Research Lab 2023

Achyut Bharadwaj, Lex Harie Pisco, Krittika Garg, Swayam Chaulagain
Counsellor: Sanskar Agrawal
Mentor: Nischay Reddy

May 2023

1 Formal Power Series

1.1 The Ring $R[[x]]$

Prove that $R[[x]]$ is a ring under the natural operations of addition and multiplication.

Addition : Let $f, g \in R[[x]]$ such that $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b^j x^j$. Then $f(x) + g(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{j=0}^{\infty} b^j x^j = \sum_{i,j=0}^{\infty} (a_i + b_j) x^i$. Since $a_i + b_j$ is closed under addition as $a_i$and $b_j \in R$ we can say, $R[[x]]$ is a ring under addition.

Multiplication : For proving the multiplication, we need to prove the commutative property in a formal power series. Let $f, g \in R[[x]]$ such that $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{j=0}^{\infty} b^j x^j$. Then

$$f(x)g(x) = \sum_{i=0}^{\infty} a_i x^i \times \sum_{j=0}^{\infty} b^j x^j = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

Since the sum $\sum_{i=0}^{k} a_i b_{k-i}$ is a sum of products of elements of R, the sum itself is in R since R is closed under addition and multiplication. Therefore, the above sum is a power series in R, that is the products $fg \in R[[x]]$.

Now, since the ring is commutative over both $+$ and $\cdot$, it follows that $R[[x]]$ is also commutative. Moreover, it is clearly associative over $+$ since the ring R is itself associative over $+$. Next, the ring has a zero element, i.e. $0 \in R[[x]]$ since for any $f \in R[[x]]$, we have $f + 0 = f$. Similarly, it also has an identity element, i.e. 1. Also, the additive inverse of f is the power series with the coefficients each being the additive inverse of the coefficients of f. Thus, every element of $R[[x]]$ has an inverse element. Distributivity can also be easily seen from the fact that R is itself distributive.

We will now prove associativity over multiplication. Let

$$a = \sum_{i=0}^{\infty} a_i x^i, b = \sum_{i=0}^{\infty} b_i x^i, c = \sum_{i=0}^{\infty} c_i x_i$$

Now,

$$ab = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k = \sum_{i=0}^{\infty} p_i x^i$$

So,

$$(ab)c = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} p_i c_{k-i} \right) x^k = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) c_{k-i} \right) x^k$$

The above can be expanded as

$$\sum_{k=0}^{\infty} (c_0 a_0 b_0 + c_1 (a_0 b_1 + a_1 b_0) + \cdots c_k (a_0 b_k + \cdots a_k b_0) x^k$$

Now, $a(bc) = (bc)a$ by commutativity. Therefore, we may use a similar approach as above to show that

$$a(bc) = \sum_{k=0}^{\infty} (a_0b_0c_0 + a_1(b_0c_1 + b_1c_0) + \cdots + a_k(b_0c_k + \cdots b_kc_0))x^k$$

By rearranging the terms above, we get

$$a(bc) = \sum_{k=0}^{\infty} (c_0a_0b_0 + c_0(a_0b_1 + a_1b_0) + \cdots + c_k(a_0b_k + \cdots a_kb_0))x^k = (ab)c$$

This proves associativity over multiplication.

1.2 Units in $R[[x]]$

Definition 1. *$f(x) \in R[[x]]$ then $f(0) = a_0$*

Definition 2. *Units in $R[[x]]$ are all f and g in $R[[x]]$ such that $[f \cdot g](x) = 1$.*

Examples of these units are:

(a) $f(x) = -(x-1)$

(b) $f(x) = \sum_{i=0}^{\infty} x^i$

(c) $f(x) = 1 + \sum_{i=1}^{n} a_i x^i$ for $a_i \in R$

(d) $f(x) = (\pm(x-1) \cdot \sum_{i=0}^{\infty} x^i)^n$ for $n \in \mathbb{N}$

Proposition 1. *If $f(x) \in R[[x]]$ and $f(0) = 1$, then $f(x)$ is a unit in $R[[x]]$.*

Proof. Let $f(x), g(x)$ be in $R[[x]]$ such that $f \cdot g = 1$. We need to prove that such a power series g exists if and only if we have $f(0) = 1$. Let $f(x) = a_0 + a_1x + \cdots$ and $g(x) = b_0 + b_1x + \cdots$. Thus, proving the existence of g is equivalent to proving that there exists a sequence $\{b_i\}$ such that $(a_0 + a_1x + \cdots)(b_0 + b_1x + \cdots) = 1$. Expanding this product, and combining the terms of equal degree, we get:

$$a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_0b_n + \cdots + a_nb_0)x^n + \cdots = 1$$

Since the RHS is simply 1, we need all terms $(a_0b_n + \cdots a_nb_0) = 0$ for all $n \geqslant 1$ and $a_0b_0 = 1$.

Now, if $f(0) = a_0$ is not a unit, then we cannot find a b_0 in R such that $a_0b_0 = 1$. This shows that we cannot find the desired sequence $\{b_i\}$. Thus, if $f(x)$ is a unit in $R[x]$, it follows that $f(0)$ is a unit.

We now prove the converse. That is, if $f(0)$ is a unit in R, then there exists some sequence $\{b_i\}$ so that $g(x) = \sum_{i \geqslant 0} b_i x^i$ and $f(x)g(x) = 1$. We use induction in order to do so. We will first prove that there exists some sequence $\{b_i\}_{i=0}$ (i.e. a single term b_0) so that $a_0b_0 = 1$. This finishes our base case. Now, assume that there exists some sequence $\{b_i\}_{i=0}^{n}$ so that $a_0b_0 = 1$ and for all $0 < k \leqslant n$ we have $(a_0b_k + \cdots a_kb_0) = 0$. We prove that there exists a sequence $\{b_i\}_{i=0}^{n+1}$ so that the same holds for $k = n+1$ as well. We have $a_{n+1}b_0 + \cdots a_0b_{n+1} = 0$. Therefore, we have

$$b_{n+1} = -\frac{a_{n+1}b_0 + \cdots + a_1b_n}{a_0}$$

Since we know b_i exist for all i less than or equal to n, we have that b_{n+1} also exists, completing our inductive step. Thus, if $f(0)$ is a unit, then $f(x)$ has an inverse.

□

1.3 Compositions of formal power series

We will now generalize as to when $f(g(x))$ where $g(x) \in R[[x]]$ is an element of $R[[x]]$ itself.

Proposition 2. *Let $f, g \in R[[x]]$. Then, $f(g(x)) \in R[[x]]$ if and only if $g(0) = 0$.*

Proof. Suppose $g(0) = 0$. Then, we can write $g(x) = x^k + h(x)$ where k is the smallest power of x in $g(x)$, and $k \neq 0$ since $g(0) = 0$. Moreover, the smallest power of x in $h(x)$ is more than k. Also, let

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

Therefore,

$$f(g(x)) = a_0 + a_1 g(x) + a_2 g(x)^2 + \cdots = a_0 + a_1(x^k + h(x)) + a_2(x^k + h(x))^2 + \cdots$$

Also let

$$f(g(x)) = c_0 + c_1 x + c_2 x^2 + \cdots$$

In order to prove that $f(g(x)) \in R[[x]]$ it suffices to prove that $c_n \in R$ for all n. So, we will work on finding the coefficient of the x^n term, i.e. c_n.

Consider the term $a_{n+1}(x^k + h(x))^{n+1}$ in the expansion for $f(g(x))$. The term with the lowest power in this expansion is $x^{(n+1)k}$. Since $k \neq 0$, it follows that $(n+1)k > n$. Therefore, the coefficient c_n of x^n is independent of a_{n+1}. By a similar argument, c_n is independent of a_j for all $j > n$. In other words, it follows that

$$c_n = \sum_{i=0}^{n} a_i t_i$$

where $t_i \in R$. Note that there will be no powers of a_i in the expansion since the coefficients a_i are not raised to a power in the expansion of $f(g(x))$. Since $a_i, t_i \in R$, it follows that $a_i t_i \in R$. Thus, $\sum_{i=0}^{n} a_i t_i \in R$. Therefore, for all n, we have $c_n \in R$, where

$$f(g(x)) = c_0 + c_1 x + \cdots$$

Therefore, by definition of a formal power series, $f(g(x)) \in R[[x]]$.

Now, suppose $g(0) = c \neq 0$. Let $g(x) = c + h(x)$. Then,

$$f(g(x)) = a_0 + a_1(c + h(x)) + a_2(c + h(x))^2 + \cdots = c_0 + c_1 x + \cdots$$

In the nth term of the above expansion, we have a constant c^n. Since there are infinitely many terms in the expansion, c_0 is an infinite sum, which is not defined in R. Therefore, $c_0 \notin R$. It follows that $f(g(x)) \notin R[[x]]$. □

1.4 Multivariate Power Series

We can define the system $R[[x, y]]$ to $(R[[x]])[[y]]$. Inductively, we may define

$$R[[x_1, \ldots, x_k]] = (R[[x_1, \ldots, x_{k-1}]])[[x_k]]$$

Since R is a ring implies $R[[x]]$ is a ring (base case) Then, we assume that $R[[x_1, x_2, x_3, ...x_k]]$ is a ring Now, $R[[x_1, x_2, X_3, ...x_k + 1]]$ is $(R[[x_1, x_2, x_3, ...x_k]])[[x_k + 1]]$ which is a ring (inductive case). Thus, by induction we can say that $R[[x_1, x_2, X_3, ...x_n + 1]]$ is a ring.

We will now generalize to for which power series $g \in R[[x, y]]$ can we define $f(g(x, y))$ for any $f \in R[[t]]$?

Proposition 3. *For $f, g \in \mathbb{R}[[x, y]]$, we have that $f(g(x, y))$ is defined in $R[[x, y]]$ if and only if $g(0, 0) \neq 0$.*

Proof. Suppose $g(0, 0) = 0$. Thus, the smallest power of x and y can be represented as $b_{mn}x^m y^n$ where both m and n are not 0 at the same time. So, we let $g(x, y) = b_{mn}x^m y^n + h(x, y)$. Thus,

$$\begin{aligned} f(g(x, y)) = f(b_{mn}x^m y^n + h(x, y)) &= a_0 + a_1(b_{mn}x^m y^n + h(x, y)) + a_2(b_{mn}x^m y^n + h(x, y))^2 + \cdots \\ &= c_{00} + c_{10}x + c_{01}y + \cdots \end{aligned}$$

Now, consider the coefficient, c_{pq}. We know that the term

$$a_{p+q+1}(b_{mn}x^m + y^n + h(x, y)^{p+q+1})$$

has smallest power $x^{m(p+q+1)}y^{n(p+q+1)}$ which is clearly greater than the power of x^py^q. Hence, c_{pq} is independent of a_k for all $k > p+q$. Therefore, we have that

$$c_{pq} = \sum_{i=0}^{p+q} a_i d_i$$

which is clearly an element of R. Therefore, $f(g(x,y))$ makes sense in $R[[x,y]]$.

Now, if $g(0,0) = c$ which is a constant, then let $g(x,y) = c + h(x,y)$. Therefore, we have

$$f(g(x,y)) = a_0 + a_1(c + h(x,y)) + a_2(c + h(x,y))^2 + \cdots$$

The constant term of the above expansion will be $a_0 + a_1c + a_2c^2 + \cdots$ which is an infinite sum. This does not make sense in R since we can only compute finite sums in R. Therefore, if $c \neq 0$, then there is no way to make sense of $f(g(x,y))$ as an element of $R[[x,y]]$. □

1.5 Polynomial Fields and Rational Functions

For some field k, we write $k[x]$ to denote the set of polynomials with coefficients in k. We write $k(x)$ to denote the set

$$\left\{ \frac{g(x)}{h(x)} \middle| g(x), h(x) \in R[[x]] \right\}$$

We will now explore the relation between $k(x), k[x]$ and $k[[x]]$. Firstly, note that $k[x] \in k(x)$ by letting $g(x) = 1$. Also, clearly $k[x] \in k[[x]]$. This is because a polynomial is a formal power series with the coefficients equal to 0 for all x^n where n is greater than the degree of the polynomial. We now check when an element of $k(x)$ can be written as a formal power series. Consider an example of the power series expansion of a rational function $g(x)/h(x)$, $t(x)$. Let

$g(x) = 2x + 1$ and $h(x) = x^1 + 1$. Then,

$$\frac{g(x)}{h(x)} = \frac{2x+1}{x^2+1} = 1 + x + 2x - x^3 - 2x^4 + x^5 + 2x^6 - \cdots$$

Notice how the terms of the power series are recursive. The nth term of $t(x)$ can be found in terms of the previous terms of $t(x)$. In fact, this holds in general too!

