < \delta \Longrightarrow |f(x) - f(y)| < \varepsilon.$

Definition 8.5 Let $U \subset Q_p$ be an open set, and let $f : U \to Q_p$ be a function. We say f is ***differentiable*** *at $x \in U$ if the limit*

$$f'(x) = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h}$$

exists. If f'(x) exists for every x in U we say f is differentiable in U, and we write f': U → Q_p for the function x → f'(x).

Section 9: Power Series

Proposition 9.1:

$$\rho = \frac{1}{\limsup\limits_{n\to\infty} \sqrt[n]{|a_n|}},$$

where we use the usual conventions when the limit is zero or infinity, so that

$0 \leq \rho \leq \infty$.

i) If $\rho = 0$, then f(x) converges only when x = 0.

ii) If $\rho = \infty$, then f(x) converges for every $x \in Q_p$.

iii) If $0 < \rho < \infty$ and $\lim_{n\to\infty} |a_n|\rho^n = 0$, then f(x) converges if and only if $|x| \leq \rho$.

iv) If $0 < \rho < \infty$ and $|a_n|\rho^n$ does not tend to zero as n goes to infinity, then f(x) converges if and only if $|x| < \rho$.

Proof:

We know that the region of convergence for the problem is:

$$\left\{x \in \mathbb{Q}_p : \lim_{n\to\infty} |a_n x^n| = 0\right\}$$

From this we can directly conclude that f(0)=0.

(i) if $|x| > \rho$, we see that $|a_n||x|^n$ cannot tend to zero when n tends to infinity: the definition of ρ implies that for infinitely many values of n, |an| is close to $1/\rho^n$, and, since $|x| > \rho$, $(|x|/\rho)^n$ gets arbitrarily large as n grows.

(ii) Similarly, if $|x| < \rho$, choose a ρ1 such that $|x| < \rho_1 < \rho$. Then $|x|/\rho_1 < 1$ and for all but finitely many n we have $|a_n| < 1/ \rho_1^n$, so $|a_n x_n| \leq |x|^n/\rho_1^n$ and so $|a_n x_n| \to 0$

(iii) Finally, the statements about what happens when $|x| = \rho$: Applying the corollary 8.2 directly gives us the remaining conditions.

Lemma 9.2 Let f(X) = $\sum_{n=0}^{\infty} a_n$ be a power series with coefficients in Qp. If f(x) converges when $|x| \leq r$, then the function f : B(0, r) → Qp defined by x→ f(x) is bounded and uniformly continuous.

Proof:

Bounded:

Since f converges on B(0, r), we know that $|a_n|r^n$ tends to 0 as n → ∞.

It follows that $M = \max_{n\geq 0}\{|a_n|r^n\}$is finite.

We first show f(x) is bounded on B(0, r).

If $|x| \leq r$ we have $|f(x)| \leq \max\{| a_n x_n |\} \leq \max\{|a_n|x_n \} = M$, which shows that f(x) is bounded by M when x ∈ B(0, r)

Uniformly Continuous:

For uniform continuity, suppose x, y ∈ B(0, r). If we subtract f(y) from f(x), the constant terms cancel and we can factor out (x − y) from the remaining sum:

$$\begin{aligned} f(x) - f(y) &= \sum_{n=1} a_n(x^n - y^n) \\ &= \sum_{n=1}^{\infty} a_n(x-y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}) \\ &= (x-y)\sum_{n=1}^{\infty} a_n(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}). \end{aligned}$$

$$\left|x^{n-1} + x^{n-2}y + \cdots + y^{n-1}\right| \leq \max_{0\leq i\leq n-1}\{|x|^{n-1-i}|y|^i\} \leq r^{n-1}$$

$$\left|\sum_{n=1}^{\infty} a_n(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})\right| \leq \max\{|a_n|r^{n-1}\} = \frac{1}{r}M_r.$$

$$|f(x) - f(y)| \leq \frac{1}{r}M_r|x-y|,$$

Corollary 9.3 Let $f(X) = \sum a_n X^n$ be a power series with coefficients in Qp, and let D ⊂ Qp be its region of convergence, i.e., the set of x ∈ Qp for which f(x) converges. The function

f : D → Qp

defined by x → f(x) is continuous on D.

Proof:

Let $f(X) = \sum a_n X^n$ and let D be its region of convergence, which is a ball centred at 0 which might be open or closed.

If f(x) converges and |x| = r, then we know by Proposition 9.1 that the closed ball B(0, r) is contained in D. Hence, f is continuous on B(0, r), and thus continuous at x.