Proposition 4. *We claim that a rational function $g(x)/h(x)$, i.e. an element of $k(x)$ with $h(0) \neq 0$ can be written as a power series $t(x)$.*

Proof. If $h(0) \neq 0$, then we have already proved that $h(x)$ is a unit. Thus, $1/h(x) \in R[[x]]$. So, since formal power series are closed under multiplication, $g(x).(1/h(x)) \in R[[x]]$. Thus, $g(x)/h(x)$ can be written as a power series $t(x)$. If $h(0) = 0$, then $h(x)$ is not a unit which implies $1/h(x) \notin R[[x]]$ and thus, $g(x)/h(x)$ cant be expressed as a formal power series. □

Proposition 5. *Let $t(x) = g(x)/h(x)$ be the power series expansion of a rational function. Then, the terms a_n of $t(x)$ satisfy a linear recursion. Formally, this means that there exists a number $m \geqslant 1$ and constants $c_1, \ldots, c_m \in k$ such that for all n that is sufficiently large,*

$$a_n = \sum_{i=1}^{m} c_i a_{n-i}$$

Proof. Firstly, let the degree of $h(x)$ be m and the degree of $g(x)$ be k. Let $h(x) = b_0 + b_1x + \cdots b_mx^m$ and $t(x) = a_0 + a_1x + \cdots$. Now, since $t(x) = g(x)/h(x)$, we may write $g(x) = t(x)h(x)$.

Since the degree of $g(x)$ is k, it follows that the coefficients of x^n in the expansion of the product on the RHS is 0 for all n that is greater than k.

Now, consider some $n > \max(m,k)$. Clearly, $n > k$. Therefore, the coefficient of x^n in the expansion will be 0. Let us find the coefficient using the fact that $t(x) = a_0 + a_1x + \cdots$ and $h(x) = b_0 + b_1x + \cdots + b_mx^m$. This will be

$$a_nb_0 + a_{n-1}b_1 + \cdots + a_{n-m}b_m$$

Since $n > k$, the above must be 0. Rearranging the terms, we get

$$a_n b_0 = -(a_{n-1}b_1 + \cdots a_{n-m}b_m)$$

Since k is a field and $b_0 = h(0) \neq 0$, we have

$$a_n = -b_0^{-1}\left(a_{n-1}b_1 + \cdots a_{n-m}b_m\right) = \sum_{i=1}^{m} c_i a_{n-i}$$

where $c_i = -b_0^{-1}b_i$. This proves that the coefficients of the power series $t(x)$ satisfy a linear recursion. □

Proposition 6. *The converse of the previous lemma also holds true. That is, if $t(x) = \sum_{n\geqslant} a_n x^n \in k[[x]]$ is such that the coefficients a_n satisfy a linear recursion, then there exists some rational function $g(x)/h(x)$ which has a power series expansion of $t(x)$.*

Proof. We know that for $t(x)$, we have

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots c_m a_{n-m}$$

for n that is sufficiently large enough, since we are given that the coefficients of t satisfy a linear recursion. Therefore, we have

$$a_n - c_1 a_{n-1} - \cdots - c_m a_{n-m} = 0$$

Let $b_0 = 1$ and $b_i = -c_i$ when $i \geqslant 1$. Therefore, we may write

$$a_n b_0 + a_{n-1}b_1 + \cdots a_{n-m}b_m = 0$$

Now, consider $h(x) = b_0 + b_1 x + \cdots b_m x^m$. Consider the product $t(x)h(x)$. The coefficient of x^n in this product will be

$$b_0 a_n + b_1 a_{n-1} + \cdots b_m a_{n-m}$$

which is 0 by our assumption. Therefore, all terms of $t(x)h(x)$ have a coefficient of 0 for n sufficiently large. Suppose for all $n > k$ we have that the coefficient of x^k is 0 (and not 0 for n not more than k). Therefore, $t(x)h(x) = g(x)$ is a polynomial of degree k. Therefore, $g(x)/h(x)$ is a rational function that is represented by $t(x)$. Therefore, we have found some rational function that is represented by $t(x)$ given that the coefficients of $t(x)$ satisfy a linear recursion. This completes our proof. □

2 The p-adic numbers

The p-adic numbers are defined as follows:

Definition 3. *The set of p-adic numbers $\mathbb{Z}_p$ is defined as:*

$$\mathbb{Z}_p = \{(a_1, a_2, \dots) \mid a_i \in \mathbb{Z}/p^i\mathbb{Z} \text{ and } a_{i+1} \equiv a_i \pmod{p^i}\}$$

One can prove that the set of p-adic numbers, $\mathbb{Z}_p$ forms a ring under term-wise addition and multiplication.

Proposition 7. *The ring $\mathbb{Z}_p$ is an integral domain, i.e., if for some $a, b \in \mathbb{Z}_p$ we have $ab = 0$, then either $a = 0$ or $b = 0$.*

Proof. In $\mathbb{Z}_p$, we have $0 = (0, 0, \dots)$. Thus, we need to prove that either $a = (0, 0, \dots)$ or $b = (0, 0, \dots)$ given that $ab = (0, 0, \dots)$. First, let $a = (a_1, a_2, \dots)$ and $b = (b_1, b_2, \dots)$. Then,

$$ab = (a_1 b_1, a_2 b_2, \dots) = (0, 0, \dots)$$

This implies that we must have $a_i b_i \equiv 0 \pmod{p^i}$ for all i. Clearly, we must also have $a_1 b_1 \equiv 0 \pmod{p}$. Since $\mathbb{Z}_p$ is an integral domain, we must have $a_1 \equiv 0 \pmod{p}$ or $b_1 \equiv 0 \pmod{p}$. Assume without loss of generality that $a_1 \equiv 0 \pmod{p}$. We will prove that either $a_i = 0$ for all i or $b_i = 0$ for all i.

We will prove this by contradiction. Suppose that $a_i \neq 0$ and $b_i \neq 0$. Then, there exists some a_k such that $a_k \equiv 0 \pmod{p^k}$. Also assume without loss of generality that $b_i \neq 0$ for some $i \leqslant k$ (if the smallest such i is greater than k, then we just exchange a and b). If $a_k \equiv 0 \pmod{p^k}$, then by the

definition of a p-adic number, we must have $a_{k+1} \equiv a_k \not\equiv 0 \pmod{p^k}$. Thus, $a_{k+1} \neq 0$. It follows that for any $i \geqslant k$, we must have $a_i \neq 0$ as well as $b_i \neq 0$.

Now, since $ab = 0$, we must have $a_i b_i \equiv 0 \pmod{p^i}$ for all $i \geqslant k$. Now, we have $a_{k-1} \equiv 0 \pmod{p^{k-1}}$ but $a_k \equiv 0 \pmod{p^k}$. Moreover, by definition, we have $a_k \equiv a_{k-1} \pmod{p^{k-1}}$. Therefore, it follows that

$$a_k \equiv p^{k-1} m_1 \pmod{p^k}$$

where $0 < m_1 < p$. Next, we have

$$a_{k+1} \equiv p^k m_0 + p^{k-1} m_1 \pmod{p^{k+1}}$$

where $0 < m_0 < p$. In general, we therefore have

$$a_{k+i} \equiv p^{k+i-1} m_{i-1} + \cdots + p^k m_0 \pmod{p^{k+i}}$$

Let us say the smallest value of i for which $b_i \neq 0$ is $i = r$. We assumed earlier (WLOG) that $r < k$. Now, just as before, we may write:

$$b_{r+j} \equiv p^{r+j-1} n_{j-1} + \cdots + p^r n_0 \pmod{p^{r+j}}$$

Since $k > r$, let $k = r + l$ where l is some natural number. Also, let $i = r - k + j$. Therefore,

$$b_{r+j} = b_{k+i} \equiv p^{k+i-1} n_{j-1} + \cdots + p^r n_0 \pmod{p^{k+i}}$$

Now, $v_p(a_{k+i} b_{k+i}) = v_p(a_{k+i}) + v_p(b_{k+i})$. Since the smallest power of p in the expansion of a_{k+i} is k. Therefore, we have $v_p(a_{k+i}) = k$. Since the smallest power of p in the expansion of b_{k+i} is r, we have that $v_p(b_{k+i}) = r < k$. Thus, $v_p(a_{k+i} b_{k+i}) = kr \leqslant k^2$. Now, consider the case when $i = k^2 - k + 1$. We therefore have $v_p(a_{k^+1} b_{k^2+1}) \leqslant k^2$. This implies that

$$a_{k^2+1} b_{k^2+1} \not\equiv 0 \pmod{p^{k^2+1}}$$

However, since $ab = 0$, we must have $a_{k^2+1} b_{k^2+1} \equiv 0 \pmod{p^{k^2+1}}$. A contradiction. Thus, we cannot have both $a \neq 0$ as well as $b \neq 0$. □

Let us explore what the units in $\mathbb{Z}_p$ are. We first take an example. Consider $\mathbb{Z}_3$. Consider $a = (1, 4, 13, 40, \dots) \in \mathbb{Z}_p$. Also, let $b = (1, 7, 25, 79, \dots)$. Clearly, b also is an element of $\mathbb{Z}_p$. Moreover,

$$ab = (1 \cdot 1, 4 \cdot 7, 13 \cdot 25, 40 \cdot 79, \dots) = (1, 1, 1, 1, \dots)$$

Thus, b is the inverse of a in $\mathbb{Z}_p$. Since a has an inverse in $\mathbb{Z}_p$, it follows that a is a unit in $\mathbb{Z}_p$. Note that however, $a = (0, 3, 12, \dots)$ is not a unit in $\mathbb{Z}_p$. It seems that in general, $a \in \mathbb{Z}_p$ is a unit if and only if the first term of a is non-zero. In other words, we claim that $a \in \mathbb{Z}_p$ is a unit if and only if $a \equiv 0 \pmod{p}$.

Proposition 8. *In $\mathbb{Z}_p$, a p-adic number u is a unit if and only if $u_1 \not\equiv 0 \pmod{p}$*

Proof. Let $u = (u_1, u_2, \dots)$. Suppose $u_1 = 0$. Then, there is clearly no inverse for u since there is no $b_1 \in \mathbb{Z}/p\mathbb{Z}$ such that $u_1 b_1 \equiv 1 \pmod{p}$ (0 is not a unit modulo p). Hence, if u is a unit, then it follows that $u_1 \not\equiv 0$ or equivalently, $u \equiv 0 \pmod{p}$.

We now prove the other direction. Suppose $u \not\equiv 0 \pmod{p}$. Then, we must prove that u is a unit in $\mathbb{Z}_p$. Since p is prime, if $u \neq 0 \pmod{p}$, it means that $u_1 \not\equiv 0 \pmod{p}$. Since p is a prime, it follows that $(u_1, p) = 1$. Thus, u_1 is a unit in $\mathbb{Z}/p\mathbb{Z}$.

Now, suppose that $(u_k, p) = 1$. Now, by definition of a p-adic number, we have $u_{k+1} \equiv u_k \pmod{p^k}$. This in turn implies that $u_{k+1} \equiv u_k \pmod{p}$. Thus, $(u_{k+1}, p) = 1$. Hence, $(u_{k+1}, p^{k+1}) = 1$. Thus, u_{k+1} is a unit in $\mathbb{Z}/p^{k+1}\mathbb{Z}$.

By induction, this implies that for all k, we have u_k is a unit in $\mathbb{Z}/p^k\mathbb{Z}$. Since the multiplication operation is termwise in $\mathbb{Z}_p$, it follows that u is a unit in $\mathbb{Z}_p$. □

This leads to another important result:

Proposition 9. *Let $a \neq 0$ be a p-adic number. Then, there exists a unique pair (u, k) such that $a = p^k u$ and u is a unit.*

Proof. We will first prove existence. Let $a = (a_1, a_2, \dots)$. If $a_1 \neq 0$, then by the previous proposition, we have that a itself is a unit. Thus, $a = p^0 u$ where $u = a$.

Now, suppose that $a_k = 0$ for some k (this automatically implies that $a_1, a_2, \dots, a_k = 0$ by the construction of p-adic numbers) such that $a_{k+1} \neq 0$. Now, consider the p-adic number

$$b = (a_{k+1}/p^k, a_{k+2}/p^k, \dots)$$

We must first prove that b is indeed a p-adic integer.

For any $i > k$, by the definition of p-adics, we know that $a_i \equiv a_k \equiv 0 \pmod{p^k}$. Thus, a_i/p^k is an integer for all a_i.

Now, for some i, we have $a_{k+i+1} \equiv a_{k+i} \pmod{p^{k+i}}$ by the definition of p-adics. Thus, $a_{k+i+1} = p^i n + a_{k+i}$ where $0 < n < p$. Dividing both sides by p^k, we get

$$\frac{a_{k+i+1}}{p^k} = p^i n + \frac{a_{k+i}}{p^k}$$

Hence, taking mod p^i on both sides, we get

$$\frac{a_{k+i+1}}{p^k} \equiv \frac{a_{k+i}}{p^k} \pmod{p^i}$$

Hence, we conclude that $b \in \mathbb{Z}_p$. Now, consider the p-adic integer $p^k b$. We get

$$\begin{aligned} p^k b &= p^k(a_{k+1}/p^k, a_{k+2}/p^k, \dots, a_{k+k}/p^k, a_{k+k+1}/p^k, \dots) \\ &= (a_{k+1}, a_{k+2}, \dots, a_{k+k}, a_{k+k+1}, \dots) \end{aligned}$$

Now, $a_{i+1} \equiv a_k \pmod{p^i}$, or in general, $a_{k+i} \equiv a_i \pmod{p^i}$ by induction on k. Thus,

$$p^k b = (a_1, a_2, \dots) = a$$

Now, clearly, $a_{k+1}/p^k \not\equiv 0 \pmod{p}$ since a_{k+1} is nonzero. Thus, b is a unit. Thus, for arbitrary a, we have found a specific unit b and power k such that $a = p^k b$, which completes our proof for existence.

Now, we prove uniqueness. To do so, suppose that $a = p^{k_1} u_1 = p^{k_2} u_2$. Assume WLOG that $k_1 \geqslant k_2$. Then,

$$p^{k_1} u_1 - p^{k_2} u_2 = p^{k_2}(p^{k_1 - k_2} u_1 - u_2) = 0$$

Since $\mathbb{Z}_p$ is an integral domain, it follows that either $p^{k_2} = 0$ or $p^{k_1 - k_2} u_1 - u_2 = 0$. Since p^{k_1} is clearly not 0, it follows that

$$p^{k_1 - k_2} u_1 = u_2$$

If $k_1 > k_2$, then the first term of u_2 will be 0, which is a contradiction since u_2 is a unit. Therefore, $k_1 = k_2$. Thus, $u_2 = p^0 u_1 = u_1$. Hence, the pair (u, k) is unique. □

Now, we will explore some properties related to $\mathbb{Z}_p[x]$, i.e. polynomials with coefficients in $\mathbb{Z}_p$.

Theorem 1. *Let $f(x) \in \mathbb{Z}_p[x]$. Consider some a_1 (if there exists one) such that $f(a_1) \equiv 0 \pmod{p}$ such that $f'(a_1) \not\equiv 0 \pmod{p}$. Then, there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_1 \pmod{p}$.*

Proof. If we prove that if there exists a root, a_k to $f(x)$ in $\mathbb{Z}/p^k\mathbb{Z}$ with $f'(a_k) \neq 0$, then there exists a unique a_{k+1} such that $f(a_{k+1}) = 0$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$, it will by induction imply that there exists some unique p-adic number $a = (a_1, a_2, \dots)$ such that $f(a) = 0$ in $\mathbb{Z}_p$. However, note the condition that $a_{k+1} \equiv a_k \pmod{p^k}$. Let us first prove this result for $k = 1$.

Suppose $f(a_1) \equiv 0 \pmod{p}$ and $f'(a_1) \not\equiv 0 \pmod{p}$. We will try to find some a_2 such that $f(a_2) \equiv 0 \pmod{p^2}$ and $a_2 \equiv a_1 \pmod{p}$.

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

in $\mathbb{Z}/p\mathbb{Z}$. Then, we have $f(a_1) = c_0 + c_1a_1 + \cdots + c_na_1^n$. Consider $a_2 = a_1 + mp$ for some integer $0 < m < p$. Then, we have

$$\begin{aligned} f(a_2) = f(a_1 + mp) &= c_0 + c_1(a_1 + mp) + \cdots + c_n(a_1 + mp)^n \\ &= c_0 + c_1(a_1 + mp) + \cdots + c_n(a_1^n + na_1^{n-1}mp + \cdots + (mp)^n) \end{aligned}$$

Now, if we take mod p^2 on both sides of the above, all terms with powers of p over 2 get cancelled to 0. Thus, we get:

$$\begin{aligned} f(a_2) &\equiv c_0 + c_1(a_1 + mp) + c_2(a_1^2 + 2a_1mp) + \cdots + c_n(a_1^n + na_1^{n-1}mp) \\ &\equiv (c_0 + c_1a_1 + \cdots c_na_n) + (c_1(mp) + 2c_2(mp)a_1 + \cdots nc_n(mp)a_1^{n-1}) \\ &\equiv f(a_1) + mpf'(a_1) \pmod{p^2} \end{aligned}$$

Now, we know that $a_2 \equiv a_2 \pmod{p}$ since $a_2 = mp + a_1$. If a_2 is a root modulo p^2, it implies that $f(a_2) \equiv 0 \pmod{p^2}$. Therefore, $f(a_1) + mpf'(a_1) \equiv 0 \pmod{p^2}$. Since $f(a_1) \equiv 0 \pmod{p}$, let $f(a_1) = kp$. So, we must have $kp + mpf'(a_1) \equiv 0 \pmod{p}$. So, $m \equiv -k(f'(a_1))^{-1} \pmod{p}$. We can do this step since $f'(a_1) \not\equiv 0 \pmod{p}$. Thus, we have found a unique m such that $f(a_1 + mp) \equiv 0 \pmod{p^2}$. In other words, given a value a_1, we have proved that there exists a unique a_2 such that $f(a_2) \equiv 0 \pmod{p^2}$.

Now, suppose we are given some a_k such that $f(a_k) \equiv 0 \pmod{p^k}$. We will prove that there exists a unique a_{k+1} such that $f(a_{k+1}) \equiv 0 \pmod{p^{k+1}}$ and $a_{k+1} \equiv a_k \pmod{p^k}$.

Let $f(x) = c_0 + \cdots + c_nx^n$. Then,

$$f(a_k) \equiv c_0 + c_1a_k + \cdots c_na_n^n \equiv 0 \pmod{p^k}$$

Now, since $a_{k+1} \equiv a_k \pmod{p^k}$, we have $a_{k+1} \equiv p^km + a_k$ where $0 < m < p$. Therefore,

$$\begin{aligned} f(a_{k+1}) &= c_0 + c_1a_{k+1} + \cdots + c_na_{k+1}^n \\ &= c_0 + c_1(a_k + p^km) + \cdots + c_n(a_k + p^km)^n \\ &= c_0 + c_1(a_k + p^km) + \cdots + c_n(a_k^n + na_k^{n-1}mp + \cdots (mp)^n) \end{aligned}$$

If we take mod p^{k+1} on both sides, all terms apart from the p^k and constant terms cancel out since $2k >\geqslant k + 1$ for all positive k. Thus,

$$\begin{aligned} f(a_{k+1}) &\equiv c_0 + c_1(a_k + p^km) + c_2(a_k^2 + 2a_kp^km) + \cdots + c_n(a_k^n + na_k^{n-1}p^km) \\ &\equiv (c_0 + c_1a_k + \cdots c_na_k^n) + p^km(c_1 + 2c_2a_k + \cdots nc_na_k^{n-1}) \\ &\equiv f(a_k) + p^kmf'(a_k) \equiv 0 \pmod{p^{k+1}} \end{aligned}$$

Since $f(a_k) \equiv 0 \pmod{p^k}$, we have $f(a_k) = p^kt$. So, $p^kt + p^kmf'(a_k) \equiv 0 \pmod{p^{k+1}}$. Hence,

$$-t + mf'(a_k) \equiv 0 \pmod{p}$$

Hence, $m \equiv t(f'(a_k))^{-1} \pmod{p}$. Since $f'(a_k) \not\equiv 0 \pmod{p^k}$, its inverse exists and is unique. Thus, there exists a unique m, given as above, such that $a_{k+1} = mp^k + a_k$ is a root of $f(x)$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ and $a_{k+1} \equiv a_k \pmod{p^k}$.

We are given the value a_1 that is a root of $f(x)$ in $\mathbb{Z}/p\mathbb{Z}$. Thus, we can find the corresponding value of a_2 and hence a_3 and so on. Thus, by induction, there exists a unique sequence $a = (a_1, a_2, \dots)$ that satisfies $f(a_k) \equiv 0 \pmod{p^k}$ and $a_{k+1} \equiv a_k \pmod{p^k}$. By definition of a p-adic number, $a \in \mathbb{Z}_p$. Moreover, since $f(a_k) \equiv 0 \pmod{p^k}$ it follows that $f(a) = 0$ in $\mathbb{Z}_p$. Thus, there exists a unique p-adic number $a \in \mathbb{Z}_p$ such that $f(a) = 0$ given a_1. □

3 The p-adic Numbers $\mathbb{Q}_p$

3.1 As an Extension of $\mathbb{Z}_p$

Definition 4. *We define* $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

For example,

$$\frac{(1,4,13,\dots)}{1}+\frac{(3,3,3,\dots)}{3}+\frac{(2,5,14,\dots)}{9}\in\mathbb{Q}_3$$

Note that the above is NOT equal to

$$(1,4,13,\dots)+(1,1,1,\dots)+\left(\frac{2}{9},\frac{5}{9},\frac{13}{9},\dots\right)$$

The divided by sybmol is merely used as a notation and does not translate to the above. More generally, any element of $\mathbb{Q}_p$ is:

$$a_0+\frac{a_1}{p}+\cdots+\frac{a_k}{p^k}$$

By taking p^k as the common denominator, the above can be rewritten as:

$$\frac{a_0p^k+a_1p^{k-1}+\cdots+a_k}{p^k}=\frac{a}{p^k}$$

where $a_i, a\in\mathbb{Z}_p$. Moreover, we have that two p-adic numbers $\frac{a}{p^k}$ and $\frac{b}{p^m}$ are equal if and only if $ap^m=bp^k$.

Proposition 10. *$\mathbb{Q}_p$ is a field. Moreover, $\mathbb{Q}\in\mathbb{Q}_p$.*

Proof. Consider some p-adic number $\alpha=\frac{a}{p^k}$. We will prove that there exists some p-adic number $\beta=\frac{b}{p^m}$ such that $\alpha\beta=1$ for every $\alpha\in\mathbb{Q}_p$ that is non-zero, i.e. $a\neq 0$.