Proposition 9.4 Let f(X) = $\sum_{n=0}^{\infty} a_n$ be a power series with coefficients in Qp, and let α ∈ Qp, α ≠ 0, be a point for which f(α) converges. For each m ≥ 0, define

$$b_m = \sum_{n \geq m} \binom{n}{m} a_n \alpha^{n-m},$$

and consider the power series

$$g(X) = \sum_{m=0}^{\infty} b_m (X - \alpha)^m.$$

i) The series defining b_m converges for every m, so that the b_m are well defined.

ii) The power series f(X) and g(X) have the same region of convergence, that is, f(λ) converges if and only if g(λ) converges.

iii) For any λ in the region of convergence, we have g(λ) = f(λ).

Proof:

Since binomial coefficients are integers and α belongs to the region of convergence for f(X), we get

$$\left| \binom{n}{m} a_n \alpha^{n-m} \right| \leq |a_n \alpha^{n-m}| = |\alpha|^{-m} \cdot |a_n \alpha^n| \to 0,$$

which gives the desired convergence by Corollary 8.2.

To show (ii) and (iii), we take any λ in the region of convergence of f(X), and compute

$$f(\lambda) = \sum_n a_n (\lambda - \alpha + \alpha)^n = \sum_n \sum_{m \leq n} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m.$$

The last sum looks a lot like a partial sum for g(λ), except that it needs to be re-ordered. For that, we use Proposition 8.3. To check that the condition is satisfied, we set

$$\beta_{nm} = \begin{cases} \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m & \text{if } m \leq n \\ 0 & \text{if } m > n \end{cases}$$

We need to check that the sequence β_{nm} satisfies the conditions in Proposition 8.3. We see that

$$|\beta_{nm}| = \left| \binom{n}{m} a_n \alpha^{n-m} (\lambda - \alpha)^m \right| \leq \left| a_n \alpha^{n-m} (\lambda - \alpha)^m \right|$$

so that the problem is bounding this last expression.

To do that, we use the concept that the region of convergence is a disk of some radius ρ; since both λ and α are in the region of convergence, there exists a radius ρ_1 such that

- The closed disk of radius ρ_1 is contained in the region of convergence, and
- We have both $|\lambda| \leq \rho_1$ and $|\alpha| \leq \rho_1$.

Then we have:

- $|\alpha|^{n-m} \leq \rho_1^{n-m}$ by construction, and
- $|\lambda - \alpha|^m \leq \max\{|\lambda|, |\alpha|\}^m \leq \rho_1^m$ by the non-Archimedean property.

Going back to the terms we want to estimate, we get

$|\beta_{nm}| \leq |a_n \alpha^{n-m} (\lambda - \alpha)^m| \leq |a_n| \rho_1^n$, which is independent of m and tends to zero as $n \to \infty$.

This means that given any $\varepsilon > 0$ there exists an N for which $|\beta_{nm}| < \varepsilon$ if $n \geq N$ and for any m. This shows that β_{nm} tends to zero uniformly in m.

The other condition: if m>n, we have $\beta_{nm} = 0$, hence it's certainly true that for every n we have $\beta_{nm} \to 0$ when $m \to \infty$.

Thus, the conditions in Proposition 8.3 are satisfied, and we can reverse the order of summation. Changing the order of summation in the expression for $f(\lambda)$ gives the expression for $g(\lambda)$, so that applying Proposition 8.3 allows us to conclude that $g(\lambda)$ converges and is equal to $f(\lambda)$. This shows that g converges whenever f does, and in that case their values are equal.

Proposition 9.5 Let f(X) and g(X) be formal power series, and suppose there is a non-stationary sequence $x_m \in \mathbb{Q}_p$ converging to zero in $\mathbb{Q}_p$ and such that $f(x_m) = g(x_m)$ for every m. Then f(X) = g(X), i.e., f(X) and g(X) have the same coefficients.

Proof:

Replacing the sequence (x_m) by a subsequence if necessary, we can assume $x_m \neq 0$ for all m. If we consider the difference $h(X) = f(X) - g(X) = \sum a_n Xn$, then we have $h(x_m) = 0$ for every m, and we want to show that $a_n = 0$ for every n. Let us assume this to be false and then let r be the least index for which $ar \neq 0$, so that

$$\begin{aligned} h(X) &= a_r X^r + a_{r+1} X^{r+1} + a_{r+2} X^{r+2} \dots \\ &= X^r (a_r + a_{r+1} X + a_{r+2} X^2 + \cdots) \\ &= X^r h_1(X), \end{aligned}$$

where $h_1(0) = a_r \neq 0$. Since h1 is a function defined by a power series, it is continuous, so $h_1(x_m) \to a_r$ as $m \to \infty$ (our assumption is that $x_m \to 0$); in particular, $h_1(x_m)$ is non-zero for large enough m.

Since we know $x_m \neq 0$, it follows that $h(x_m) = x_m^r h_1(x_m)$ is non-zero for large enough m, which is a contradiction.