Firstly, we know that since $a\in\mathbb{Z}_p$, we have that there exists some a' that is a unit in $\mathbb{Z}_p$ and n_1 a non-negative integer so that $a=a'p^{n_1}$. Let $\beta\in\mathbb{Q}_p$ be such that

$$\beta=\frac{b}{1}=\frac{(a')^{-1}p^{k-n_1}}{1}$$

The inverse of a' exists since a' is a unit as defined. Then,

$$\alpha\beta=\frac{a'p^{n_1}}{p^k}\cdot\frac{(a')^{-1}p^{k-n_1}}{1}=\frac{p^k}{p^k}$$

Now since $a/p^k=b/p^m\iff ap^m=bp^k$, it follows that the above equals 1 if and only if $p^k=p^k$. Thus, $\alpha\beta=1$. Thus, we have found a $\beta\in\mathbb{Q}_p$ given $\alpha\in\mathbb{Q}_p\backslash\{0\}$ such that $\alpha\beta=1$. Hence, $\mathbb{Q}_p$ is a field.

We will now prove that $\mathbb{Q}\in\mathbb{Q}_p$. Consider an element of $\mathbb{Q}$, say a/b. Let $a=p^{k_1}a'$ and $b=p^{k_2}b'$ where a' and b' are co-prime with p. Thus,

$$\frac{a}{b}=p^{k_1}\frac{\frac{a'}{b'}}{p^{k_2}}$$

where $\alpha\in\mathbb{Z}_p$. Thus, any rational number is also a p-adic number. Hence $\mathbb{Q}_p$ contains $\mathbb{Q}$. □

3.2 $\mathbb{Q}_p$ as Completion of $\mathbb{Q}$

We will first define metric spaces.

Definition 5. *We call a set X along with a function (metric) $d\colon X\times X\to\mathbb{R}$, (X,d), a metric space if the following properties are satisfied for any $x,y,z\in X$:*

1. *$d(x,x)=0$*
2. *If $x\neq y$ then $d(x,y)>0$*
3. *$d(x,z)\leqslant d(x,y)+d(y,z)$*
4. *$d(x,y)=d(y,x)$*

For example, $(\mathbb{Q},|\cdot|)$ is a metric space.

Definition 6. *For a metric space (X, d), we define a Cauchy sequence of X wrt d as follows: A sequence $(x_n)_{n\geqslant 0}$ where $x_n \in X$ is called a Cauchy sequence if for all $\epsilon \in \mathbb{R}^+$, there exists some $N_\epsilon \in \mathbb{N}$ such that for all integers $m, n \geqslant N$, we have $d(x_n, x_m) < \epsilon$.*

In simple terms, any sequence that should converge under the given metric is called a Cauchy sequence. We now define what a completion with respect to a metric is.

Definition 7. *Let $S_{(X,d)}$ be the set of Cauchy sequences in X with respect to the metric d. Then, given two elements x_n, y_n of $S_{(X,d)}$, we say that x_n is equivalent to y_n iff for every real number ϵ, there exists a natural number N_ϵ such that for all integers $n \geqslant N$, we have $d(x_n, y_n) < \epsilon$. We denote this equivalence by $x_n \sim y_n$.*

Definition 8. *We define the completion of X with respect to d as the set $S_{(X,d)}/\sim$.*

In more intuitive terms, the completion of a metric space X with respect to d is the set of limits of the Cauchy sequences in X with respect to d.

As an example, $\mathbb{R}$ is a completion of $\mathbb{Q}$ with respect to the usual metric, the absolute value.

Now, we will define $\mathbb{Q}_p$ as a completion of $\mathbb{Q}$. In order to do so, we must first define the metric on $\mathbb{Q}$ that yields $\mathbb{Q}_p$.

Definition 9. *Let p be a prime and a be an integer. Then, we define $v_p(a)$ to be the largest n such that $p^n | a$ when $a \neq 0$ and to be ∞ when $a = 0$. Now, we extend this definition to $\mathbb{Q}$. Let $q = a/b \in Q$ where a and b are integers where $b \neq 0$. Then, we define $v_p(q) = v_p(a) - v_p(b)$.*

Lemma 1. *The above definition of $v_p()$ is well-defined. That is, if $a/b = c/d = q$, then we have $v_p(a/b) = v_p(c/d)$.*

Proof. Suppose $a/b = c/d$ such that $v_p(a/b) = v_p(c/d) + m$. Then, $v_p(a) - v_p(b) = v_p(c) - v_p(d) + m$. Let $a = p^{k_1}a', b = p^{k_2}b', c = p^{k_3}c', d = p^{k_4}d'$ with each of a', b', c', d' relatively prime to p. Therefore, $k_1 - k_2 k_3 - k_4 + m$. Moreover, we have $a/b = p^{k_1-k_2}a'/b'$ and $c/d = p^{k_3-k_4}c'/d'$. Since $a/b = c/d$, we have

$$p^{k_1-k_2}\frac{a'}{b'} = p^{k_3-k_4}\frac{c'}{d'}$$

We can rewrite this as

$$p^{k_1-k_2}a'd' = p^{k_3-k_4}b'c'$$

Now, we assumed that $k_1 - k_2 = k_3 - k_4 + m$. Let $k_3 - k_4 = n$. So,

$$p^{n+m}a'd' = p^n b'c'$$

which implies that $p^m a'd' = b'c'$. Taking the v_p of both sides, we have $m = 0$. Thus □

Definition 10. *We define the p-adic absolute value to be as follows. Let $q \in \mathbb{Q}$. Then, we define $|q|_p = p^{-v_p(q)}$ when $q \neq 0$ and 0 when $q = 0$.*

We will first explore some properties of $v_p(a)$ which will help us find a metric on $\mathbb{Q}$ that gives $\mathbb{Q}_p$.

Proposition 11. *For any $a, b \in \mathbb{Z}$, the following are true:*

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a + b) \geqslant \min(v_p(a), v_p(b))$
3. *If $v_p(a) \neq v_p(b)$, then $v_p(a + b) = \min(v_p(a), v_p(b))$*

Proof. Let $v_p(a) = k_1$ and $v_p(b) = k_2$. WLOG, assume that $k_1 \geqslant k_2$. Then, clearly $a = p^{k_1}a'$ and $b = p^{k_2}b'$ where $(a', p) = 1$ and $(b', p) = 1$. Then:

1. We have $ab = a'b'p^{k_1+k_2}$ where $(a'b', p) = 1$ since each of a' and b' is co-prime to p. Hence, $v_p(ab) = k_1 + k_2 = v_p(a) + v_p(b)$.

2. We have $a + b = a'p^{k_1} + b'p^{k_2}$. Since $k_1 \geqslant k_2$, we can write

$$a + b = p^{k_2}(a'p^{k_1-k_2} + b')$$

Hence,

$$v_p(a + b) = k_2 + v_p(a'p^{k_1-k_2} + b')$$

Clearly, the above is at least k_2 since $v_p(a'p^{k_1-k_2}+b') \geqslant 0$. Hence, $v_p(a+b) \geqslant k_2 = \min(v_p(a), v_p(b))$ since we assumed that $v_p(a) \leqslant v_p(b)$.

3. Since we have that $v_p(a) \neq v_p(b)$, we know $k_1 > k_2$. Thus, $a'p^{k_1-k_2} + b' \equiv 0 + b' \equiv b' \pmod{p}$. Since b' is co-prime with p, we have $a'p^{k_1-k_2} + b' \not\equiv 0 \pmod{p}$. Hence, $p \nmid (p^{k_1-k_2}a' + b')$. Thus, $v_p(a'p^{k_1-k_2} + b') = 0$. Hence, $v_p(a + b) = k_2 = v_p(b) = \min(v_p(a), v_p(b))$ since we assume that $v_p(a) \leqslant v_p(b)$.

□

Proposition 12. *The above properties all hold for any $r, s \in \mathbb{Q}$.*

Proof. Let $r = a_1/b_1$ and $s = a_2/b_2$ where a_i, b_i are integers with $b_i \neq 0$. We know by definition that $v_p(r) = v_p(a_1) - v_p(b_1)$ and similarly $v_p(s) = v_p(a_2) - v_p(b_2)$. Hence:

1. We have

$$v_p(rs) = v_p\left(\frac{a_1a_2}{b_1b_2}\right) = v_p(a_1a_2) - v_p(b_1b_2)$$

Since $a_i \in \mathbb{Z}$ we have $v_p(a_1a_2) = v_p(a_1) + v_p(a_2)$ and similarly $v_p(b_1b_2) = v_p(b_1) + v_p(b_2)$. Thus,

$$v_p(rs) = (v_p(a_1) - v_p(b_1)) + (v_p(a_2) - v_p(b_2)) = v_p(r) + v_p(s)$$

2. We can write $v_p(r + s)$ as

$$v_p\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) = v_p\left(\frac{a_1b_2 + a_2b_1}{b_1b_2}\right) = v_p(a_1b_2 + a_2b_1) - v_p(b_1b_2)$$

Now, a_1b_2 and a_2b_1 are integers. So,

$$v_p\left(a_1b_2 + a_2b_1\right) \leqslant \min(v_p(a_1b_2), v_p(a_2b_1))$$

Thus,

$$\begin{aligned} v_p(r + s) &\geqslant \min(v_p(a_1) + v_p(b_2), v_p(a_2) + v_p(b_1)) - (v_p(b_1) + v_p(b_2)) \\ &= \min(v_p(a_1) - v_p(b_1), v_p(a_2) - v_p(b_2)) = \min(v_p(r), v_p(s)) \end{aligned}$$

We can legally perform the above step since $v_p(b_1b_2)$ is a constant.

3. If $v_p(a_1b_2) = v_p(a_2b_1)$, then we have $v_p(a_1) + v_p(b_2) = v_p(a_2)v_p(b_1)$. Thus, by rearranging the terms, we have $v_p(r) = v_p(s)$. Thus, if $v_p(r) \neq v_p(s)$, it follows that $v_p(a_1b_2) \neq v_p(a_2b_1)$. Hence, $v_p(a_1b_2 + a_2b_1) = \min(v_p(a_1b_2), v_p(a_2b_1))$. It follows directly that $v_p(r + s) = \min(v_p(r), v_p(s))$.

We have thus extend all the properties that hold for integers under v_p to rationals. □

We will now use these properties to prove some properties regarding $|\cdot|_p$, which will in turn prove that $(\mathbb{Q}, |\cdot|_p)$ is a metric space.

Proposition 13. *The following properties are true regarding $|\cdot|_p$:*

1. $|q|_p \geqslant 0$ *and equality holds iff* $q = 0$
2. $|q + r|_p \leqslant \max(|q|_p, |r|_p)$
3. $|qr|_p = |q|_p |r|_p$

Proof. 1. We have $|q|_p = p^{-v_p(q)}$. Clearly this is at least 0 for all $v_p(q)$ since $v_p(q) \in \mathbb{Q}$. We have $p^{-v_p(q)} = 0$ iff $v_p(q) = \infty$ which happens only when $q = 0$.

2. We have
$$|q+r|_p = p^{-v_p(q+r)} \leqslant p^{-\min(v_p(q),v_p(r))} = p^{\max(-v_p(q)),-v_p(r)}$$
since $v_p(q+r) \geqslant \min(v_p(q), v_p(r)))$. Thus,
$$|q+r|_p \leqslant \max(|q|_p, |r|_p)$$
Clearly, equality holds when $|q|_p \neq |r|_p$, which follows from the property of v_p.

3. We have
$$|qr|_p = p^{-v_p(qr)} = p^{-v_p q - v_p(r)} = p^{-v_p(q)} p^{-v_p(r)} = |q|_p |r|_p$$

□

With these properties, we may now define a new metric on $\mathbb{Q}$. Consider the metric d_p which is defined as follows:

Definition 11. *We define the function $d_p \colon Q \times \mathbb{Q} \to \mathbb{R}$ as follows: $d_p(x,y) = |x-y|_p$.*

Proposition 14. *$\mathbb{Q}$ is a metric space over d_p.*

Proof. In order to prove this, we must prove all properties listed in the definition of a metric space.

1. $d_p(x,x) = |x-x|_p = |0|_p = 0$
2. $d_p(x,y) = |x-y|_p > 0$ when $x \neq y$ by the previous proposition.
3. $d_p(x,z) = |x-z|_p = |(x-y)+(y-z)|_p$. By property 2 above, $|(x-y)+(y-z)|_p \leqslant \max(|x-y|_p, |y-z|_p) \leqslant |x-y|_p + |y-z|_p$ since $|q|_p \geqslant 0$. Hence, $d_p(x,z) \leqslant d_p(x,y) + d_p(y,z)$.
4. $d_p(x,y) = |x-y|_p = |y-x|_p = d_p(y,x)$

Thus, $\mathbb{Q}$ is a metric space over d_p. □

We can thus finally define $\mathbb{Q}_p$ in terms of $\mathbb{Q}$ as follows:

Definition 12. *We define $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to d_p. Thus, $\mathbb{Q}_p = \{[a_n] \mid a_n \in S_p\}$ where S_p denotes the set of Cauchy sequences in $\mathbb{Q}$ with respect to d_p.*

3.3 Operations in $\mathbb{Q}_p$

Now, we know that $\mathbb{Q}$ is a field with operations $(+,\cdot)$. We will now try to find a pair of binary operations $(+,\cdot)$ on $\mathbb{Q}_p$ such that $(\mathbb{Q}_p,+,\cdot)$ is a field.

Let $\alpha \in \mathbb{Q}_p$. Therefore, we can write $\alpha = [a]$ for some $a \in S_p$ by definition of Q_p. Similarly, let $\beta = [b] \in \mathbb{Q}_p$. We define the addition of two elements in the p-adics as
$$\alpha + \beta = [a] + [b] = [a+b]$$
and their product as
$$\alpha \cdot \beta = [a] \cdot [b] = [a \cdot b]$$
However, we have not yet defined what addition and multiplication are in S_p (a and b are elements of S_p). We define the sum of two sequences $a = (a_i)$ and $b = (b_i)$ to be $a + b = (a_i + b_i)$, i.e. the termwise sum of the terms of the sequence. Similarly, we define their product to be $a \cdot b = (a_i b_i)$. Since both a and b converge, it follows that both $a+b$ as well as ab converge. Thus, S_p is closed under multiplication.

Definition 13. *Let S be the set of all Cauchy sequences of $\mathbb{Q}$, we define a set of equivalence classes in S such that*
$$S/\sim = \{[a] | a \in S\}$$
$$[a] = \{(a_i) \sim y | \exists (y_i) \in S \lim_{i\to\infty} |a_i - y_i|_p = 0\}$$

Lemma 2. *The set $S/\sim$ has a well-defined addition and multiplication*
$$[a] + [b] \sim [a+b]$$
$$[a][b] \sim [ab]$$

Proof. We need to show that, $|(a_i + b_i) - (a_i^{'} + b_i^{'})|_p = 0$. To prove this, we can observe the following,

$$|(a_i + b_i) - (a_i^{'} + b_i^{'})|_p = |a_i - a_i^{'} + b_i - b_i^{'}|_p$$

It follows that,

$$|a_i - a_i^{'} + b_i - b_i^{'}|_p \leqslant |a_i - a_i^{'}|_p + |b_i - b_i^{'}|_p$$

the RHS converges to 0 as $i \to \infty$. For multiplication, we have,

$$\begin{aligned} |a_i b_i - a_i^{'} b_i^{'}| &= |a_i b_i - a_i b_i^{'} + a_i b_i^{'} + a_i^{'} b_i^{'}| \\ |a_i(b_i - b_i^{'}) + b_i^{'}(a_i - a_i^{'})|_p &\leqslant |a_i(b_i - b_i^{'})|_p + |b_i^{'}(a_i - a_i^{'})|_p \\ |a_i(b_i - b_i^{'})|_p + |b_i^{'}(a_i - a_i^{'})|_p &= |a_i|_p|(b_i - b_i^{'})|_p + |b_i^{'}|_p|(a_i - a_i^{'})|_p \end{aligned}$$

Since (a_i) and $(b_i^{'})$ are bounded, then we can proceed:

$$|a_i|_p \lim_{i\to\infty} |(b_i - b_i^{'})|_p + |b_i^{'}|_p| \lim_{i\to\infty} (a_i - a_i^{'})|_p = \epsilon \cdot 0 + \epsilon \cdot 0 = 0$$

□

Now, we will prove that $\mathbb{Q}_p$ is a field.

Definition 14. *If λ is an element of $\mathbb{Q}_p$ and $(x_n) \in S/\sim$ is any Cauchy sequence representing λ, we define*

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

Proposition 15. *$\mathbb{Q}_p = S/\sim$ is a field*

Proof. Let $(1/x_i)$ denote the multiplicative inverse of (x_i) in $\mathbb{Q}_p$. To know that $1/x_n$ is Cauchy, observe the following

$$\left|\frac{1}{x_i} - \frac{1}{x_j}\right|_p = \left|\frac{x_j - x_i}{x_j x_i}\right|_p$$

Since (x_n) is Cauchy, we have that $(x_j - x_i)$ is bounded by ϵ. It follows that for a fix large N and for every $i, j > N$, we have that for every $\epsilon > 0$, the following holds

$$\left|\frac{1}{x_i} - \frac{1}{x_j}\right|_p < \epsilon$$

□

3.4 Sequences and Series in $\mathbb{Q}_p$

Till now, we only talked about sequences in $\mathbb{Q}$, and used them to define the system $\mathbb{Q}_p$. We will now talk about sequences in $\mathbb{Q}_p$ itself. They can be thought of as sequences of sequences, since each element of $\mathbb{Q}_p$ is itself a sequence of elements in $\mathbb{Q}$. We will now extend the p-adic absolute value to even p-adic numbers. There are two things we need to take care of here. Firstly, we only know what $|q|_p$ where q is a rational number is, not a sequence of rational numbers. So, we need to define the notion of p-adic absolute value for Cauchy sequences. Next, $[a]$ is not a single sequence. It is a set of sequences. Therefore, we need to show that for any sequence in $[a]$, the result of $|[a]|_p$ is the same. In other words, if $x \sim y$ are two sequences, then we must show that $|x|_p = |y|_p$.

Definition 15. *Let (x_n) be a Cauchy sequence. Then, the sequence $(|x_n|_p)$ converges to some real number, say $y \in \mathbb{R}$. Then, we define $|(x_n)|_p$ to be y. In other words, $|(x_n)|_p = \lim_{n\to\infty} |x_n|_p$.*

Proof. We will prove that if (x_n) is a Cauchy sequence, then $(|x_n|_p)$ converges in $\mathbb{R}$. So, we must prove that for all $\epsilon \in \mathbb{R}^+$, we have that there exists some $N_\epsilon \in \mathbb{N}$ such that for all $m, n \geqslant N_\epsilon$ we have

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

By the definition of a Cauchy sequence with respect to $|\cdot|_p$, we have that for every $\epsilon \in \mathbb{R}^+$, there exists some natural number N_ϵ such that for all $m, n \geqslant N_\epsilon$, we have $|x_n - x_m|_p < \epsilon$. Let us now keep ϵ and N_ϵ fixed. Now, consider some integers $m, n \geqslant N_\epsilon$ such that $|x_n|_p \neq |x_m|_p$. Then, we have

$$|x_n - x_m|_p = \max(|x_n|_p, |x_m|_p) < \epsilon$$

Therefore, we have $0 < |x_m|_p < |x_n|_p < \epsilon$ (WLOG). Thus, $|x_n|_p - |x_m|_p < \epsilon$. In general, $||x_n|_p - |x_m|_p| < \epsilon$.

Now, if $|x_n|_p = |x_m|_p$, this implies that $||x_n|_p - |x_m|_p| = 0 < \epsilon$ since $\epsilon \in \mathbb{R}^+$. Thus, for all $m, n \geqslant N_\epsilon$ we have $||x_m|_p - |x_n|_p| < \epsilon$. This holds true for every value of ϵ that is a positive real and its corresponding N_ϵ. Therefore, the sequence $(|x_n|_p)$ converges. □

We will now show that $|[a]|_p$ is well defined where $[a]$ is the equivalence class of a Cauchy sequence a of $\mathbb{Q}$. Recall that this is equivalent to proving that if $x_n \sim y_n$ then $|x_n|_p = |y_n|_p$.

Proposition 16. *If $(x_n), (y_n) \in S_p$ are equivalent (where equivalence is as defined before), then $|(x_n)|_p = |(y_n)|_p$. In other words,*

$$\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$$

Proof. Given that $(x_n) \sim (y_n)$, by definition, we have that for all $\epsilon \in \mathbb{R}^+$, there exists some $N_\epsilon \in \mathbb{N}$ such that for all $n \geqslant N_\epsilon$, we have $|x_n - y_n|_p < \epsilon$. In other words, if $(x_n) \sim (y_n)$, then

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

Let us assume for the sake of contradiction that $\lim_{n\to\infty} |x_n|_p \neq \lim_{n\to\infty} |y_n|_p$. Also, let us assume WLOG that $\lim_{n\to\infty} |x_n|_p > \lim_{n\to\infty} |y_n|_p$. Since $|x_n - y_n|_p = \max(|x_n|_p, |y_n|_p)$ when $|x_n|_p \neq |y_n|_p$, it follows that

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

However, we assumed that $\lim_{n\to\infty} |y_n|_p < \lim_{n\to\infty} |x_n|_p = 0$. A contradiction since the absolute value is always positive. It follows that $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$. Hence, $|(x_n)|_p = |(y_n)|_p$. □

From this, one may conclude that $|\alpha|_p$ is well defined for all $\alpha \in \mathbb{Q}_p$. Moreover, the same properties hold for $|\alpha|_p$ for $\alpha \in \mathbb{Q}_p$ as in $\mathbb{Q}$, which can be easily seen from the fact that $|(x_n)|_p = \lim_{n\to\infty} |x_n|_p$.

With the new extension of the p-adic absolute value in the p-adic numbers, we may now extend the notion of convergence to $\mathbb{Q}_p$ as well.

Definition 16. *Consider a sequence (x_n) where $x_n \in \mathbb{Q}_p$. We say that (x_n) converges to a limit $L \in \mathbb{Q}_p$, iff for all $\epsilon \in \mathbb{R}^+$, there is some natural number N_ϵ such that for all $n \geqslant N_\epsilon$ we have $|x_n - L|_p < \epsilon$. Note that here, each x_k is itself a p-adic number. So, (x_n) is essentially a sequence of sequences of rationals.*

We now give the condition of convergence for a sequence in $\mathbb{Q}_p$.

Definition 17. *A sequence (a_n) converges iff there exists an element of $\mathbb{Q}_p$ that it converges to.*

Proposition 17. *In $\mathbb{Q}_p$, a sequence (x_n) converges then $(|x_n|_p)$ converges in $\mathbb{R}$. Moreover, $\lim_{n\to\infty} |x_n|_p = |\lim_{n\to\infty} x_n|_p$*

Proof. Suppose (x_n) converges to $L \in \mathbb{Q}_p$. Then, by definition, we have that

$$\forall \epsilon \in \mathbb{R}^+ \exists N_\epsilon \in \mathbb{N} \text{ st } \forall n \geqslant N_\epsilon, |x_n - L|_p < \epsilon$$

Now, $|x_n - L|_p = \max(|x_n|_p, |L|_p) < \epsilon$ if $|x_n|_p \neq |L|_p$. Therefore, we have $0 \leqslant |x_n|_p < \epsilon$ and $0 \leqslant |L|_p < \epsilon$ for all real numbers $\epsilon > 0$. Thus, we have $||x_n|_p - |L|_p| < \epsilon$. If $|x_n|_p = |L|_p$ the previous statement still holds. Therefore,

$$\lim_{n\to\infty} |x_n|_p = |L|_p = \left|\lim_{n\to\infty} x_n\right|_p$$

which proves the desired result. □

4 Power series in $\mathbb{Q}_p$

Definition 18. *A series $\sum_{i\geqslant 0} a_i$ is said to converge if and only if the sequence (S_n) given by $S_n = \sum_{i=0}^{n} a_i$ converges.*

We will now give the condition of convergence for a series in $\mathbb{Q}_p$. The condition turns out to be much simpler than that in $\mathbb{R}$, in which there are multiple convergence tests for series.