Proposition 9.6 Let $f(X) = \sum a_n X^n$ be a power series with non-zero radius of convergence and let f’(X) be its formal derivative. Let $x \in Q_p$. If f(x) converges, then so does f’(x), and we have

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

Proof:

Let ρ be the radius of convergence.

If $x = 0$, any h with $|h| < \rho$ works;

If $x \neq 0$, then any h with $|h| < |x|$ works. (If $|h| < |x|$, then $|x + h| = |x|$.)

Suppose, then, that f ’(x) converges, which is equivalent to saying that $a_n x^n \to 0$.

If $x = 0$ then it is clear that f(x) converges.

If $x \neq 0$, notice that since the absolute value of an integer is at most 1, as $n \to \infty$ we have

$$|na_n x^{n-1}| \leq |a_n x^{n-1}| = \frac{1}{|x|} |a_n x^n| \to 0,$$

and again we see that f ‘(x) converges.

f(x) either converges in the closed ball $B^{\sim}(0, \rho)$ or in the open ball $B(0, \rho)$.

In the first case, set $\rho_1 = \rho$.

In the second case, choose ρ_1 such that $|x| \leq \rho_1 < \rho$. The point is that in either case the series will converge when $|x| \leq \rho_1$

Since we only care about h close to zero, we may assume, if $x \neq 0$, that $|h| < |x| \leq \rho_1$.

Otherwise, $x = 0$ and we can simply assume $|h| \leq \rho_1$.

Now,

$$f(x+h)=\sum_{n=0}^{\infty}a_n(x+h)^n=\sum_{n=0}^{\infty}a_n\sum_{m=0}^{n}\binom{n}{m}x^{n-m}h^m.$$

Subtracting f(x) and dividing by h, we get

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

Taking the limit as h → 0 on both sides; On the left we will get f ‘(x). On the right, the question is whether we can take the limit of a sum by computing the sum of the limits. Since we have $|x| \leq \rho_1$ and $|h| \leq \rho_1$, we have

$$\left|a_n\binom{n}{m}x^{n-m}h^{m-1}\right|\leq|a_n|\rho_1^{n-1},$$

and the series converges when $|x| = \rho_1$ we have $|a_n|\rho_1^n \to 0$.

Given $\varepsilon > 0$, we can find an M so that $m \geq M$ implies $|a_n|\rho_1^{n-1} < \varepsilon$, and this implies that for our fixed $|x| \leq \rho_1$ and all $|h| \leq \rho_1$ we have

$$\left|a_n\binom{n}{m}x^{n-m}h^{m-1}\right|\leq|a_n|\rho_1^{n-1}<\varepsilon$$

for all n. In other words, the inner terms tend to zero uniformly in h. This implies that we can take the limit term-by-term. In the case of the inner terms, that amounts to setting h = 0 in the polynomial

$$\sum_{m=1}^{n}a_n\binom{n}{m}x^{n-m}h^{m-1}=na_nx^{n-1}+\binom{n}{2}a_nx^{n-2}h+\cdots$$

which gives na_nx^{n-1}. And thus,

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

Corollary 9.7 Suppose f(X) and g(X) are power series, and suppose that both series converge for $|x| < \rho$. If f’(x) = g’(x) for all $|x| < \rho$, then there exists a constant $c \in Q_p$ such that f(X) = g(X) + c as power series. In particular, f(X) and g(X) have the same disk of convergence, and we have f(x) = g(x) + c for all x in the disk of convergence.

Proof:

Let $f(X) = \sum a_n X^n$, $g(X) = \sum b_n X^n$, and let $f'(X)$ and $g'(X)$ be the formal derivatives. We know that whenever $|x| < \rho$ we have

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

By Proposition 9.5, we can conclude that $a_n = b_n$ for all $n \geq 1$, and the conclusion follows

----

Section 10: Strassman's Theorem

Theorem 10.1 (Strassman) Let

$$f(X) = \sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \cdots$$

be a non-zero power series with coefficients in Qp, and suppose that we have $\lim_{n\to\infty} a_n = 0$, so that f(x) converges for all x ∈ Zp. Let N be the integer defined by the two conditions

$|a_N| = \max_n |a_n|$ and $|a_n| < |a_N|$ for n > N.

Then the function $f : Z_p \to Q_p$ defined by $x \to f(x)$ has at most N zeros.

Proof: We use induction on N.

a) If N = 0, we must have $|a_0| > |a_n|$ for all $n \geq 1$, and what we want to prove is that in that case there are no zeros: $f(x) \neq 0$ for all $x \in Z_p$.

Indeed, if we had $f(x) = 0$, then $0 = f(x) = a_0 + a_1x + a_2x^2 + \cdots$, from which it would follow that $|a_0| = |a_1x + a_2x^2 + \cdots|$

$\leq \max_{n\geq 1}|a_nx^n|$

$\leq \max_{n\geq 1} |a_n|$.