Proposition 18. *The series $\sum_{n\geqslant 0} a_n$ converges in $\mathbb{Q}_p \iff$ the sequence $(a_n)_{n\geqslant 0}$ converges to 0 in $\mathbb{Q}_p$.*

Proof. Consider the sequence (S_n) given by $S_n = \sum_{i=0}^{n} a_i$. We need to show that (S_n) converges if and only if (a_n) converges.

Suppose (S_n) converges. We know that, by definition, (S_n) converges if and only if for all $\epsilon \in \mathbb{R}^+$ we have that there exists some natural number N_ϵ such that for all $m, n \geqslant N_\epsilon$ we have $|S_m - S_n|_p < \epsilon$. Consider some $n \geqslant N_\epsilon$. Then, we clearly have that

$$|S_{n+1} - S_n|_p < \epsilon$$

Now, by definition of S_n, we have $S_{n+1} - S_n = a_{n+1}$. Thus, $|a_{n+1}|_p < \epsilon$ for all $n \geqslant N_\epsilon$. Therefore, in general, we have that for every $\epsilon \in \mathbb{R}^+$, there is some $M_\epsilon = N_\epsilon + 1$ such that for all $n \geqslant M_\epsilon$ we have $|a_n|_p < \epsilon$. It follows that (a_n) converges to 0, by definition. Note that this direction of the proof holds in $\mathbb{R}$ as well. The opposite direction is what makes convergence in $\mathbb{R}$ more difficult.

Now, we will prove that if (a_n) converges to 0, then (S_n) converges. By definition, we have that for every $\epsilon \in \mathbb{R}^+$, there exists some natural number N_ϵ such that for all $n \geqslant N_\epsilon$ we have $|a_n|_p < \epsilon$. Now, consider some integers m, n such that $m > n \geqslant N_\epsilon$. We have

$$S_m - S_n = a_{n+1} + \cdots + a_m$$

Thus,

$$|S_m - S_n|_p = |a_{n+1} + \cdots + a_m|_p \leqslant \max(a_{n+1}, \ldots, a_m)$$

Since for all $n \geqslant N_\epsilon$, we have that $a_n < \epsilon$, it follows that $\max(a_{n+1}, \ldots, a_m) < \epsilon$. Hence $|S_m - S_n|_p < \epsilon$ for all $m, n > N_\epsilon$.

Thus, in general, for all $\epsilon \in \mathbb{R}^+$, we have that there exists some $N_\epsilon \in \mathbb{N}$ such that for all $m, n \geqslant N_\epsilon$, $|S_m - S_n|_p$. Hence, (S_n) converges. □

Note that the above proof holds entirely because of the fact that $|a + b|_p \leqslant \max(|a|_p, |b|_p)$.

4.1 Radius of Convergence

We define the radius of convergence of a power series $\sum_{n\geqslant 0} a_n x^n$ to be the value r so that the sequence $|a_n|_p c^n$ converges to 0 for all $c < r$ and does not converge for $c > r$. The following result is fundamental:

Proposition 19. *The radius of convergence of $\sum_{n\geqslant 0} a_n x^n$ is given by $r = \left(\limsup |a_n|_p^{1/n}\right)^{-1}$*

4.2 Discs

Definition 19. *For any $a \in \mathbb{Q}_p$ and $r \in \mathbb{R}^+$, we define a closed disc of radius r, centered at a to be the set $D(a; r) := \{z \in \mathbb{Q}_p \colon |z - a|_p \leqslant r\}$ and an open disc of radius r, centered at a to be the set $D(a; r^-) := \{z \in \mathbb{Q}_p \colon |z - a|_p < r\}$.*

Now, consider $f(x) = \sum_{n\geqslant 0} a_n x^n \in \mathbb{Q}_p[[x]]$, a power series, and suppose that its radius of convergence is r. Therefore, we can define a function $f \colon D(0; r^-) \to \mathbb{Q}_p$ so that for any $t \in D(0; r^-)$, we have

$$f(t) = \lim_{n\to\infty} \left(\sum_{k=0}^{n} a_k t^k \right)$$

Since $t \in D(0; r^-)$, the above sum indeed converges, and therefore, f is well defined.

We now defined continuity in $\mathbb{Q}_p$.

Definition 20. *We say that a function $f \colon S \to \mathbb{Q}_p$ is continuous at a point $x \in S$ if for all $\epsilon \in \mathbb{R}^+$, there exists some positive real δ such that $|x - y|_p < \delta$ implies $|f(x) - f(y)|_p < \epsilon$.*

Definition 21. *We say that a function $f \colon S \to \mathbb{Q}_p$ is continuous, if it is continuous at every point in S.*

Proposition 20. *Every function $f\colon D(0;r^-) \to \mathbb{Q}_p$ such that*

$$f(x) = \lim_{n\to\infty} \sum_{k=0}^{n} a_k x^k$$

for all $x \in D(0;r^-)$ is continuous in $\mathbb{Q}_p$.

Proof. We first prove a lemma:

Lemma 3. *Let $S_n = \sum_{k=0}^{n} a_k$ and let $S = \lim_{n\to\infty} S_n$. Then, $|S|_p \leqslant \lim_{n\to\infty} \max(|a_1|_p, \dots, |a_n|_p)$. This can also be written as $\max(|a_1|_p, |a_2|_p, \dots)$. Notationally, we shall express this as $\max(|a_k|_p)_{n\geqslant 0}$.*

Proof. We know that

$$S = \lim_{n\to\infty} S_n$$

Thus,

$$|S|_p = \left|\lim_{n\to\infty} S_n\right|_p$$

As we saw earlier, the above is equal to $\lim_{n\to\infty} |S_n|_p$, which is at most $\lim_{n\to\infty} \max(|a_1|_p, \dots, |a_n|_p)$. □

Let $x \in D(0;r^-)$ be any point in $D(0;r^-)$. Let y be another point in $D(0;r^-)$. Therefore, we have $|x|_p < r$ and $|y|_p < r$. Consider some positive real ϵ. Now, suppose that there is some $\delta \in \mathbb{R}^+$ such that $|x-y|_p < \delta$. Now, we have

$$\begin{aligned}
|f(x) - f(y)|_p &= \left|\lim_{n\to\infty}\left(\sum_{k=0}^{n} a_k x^k\right) - \lim_{n\to\infty}\left(\sum_{k=0}^{n} a_k y^k\right)\right|_p = \left|\lim_{n\to\infty}\left(\sum_{k=0}^{n} a_k (x^k - y^k)\right)\right|_p \\
&= \left|\lim_{n\to\infty}\left((x-y)\sum_{k=0}^{n} a_k (x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1})\right)\right|_p \\
&= |x-y|_p \left|\lim_{n\to\infty}\left(\sum_{k=0}^{n} a_k (x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1})\right)\right|_p
\end{aligned}$$

By the Lemma, we may simplify the above to get:

$$|f(x) - f(y)|_p \leqslant |x-y|_p \max\left(\left|a_n(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})\right|_p\right)_{n\geqslant 0}$$

Now,

$$\left|x^{n-1} + x^{n-2}y + \cdots xy^{n-2} + y^{n-1}\right|_p \leqslant \max\left(\left|x^{n-k}y^{k-1}\right|_p\right)_{k=1}^{n-1}$$

Since $|x|_p < r$ and $|y|_p < r$, it follows that $\left|x^{n-k}y^{k-1}\right|_p < r^{n-k}r^{k-1} = r^{n-1}$. Therefore,

$$\left|x^{n-1} + x^{n-2}y + \cdots xy^{n-2} + y^{n-1}\right|_p < r^{n-1}$$

Thus,

$$|f(x) - f(y)|_p < |x-y|_p \max\left(|a_n|_p\, r^{n-1}\right)_{n\geqslant 0}$$

Now, by the definition of continuity, we must prove that for all $\epsilon \in \mathbb{R}^+$, there exists some $\delta \in \mathbb{R}^+$ such that $|x-y|_p < \delta$ implies $|f(x) - f(y)|_p < \epsilon$. We can let

$$\delta = \frac{\epsilon}{\max\left(|a_n|_p\, r^{n-1}\right)_{n\geqslant 0}}$$

for any given positive real ϵ. Then, clearly $|x-y|_p < \delta$ implies $|f(x) - f(y)|_p$. Therefore, there always exists such a real number δ and hence $f(x)$ is continuous. □

For an alternative proof, we will use the notion of continuity between the mapping of two topological spaces.

Definition 22. *Let X and Y be topological spaces. The map $f\colon X \to Y$ is continuous $\iff$ the preimage of the open set is open.*

In other words, if you have a function f mapping from one topological space X to another topological space Y, and for any open set $U \subset Y$, the set of all points in X that map to points in U (i.e., the preimage of U) is open in X, then f is a continuous map.

Proof. To begin, let's prove first the following lemma:

Lemma 4. *Let $a, b \in \mathbb{Q}_p$ and $r, s \in \mathbb{R}^+$, we have the following properties of $D(a; r^-)$:*

i *If $b \in D(a; r^-)$, then $D(a; r^-) = D(b; r^-)$.*

ii *The open disc $D(a; r^-)$ is also a closed set.*

iii $D(a; r^-) \cap D(b; s^-) \neq \varnothing \iff D(a; r^-) \subset D(b; s^-)$ *or* $D(a; r^-) \supset D(b; s^-)$

Proof. *i* Observe the following, we can rewrite $x \in D(a; r^-)$ as,

$$|x - a|_p < r$$
$$|x - a|_p = (|x - b + b - a|_p) \leqslant \max(|x - b|_p, |b - a|_p) < r$$

We have that $\max(|x-b|_p, |b-a|_p)$ is contained $D(b; r^-)$, but then $|x-a|_p \leqslant \max(|x-b|_p, |b-a|_p)$, thus $D(a; r^-) \subset D(b; r^-)$, and since it is given that $b \in D(a; r^-)$ we also have $D(b; r^-) \supset D(a; r^-)$. Hence, $D(a; r^-) = D(b; r^-)$ as claimed.

ii By definition, $D(a; r^-)$ is an open set. We will show that it is also a closed set. Pick a boundary point in $D(a; r)$, and call it x, and also choose $s \leqslant r$. Since x is a boundary point, we have $D(a; r) \cap D(x; s) \neq \varnothing$, then $\exists y \in D(a; r) \cap D(x, s)$, this means that $|y - a| < r$ and $|y - x| < s \leqslant r$. Using the non-archimedean inequality, we have:

$$|x - a| < \max(|x - y|, |y - a|) < \max(s, r) \leqslant r$$

thus $x \in D(a; r)$ such that $D(a; r)$ contains each of its boundary points, making $D(a; r)$ a closed set by definition.

iii Assume W.L.O.G that $r \leqslant s$. If the intersection is non-empty then there exists a c in $D(a; r) \cap D(b; s)$. Then we know, from (i), that $D(a; r) = D(c; r)$ and $D(b; s) = D(c; s)$. Hence

$$D(a; r) = D(c; r) \subset D(c; s) = D(b; s)$$

□

Now to begin the proof, we define the preimage of $D(y; s^-)$ under f as,

$$f^{-1}(D(y; s^-)) = \{a \in D(0; r^-) | f(a) \in D(y; s^-)\}$$

For a sketch-proof, when these set of points in $D(0; r^-)$ that is in the preimage of f are open then f is continuous. Now, fix an element of the preimage of $D(y; s^-)$ under f, and call it t such that $|t|_p < r$. By definition, $f(t)$ converges in $D(y; s^-)$. By Proposition 16, it follows that $|a_n t^n|$ converges to 0 in $D(y; s^-)$. We have that $|a_n t^n|_p$ is a Cauchy sequence. Since $a_n \in \mathbb{Q}_p$, it is Cauchy, then we have $|a_n t^n|_p = |a_n|_p |t^n|_p < \epsilon \cdot |t^n|_p$. For which it follows that (t^n) is Cauchy since we have $|a_m t^m|_p < \epsilon$ for every $m > M$ (for a fix large M). Then it follows that t converges in $D(y; s^-)$. Next, we have that $t \in D(y; s^-)$, and also $t \in D(0; r^-)$ then $D(y; s^-) \cap D(0; r^-) = \{t\}$. By Lemma 4, we know that $D(0; r^-) = D(t; r^-) \subset D(t; s^-) = D(y; s^-)$. Then we have a union of open disks which are the preimage of $D(y; s^-)$ under f,

$$f^{-1}(D(y; s^-)) = \bigcup_{|t|_p < r} D(t; r^-)$$

Hence it follows that f is continuous as claimed. □

Remarks 1. *The characterization all power series $f(x) \in \mathbb{Q}_p[[x]]$ such that $f(x)$ converges at every point of the closed unit disk $D(0; 1)$ are as follows:*

- *The function $f : D(0; r^-) \to D(0; 1^-)$ must be continuous.*
- *Given $t \in D(0; r^-)$, the sequence of coefficient of f, given by (a_n) satisfy that $|a_n t^n|_p$ converges to 0 in $D(0; 1)$.*
- *For a power series to converge to 1, it needs $f(0) = 1$. Since there exists $g \in \mathbb{Q}_p[[x]]$ such that $f \cdot g = 1$ for which multiplication is closed in $\mathbb{Q}_p[[x]]$. In other words, $f(x) \in 1 + x\mathbb{Q}_p[[x]]$.*

5 Exponentiation in p-adics

We define the exponentiation of x in the p-adics to be the following element of $\mathbb{Q}_p[[x]]$:

$$\exp(x) = \sum_{n \geqslant 0} \frac{x^n}{n!}$$

We see that the exp function has the following properties:

Proposition 21. *We have* $\exp(x+y) = \exp(x) \cdot \exp(y)$ *in* $\mathbb{Q}_p[[x,y]]$.

Proof. We have

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

and

$$\exp(y) = 1 + x + \frac{y^2}{2!} + \frac{y^3}{3!} + \cdots$$

Thus,

$$\exp(x) \cdot \exp(y) = \left(1 + x + \frac{x^2}{2!} + \cdots\right)\left(1 + y + \frac{y^2}{2!} + \cdots\right)$$

Expanding the above product and combining all terms with the same degree, we get:

$$\exp(x) \cdot \exp(y) = 1 + (x+y) + \left(\frac{x^2}{2!} + xy + \frac{y^2}{2!}\right) + \cdots + \sum_{k=0}^{n}\left(\frac{x^k y^{n-k}}{k!(n-k)!}\right) + \cdots$$

Writing the above as a summation with respect to n, we get:

$$\exp(x) \cdot \exp(y) = \sum_{n \geqslant 0}\left(\sum_{k=0}^{n} \frac{x^k y^{n-k}}{k!(n-k)!}\right) = \sum_{n \geqslant 0}\left(\frac{\sum_{k=0}^{n}\binom{n}{k} x^k y^{n-k}}{n!}\right) = \sum_{n \geqslant 0} \frac{(x+y)^n}{n!} = \exp(x+y)$$

by the binomial theorem, and we are done. Hence, we have a homomorphism $\phi : \mathbb{Q}_p^2 \to \mathbb{Q}_p$ such that $\exp(x)$ satisfies $\phi(x \circ y) = \phi(x) \circ \phi(y)$ □

Proposition 22. *The radius of convergence of* $\exp(x)$ *is* $p^{-\frac{1}{p-1}}$

Proof. We know that the radius, r, of convergence of any power series in the p-adics is given by $r = (\limsup |a_n|_p^{1/n})^{-1}$. Therefore, we know that the radius of convergence, r of $\exp(x)$ is given by $(\limsup \left|\frac{1}{n!}\right|_p)^{-1}$. We need to therefore prove that

$$\left(\limsup \left|\frac{1}{n!}\right|_p\right)^{-1} = p^{-1/(p-1)}$$

In order to do so, we need the following lemma

Lemma 5. $v_p(n!) = \frac{n - S_p(n)}{p-1}$ *($S_p(n)$ is the sum of all digits of n over base p)*

Proof. Notice that $v_p(n!) = v_p(n) + v_p(n-1) + \cdots = \sum_{l \leqslant n} v_p(l)$. We take $v_p(l)$ $(l \leqslant n)$, and expand l over base p. Take $l = l_m p^m + \cdots + l_r p^r$ $(m \leqslant r,\ l_m \neq 0)$, where we have $v_p(l) = m$. Using telescoping techniques, observe that:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^m - p^m$$
$$l - 1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^{m-1} + (l^m - 1)p^m + \cdots + l_r p^r$$

We have that the sum of the digits (over base p) of $l-1$ is,

$$S_p(l-1) = m(p-1) + S_p(l) - 1$$

The reason why there is -1 on the RHS since we have $l_m - 1$ from the previous equation, thus it follows we have $S_p(l) - 1$. We know that $v_p(l) = m$, then solving for m, we have

$$m = \frac{1}{p-1}\left[S_p(l-1) - S_p(l) + 1\right]$$

Then we have,

$$v_p(n!) = \sum_{l \leqslant n} v_p(l) = \frac{1}{p-1} \sum_{l \leqslant n} [S_p(l-1) - S_p(l) + 1]$$

Since this is a telescoping series, we have that:

$$v_p(n!) = \frac{1}{p-1}(-S_p(n) + n) = \frac{n - S_p(n)}{p-1}$$

□

Lemma 6. $\limsup((v_p(n!)/n)$ *converges to* $1/(p-1)$.

Proof. Consider some non-negative integer k. Consider the sequence of all reals $v_p(n!)/n$ where n is so that $p^k \leqslant n < p^{k+1}$. The maximum value of this sequence occurs when $n = p^k$. Thus, the supremum of the sequence $v_p(n!)/n$ when $p^k \leqslant n < p^{k+1}$ is $v_p((p^k)!)/p^k$. By Legendre's formula

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

When $n = p^k$, this simplifies to:

$$v_p(n!) = p^{k-1} + \cdots + 1 = \frac{p^k - 1}{p-1}$$

Thus,

$$\frac{v_p(n!)}{n} = \frac{p^k - 1}{p^k(p-1)} = \frac{1}{p-1} \cdot \frac{p^k - 1}{p^k}$$

The above gives the maximum value of $v_p(n!)$ for n between p^k and p^{k+1}. Thus, one may conclude that

$$\limsup(v_p(n!)/n) = \lim_{k \to \infty} \left(\frac{1}{p-1} \cdot \frac{p^k - 1}{p_k} \right)$$

The $1/(p-1)$ term is constant. Moreover, the sequence $\frac{p^x - 1}{(p-1)p^x}$ where x is a real number converges to the same real number as $(p^k - 1)/(p^k(p-1))$ where k is an integer since $\mathbb{Z} \in \mathbb{R}$. Therefore

$$\lim_{k \to \infty} \frac{1}{p-1} \cdot \frac{p^k - 1}{p^k} = \lim_{x \to \infty} \frac{1}{p-1} \cdot \frac{p^x - 1}{p^x} = \frac{1}{p-1}$$

Hence $\limsup(v_p(n!)/n) = 1/(p-1)$. □

Now, our goal is to find lim sup of the sequence $|1/n!|_p^{1/n}$. The sequence $(|1/n!|_p^{1/n})$ can be rewritten as

$$\left(p^{-v_p(1/n!)/n}\right) = \left(p^{v_p(n!)/n}\right)$$

Now,

$$\limsup \left(p^{v_p(n!)/n}\right) = p^{\limsup(v_p(n!)/n)}$$

since p^k is a strictly increasing function with respect to k. By our lemma, we therefore have

$$\limsup(|1/n!|_p^{1/n}) = p^{1/(p-1)}$$

Thus, $r = p^{-1/(p-1)}$ and we are done. □

Proposition 23. *For all* $a, b \in D(0; \left(p^{-1/(p-1)}\right)^-)$*, we have* $a + b \in D(0; \left(p^{-1/(p-1)}\right)^-)$*. Therefore, we have* $\exp(a+b) = \exp(a) \cdot \exp(b)$.

Proof. By definition, from $a, b \in D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$ we have $|a|_p, |b|_p < p^{-1/(p-1)}$. Thus, we have $\max(|a|_p, |b|_p) < p^{-1/(p-1)}$. Hence, $|a+b|_p \leqslant \max |a|_p, |b|_p < p^{-1/(p-1)}$. Thus, we have $a+b \in D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$.

Now, we know

$$\exp(a) = \lim_{n\to\infty}\left(\sum_{k=0}^{n}\frac{a^k}{k!}\right)$$

and

$$\exp(b) = \lim_{n\to\infty}\left(\sum_{k=0}^{n}\frac{b^k}{k!}\right)$$

Thus,

$$\exp(a)\cdot\exp(b) = \left(\lim_{n\to\infty}\left(\sum_{k=0}^{n}\frac{a^k}{k!}\right)\right)\cdot\left(\lim_{n\to\infty}\left(\sum_{k=0}^{n}\frac{b^k}{k!}\right)\right) = \lim_{n\to\infty}\left(\sum_{k=0}^{n}\frac{a^k}{k!}\cdot\sum_{k=0}^{n}\frac{b^k}{k!}\right)$$

We can expand the product of the summations and combine the terms of the same degree to get:

$$\sum_{k=0}^{n}\frac{a^k}{k!}\cdot\sum_{k=0}^{n}\frac{b^k}{k!} = \sum_{k=0}^{n}\frac{(a+b)^k}{k!} + f_n(a,b)$$

where $f_n(x,y)$ is some polynomial in $\mathbb{Q}_p[x,y]$ such that the smallest degree of the terms is $n+1$. Therefore,

$$\lim_{n\to\infty}\left(\sum_{k=0}^{n}\frac{a^k}{k!}\cdot\sum_{k=0}^{n}\frac{b^k}{k!}\right) = \lim_{n\to=\infty}\left(\sum_{k=0}^{n}\frac{(a+b)^k}{k!}\right) + \lim_{n\to\infty} f_n(a,b) = \exp(a+b) + \lim_{n\to\infty} f_n(a,b)$$

by definition of $\exp(a+b)$. We know that the degree of the term with lowest degree in $f(x,y)$ is $n+1$. Moreover, we have $|x|_p, |y|_p < p^{-1/(p-1)}$. Assume WLOG that $|x|_p \leqslant |y|_p < p^{-1/(p-1)}$. Hence,

$$\left|x^k y^{n+1-k}\right|_p < \left|y^{n+1}\right|_p < p^{-n/(p-1)}$$

for any k. Moreover, for any term in $f(x,y)$ with the power of x and y being s, t respectively, we must have $|x^s y^t|_p < p^{-n/(p-1)}$ since $s+t \geqslant n+1$ for $f(x,y)$. But, each term of $f(x,y)$ also has coefficients. We know that the coefficients of $f(x)$ are at least $(1/n!)^2$. Thus, the p-adic absolute value of a term of $f(x,y)$ is at most

$$p^{2v_p(n!)}p^{-n/(p-1)}$$

Now, we know that $v_p(n!) \leqslant 1/(p-1)$ as n goes to infinity as we saw earlier. Thus, the maximum value of the p-adic absolute value of the individual terms of $f(x,y)$ is

$$p^{\frac{2-n}{p-1}}$$

as n approaches ∞. As n approaches infinity, the above approaches 0. Thus, $\lim_{n\to\infty}|f_n(a,b)|_p = 0$. Hence, $f_n(a,b)$ itself approaches 0 in $\mathbb{Q}_p$ as we have seen earlier. Hence, $\exp(a+b) = \exp(a)\exp(b)$. □

Corollary 1. $\exp(na) = \exp(a^n)$ *for all integers* n *and* $a \in D(0; \left(p^{-1/(p-1)}\right)^-)$.