But this contradicts the assumption that $|a_0| > |a_n|$ for all $n \geq 1$.

b) To handle the induction step, we use an idea from the algebra of polynomials: a zero implies a factorization. Suppose that $|a_N| = \max_n|a_n|$ and $|a_n| < |a_N|$ for n>N, and suppose that $f(\alpha) = 0$ for some $\alpha \in Z_p$. We choose any $x \in Z_p$. Then we have

$$f(x) = f(x) - f(\alpha) = \sum_{n\geq 1} a_n(x^n - \alpha^n)$$

$$= (x-\alpha)\sum_{n\geq 1}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}.$$

$$f(x) = (x-\alpha)\sum_{j=0}^{\infty} b_j x^j = (x-\alpha)g(x),$$

Where

$$b_j = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k.$$

We can see that $b_j \rightarrow 0$ as $j \rightarrow \infty$.

It's also clear that if they were all zero then f(X) would be the zero power series, contradicting one of our assumptions.

So g(X) satisfies the assumptions of the theorem.

To use the induction hypothesis we need to find the last $|b_j|$ with maximum absolute value.

First, we note that

$$|b_j| \leq \max_{k\geq 0} |a_{j+1+k}| \leq |a_N|$$

for every j, so all the |bj | are bounded by $|a_N|$.

On the other hand, since $|\alpha| \leq 1$, for any $i \geq$ we have $|a_N + i\alpha^i| \leq |a_{N+i}| < |a_N|$, so the ultrametric inequality gives

$$|b_{N-1}| = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \cdots| = |a_N|.$$

.

Finally, if $j \geq N$,

$$|b_j| \leq \max_{k\geq 0} |a_{j+k+1}| \leq \max_{j\geq N+1} |a_j| < |a_N|.$$

This shows that the number of roots of g(X) is N − 1. By induction, we can assume that g(X) has at most N − 1 zeros in Z_p, which implies that f(X) has at most N zeros (those of g(X), plus α). This proves the theorem.

Corollary 10.2 Let f(X) =∑anXn be a non-zero power series which converges on pmZp, for some m ∈ Z. Then f(X) has a finite number of zeros in pmZp.

Proof:

$g(X) = f(p^mX) = \sum a_n p^{mn} X^n$.

Since f(X) converges in p^mZp, g(x) converges for x ∈ Z_p, and applying Strassman's theorem to g(X) gives the finiteness.

Corollary 10.3 Let $f(X) = \sum a_n X^n$ be a p-adic power series which converges in some disk p^mZ_p. If the function p^mZ_p → Qp defined by x → f(x) is periodic, that is, if there exists π ∈ p^mZ_p such that f(x+π) = f(x) for all x ∈ p^mZ_p, then f(X) is constant.

Proof:

The series f(X)−f(0) has zeros at nπ for all n ∈ Z. Since π ∈ p^mZ_p, it implies nπ ∈ p^mZ_p, this gives infinitely many zeros, and hence the series f(X) − f(0) must be identically zero, i.e., f(X) must be constant.

Conclusion

This project on ‘The Introduction to p-adic numbers’ has been a culmination of 3 courses – Algebra -1, ERA, and Number Theory which I had studied in my 2nd year in college and added another dimension to it. *p*-adic numbers have come to play a central role in modern number theory. Their importance comes from the fact that they afford a natural and powerful language for talking about congruences between integers, and allow the use of methods borrowed from algebra and real analysis for studying such problems. One of the most interesting concepts that I learnt was one of non-Archimedean Valued Fields which seemed like a totally foreign concept, but I have since come to understand them a little. The best thing about this project course has been how it has integrated my previously learnt concepts little by little which has helped me reinforce the topic of p-adic numbers, as well as see the older topics in a new light.

Topics like Rings, Homomorphism, Isomorphism from Algebra -1, Metric Spaces from Elementary Real Analysis, Congruences from Number Theory, Hausdorff Spaces and Homeomorphisms from Topology as well as Newton Raphson Method from Numerical Analysis were all used during this project and have made this an enjoyable experience.

References/ Bibliography

1. Fernando Q. Gouvea, Introduction to p-adic numbers, Universitext, Springer-Verlag, Berlin, third edition, 2010
2. Svetlana Katok, P-adic Analysis compared with real, American Mathematical Society, Mathematics Advanced Study Semester,2007
3. P-adic numbers – Wikipedia
4. https://www.youtube.com/watch?v=jOFFqAwkePw; Video titled: Theorem of Ostrowski by Harpreet Bedi, published May 21,2016,
5. https://www.youtube.com/watch?reload=9&v=gsg1x6mxVIA; Video titles: Hensel's Lemma and P-adic numbers by Harpreet Bedi, published May 21, 2016