Proposition 24. *We have* $|\exp(x) - \exp(y)|_p = |x-y|_p$.

Proof. We first prove that the statement is true when $y = 0$. When $y = 0$, we have $\exp(y) = 0$. Therefore, we need to prove that $|\exp(x) - 1|_p = |x|_p$. We have

$$\exp(x) - 1 = \sum_{n\geqslant 1}\frac{x^n}{n!}$$

As we saw earlier, we have

$$|\exp(x) - 1|_p \leqslant \max\left(\left|\frac{x^n}{n!}\right|_p\right)_{n\geqslant 1}$$

We claim that the maximum absolute value is $|x|_p$. In order to do so, let us suppose for the sake of contradiction that there is some term $x^n/n!$ with an absolute value that is more than or equal to the absolute value of x. So, we have $|x^n/n!|_p \geqslant |x|_p$, which happens if and only if $|x|_p^{n-1} |1/n!|_p \geqslant 1$ or $|x|_p^{n-1} \geqslant |n!|_p$. By the definition of the p-adic absolute value, this happens if and only if

$$\begin{aligned} p^{-(n-1)v_p(x)} \geqslant p^{-v_p(n!)} &\iff -(n-1)v_p(x) \geqslant -v_p(n!) \\ &\iff (n-1)v_p(x) \leqslant v_p(n!) \\ &\iff v_p(n!)/(n-1) \geqslant v_p(x) \end{aligned}$$

Now, $|x|_p < p^{-1/(p-1)}$. Therefore, $v_p(x) > 1/(p-1)$. Thus, we finally get $v_p(n!)/(n-1) > 1/(p-1)$ which is a contradiction. Therefore, we must have that $|x|_p$ is the unique maximum value in the sequence $|x^n/n!|_p$. Since the maximum value is unique, we have

$$\left| \sum_{n \geqslant 1} \frac{x^n}{n!} \right|_p = \max \left(\left| \frac{x^n}{n!} \right|_p \right)_{n \geqslant 1} = |x|_p$$

This proves that $|\exp(x) - 1|_p = |x|_p$.

Now, consider any y in $D\left(0; \left(p^{-1/(p-1)}\right)^-\right)$. Therefore, we have

$$|\exp(x) - \exp(y)|_p = |(\exp(x) - 1) - (\exp(y) - 1)|_p \leqslant \max(|\exp(x) - 1|_p, |\exp(y) - 1|_p)$$

Since $|\exp(x) - 1|_p = |x|_p$, we have the above may be written as $\max(|x|_p, |y|_p)$. If $|x|_p \neq |y|_p$, we have $|\exp(x) - 1|_p \neq |\exp(y) - 1|_p$. Therefore, we have $|\exp(x) - \exp(y)|_p = \max(|x|_p, |y|_p) = |x - y|_p$.

□

6 Artin-Hasse Exponential Function

Theorem 2. $E(x) \in \mathbb{Z}_p[[x]]$

To prove this theorem, we need to prove the following Lemmas first:

Lemma 7. *Let $f(x) \in 1 + x\mathbb{Q}_p[[x]]$ be a power series with p-adic rational coefficients. Then $f(x) \in 1 + x\mathbb{Z}_p[[x]] \iff \frac{f(x^p)}{f(x)^p} \in 1 + px\mathbb{Z}_p[[x]]$*

Proof. We will begin with the assumption that $f(x) \in 1 + x\mathbb{Z}_p[[x]]$. We can see that the constant term is given by,

$$F(0) = f(0)^p - f(0^p) = \left(1 + \sum_{i \geqslant 1} a_i 0^i\right)^p - \left(1 + \sum_{i \geqslant 1} a_i 0^p i\right) = 1^p - 1 = 0$$

Thus we have that $f(0)^p = f(0^p) = 1$, then it follows that $f(x)^p$ and $f(x^p)$ are both invertible formal power series. Then there exists $t(x) \in 1 + px\mathbb{Z}_p[[x]]$ such that $\frac{f(x^p)}{f(x)^p} = t(x)$. The reason why $t(x) \in 1 + px\mathbb{Z}_p[[x]]$ is because that the coefficients of $t(x)$ satisfy a linear recursion that is derived from the product $f(x)^p \cdot t(x) = f(x^p)$. By construction, the coefficients of $t(x)$ are $a_n = \sum_{i=1}^m c_i a_{n-1}$ ($\exists m \geqslant 0$, $n > 0$), and (c_i) are the coefficients of $f(x)^p$. By the multinomial theorem, the coefficients (c_i) is given by $p!/(r_1!r_2!r_3!(\cdots))$ such that $\sum_{i \geqslant 0} r_i = p$. From this, we know that the coefficients (except the constant term) of $f(x)^p$ is a multiple of p. Hence it follows that $t(x) \in 1 + px\mathbb{Z}_p[[x]]$ exists. Now, supposed that $f(x^p) = f(x)^p \cdot g(x)$ with $g(x) \in 1 + px\mathbb{Z}_p[[x]]$. Let $f(x) = \sum_{n \geqslant 0} a_n x^n$, $g(x) = \sum_{n \geqslant 0} b_n x^n$. By assumption, $a_0 = 1$, and suppose that we have the required integrality for a_n with $0 \leqslant n < N-1$. We will show that the Nth coefficient of $f(x)^p \cdot g(x)$ is equal to the Nth coefficient of $(\sum_{n \leqslant N} a_n x^n)^p + \sum_{n \leqslant N} b_n x^n$ for which this sum is just a redefinition of $f(x^p)$ if we take $N \to \infty$. The proof will proceed by induction. To begin, let's expand these power series to get a sense of the terms,

$$f(x)^p = \left(\sum_{i=0}^{N-1} a_i x^i + a_N x^N + \sum_{k \geqslant N+1} a_k x^k\right)^p = \sum_{t=0}^{p} \binom{p}{t} \left(\sum_{i=0}^{N-1} a_i x^i + \sum_{k \geqslant N+1} a_k x^k\right)^{p-t} (a_N x^N)^t$$

$$\left(\sum_{n \leqslant N} a_n x^n\right)^p = \sum_{i=0}^{p} \binom{p}{i} \left(\sum_{n \leqslant N-1} a_n x^n\right)^{p-i} (a_N x^N)^i$$

We have two cases, $p \nmid N$ and $p \mid N$. Suppose $p \nmid N$, then there is no $m \in \mathbb{Z}$ such that $N = pm$ (that would give us another Nth coefficient which is $a_{\frac{N}{p}}^{p}$). Thus we have that the Nth coefficient of $(\sum_{n \leqslant N} a_n x^n)^p + \sum_{n \leqslant N} b_n x^n$ is $\binom{p}{1} a_N a_0 + b_N = p(1)(a_N) + b_N = pa_N + b_N$, while we have that the Nth coefficient of $f(x)^p \cdot g(x)$ is $g(0)\binom{p}{1} a_N + a_0 b_N$. Since we have assumed that $a_0 = 1$, then by the linear recursion definition of the coefficient of $g(x)$, we have that $a_0 b_0 = 1$ then $b_0 = 1$. It follows that the Nth term of $f(x)^p \cdot g(x)$ is $(1)pa_N + (1)b_N = pa_N + b_N$. The intuition behind the multiplication of $f(x)^p \cdot g(x)$ is just termwise multiplication, thus we can find the pairs such that they're the Nth term. Since by definition, $g(x) \in 1 + p\mathbb{Z}_p[[x]]$, it follows that $b_N \in p\mathbb{Z}_p$. Now, it follows that we can always construct the Nth coefficient using the linear-recursion definition of the coefficient of $g(x)$ then the construction is followed by induction. Hence both of them have the same Nth coefficient such that $p \nmid N$. Also, we can conclude that $a_N \in \mathbb{Z}_p$, since the Nth coefficient is not divisible by p^2 but by p only, thus it follows that the Nth coefficient is in $p\mathbb{Z}_p$ and $a_N \in \mathbb{Z}_p$. Now for our second case, suppose that $p \mid N$, then there exists $m \in \mathbb{Z}$ such that $N = pm$. We have that the Nth coefficient of $(\sum_{n \leqslant N} a_n x^n)^p + \sum_{n \leqslant N} b_n x^n$ is $a_{\frac{N}{p}}^{p} + \binom{p}{1} a_N + b_N = a_{\frac{N}{p}}^{p} + (1)a_N + b_N = a_{\frac{N}{p}}^{p} + a_N + b_N$. To find $a_{\frac{N}{p}}^{p}$ in $(\sum_{n \leqslant N} a_n x^n)^p$, consider the pth term and set $i = 0$, observe the following:

$$\left(\sum_{n \leqslant N-1} a_n x^n \right)^p = \left(\sum_{n \leqslant \frac{N}{p}-1} a_n x^n + a_{\frac{N}{p}} x^{\frac{N}{p}} + \sum_{n=\frac{N}{p}-1}^{N-1} a_n x^n \right)^p$$

$$\left(\sum_{n \leqslant \frac{N}{p}-1} a_n x^n + a_{\frac{N}{p}} x^{\frac{N}{p}} + \sum_{n=\frac{N}{p}-1}^{N-1} a_n x^n \right)^p = \left(\left(\sum_{n \leqslant \frac{N}{p}-1} a_n x^n + \sum_{n=\frac{N}{p}-1}^{N-1} a_n x^n \right) + a_{\frac{N}{p}} x^{\frac{N}{p}} \right)^p$$

Then by the binomial theorem, it follows that we have $a_{\frac{N}{p}}^{p}$ as the additional term for the Nth coefficient of $(\sum_{n \leqslant N} a_n x^n)^p + \sum_{n \leqslant N} b_n x^n$. While for the Nth coefficient of $f(x)^p \cdot g(x)$, we have $a_{\frac{N}{p}}^{p} + g(0)\binom{p}{1} a_N + a_0 b_N$. To find the value of $a_{\frac{N}{p}}^{p}$, consider the pth term and set $t = 0$, observe the following:

$$\left(\sum_{i=0}^{N-1} a_i x^i + \sum_{k \geqslant N+1} a_k x^k \right)^p = \left(\sum_{i=0}^{(N/p)-1} a_i x^i + a_{\frac{N}{p}} x^{\frac{N}{p}} + \sum_{k \geqslant \frac{N}{p}+1} a_k x^k \right)^p$$

$$\left(\sum_{i=0}^{(N/p)-1} a_i x^i + a_{\frac{N}{p}} x^{\frac{N}{p}} + \sum_{k \geqslant \frac{N}{p}+1} a_k x^k \right)^p = \left(\left(\sum_{i=0}^{(N/p)-1} a_i x^i + \sum_{k \geqslant \frac{N}{p}+1} a_k x^k \right) + a_{\frac{N}{p}} x^{\frac{N}{p}} \right)^p$$

Then by the binomial theorem, it follows that we have $a_{\frac{N}{p}}^{p}$ as the additional term for the Nth coefficient of $f(x)^p \cdot g(x)$. Now, it follows that we can always construct the Nth coefficient using the linear-recursion definition of the coefficient of $g(x)$ then the construction is followed by induction. Hence both of them have the same Nth coefficient such that $p \mid N$. Also in our second case, we can conclude that $a_N \in \mathbb{Z}_p$, since the Nth coefficient is not divisible by p^p but by p only, thus it follows that the Nth coefficient is in $p\mathbb{Z}_p$ and $a_N \in \mathbb{Z}_p$. Since we have successfully concluded that $a_N \in \mathbb{Z}_p$, it follows that $f(x) \in 1 + x\mathbb{Z}_p[[x]]$. □

Lemma 8. $\exp(-px) \in 1 + p\mathbb{Z}_p[[x]]$

Lemma 9. $\frac{E(x^p)}{E(x)^p} = \exp(-px)$

Now we are ready to prove Theorem 2.

Proof. It follows that $E(x) \in 1 + x\mathbb{Z}_p[[x]]$ by Lemma 7 due to Lemma 9, thus it follows that the coefficients of $E(x)$ is in $\mathbb{Z}_p$ by Lemma 7. □