Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea Triennale in Matematica

Analytic functions on p-adic fields

Relatore:
Prof. Maurizio Cailotto

Candidato:
Carlo Buccisano
Matricola 1152337

Data sessione di laurea: 5 luglio 2019
Anno accademico 2018/2019

Introduzione

Questa tesi si compone di due parti: nella prima (capitoli 1-3) si costruiscono i vari campi p-adici per arrivare a $\mathbb{C}_p$, campo completo e algebricamente chiuso, tentando di emulare il procedimento classico che da $(\mathbb{Q}, |\ |_\infty)$ porta a $\mathbb{C}$. Nella seconda parte (capitoli 4-5), invece, si studiano le funzioni analitiche su $\mathbb{C}_p$, definite come serie di potenze, con particolare attenzione ad alcune funzioni elementari, come l'esponenziale e il logaritmo, e alle differenze che si presentano nel caso p-adico rispetto al caso classico. Infine, nel capitolo 5, viene definito il poligono di Newton, potente strumento per capire subito il raggio di convergenza e l'ordine (p-adico) degli zeri di una funzione analitica.

Più specificamente, nel capitolo 1, dopo aver introdotto la definizione di norma e quella di valore assoluto p-adico su $\mathbb{Q}$ (e aver mostrato che definisce una norma non-Archimedea), si dimostra il teorema di Ostrowski, che afferma che ogni norma non banale su $\mathbb{Q}$ è equivalente o al valore assoluto classico o a un valore assoluto p-adico, per qualche primo p. Viene poi provato che $(\mathbb{Q}, |\ |_p)$ non è completo e viene definito, nel modo classico, il suo completamento $(\mathbb{Q}_p, |\ |_p)$, analogo di $(\mathbb{R}, |\ |_\infty)$ nel caso classico. Infine, viene provato un teorema di struttura, che afferma che ogni elemento di $\mathbb{Q}_p$ può essere scritto come una serie del tipo $\sum_{i=m}^{+\infty} a_i p^i$, con $a_i \in \{0, \ldots, p-1\}$ e $m \in \mathbb{Z}$.

Nel capitolo 2 si arriva di nuovo a costruire $(\mathbb{Q}_p, |\ |_p)$ in un modo, però, totalmente diverso dal primo e più "algebrico". Si parte infatti da $\mathbb{Z}_p$, insieme contenente tutti gli elementi del tipo $\sum_{i=0}^{+\infty} a_i p^i$ con $a_i \in \{0, \ldots, p-1\}$, equipaggiato con le operazioni di somma con riporto e prodotto alla Cauchy (con riporto). Si mostra che esso è un dominio integrale (qui si capisce perché p debba essere primo) e che contiene gli interi (o meglio, che esiste un monomorfismo $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$). Dopo un breve excursus su proprietà generiche dei gruppi topologici (dalle quali si ricaverà che $\mathbb{Z}_p$ è uno spazio compatto, completo e metrizzabile), viene mostrata un'altra definizione di $\mathbb{Z}_p$: come limite proiettivo degli insiemi $\mathbb{Z}/p^n\mathbb{Z}$. Infine si mostra che $\mathbb{Q}_p$ è esattamente il campo delle frazioni di $\mathbb{Z}_p$ e si introduce il lemma di Hensel, fondamentale strumento per "rialzare" le radici di polinomi da $\mathbb{Z}/p^n\mathbb{Z}$ a $\mathbb{Z}_p$, quando il polinomio soddisfa opportune ipotesi.

Nel capitolo 3, dopo un breve excursus su generiche proprietà di spazi ultrametrici, si studiano le estensioni di campi $K/\mathbb{Q}_p$ di grado finito e si vede come si può estendere il valore assoluto p-adico a tali campi K. Vengono poi classificate in base al loro indice di ramificazione e al grado residuo, con particolare attenzione ad estensioni non ramificate e totalmente ramificate. Dopo aver mostrato una versione analoga del criterio di Eisenstein nel caso p-adico, viene mostrato che $\mathbb{Q}_p$ ammette estensioni di qualunque grado finito, da cui si ricava che la sua chiusura algebrica, $\mathbb{Q}_p^{\text{alg cl}}$, ha necessariamente grado infinito su $\mathbb{Q}_p$. Infine si mostra che $(\mathbb{Q}_p^{\text{alg cl}}, |\ |_p)$ non è completo e si considera il suo completamento $\mathbb{C}_p$, che si mostrerà essere anche algebricamente chiuso. Si noti che qui il caso p-adico sembra essere più complicato del caso classico: ciò è dovuto al fatto che $\mathbb{Q}_p^{\text{alg cl}}$ ha grado infinito su $\mathbb{Q}_p$ e dunque la completezza si "perde", mentre nel caso classico $\mathbb{C} = \mathbb{R}^{\text{alg cl}}$ ha grado finito (2) su $\mathbb{R}$ e dunque rimane completo. Infine viene dimostrato un teorema di struttura di $\mathbb{C}_p$, che afferma che ogni elemento è prodotto di una potenza frazionaria (radice di un polinomio del tipo $X^a - p^b$, con $a, b \in \mathbb{Z}$), una radice di 1 e un elemento nel disco aperto di raggio 1 centrato in 1. In realtà, come spiegato alla fine del capitolo 3, i due processi (di costruzione di campi completi e algebricamente chiusi) possono essere fatti in modo totalmente analogo: si considera prima $\mathbb{Q}$, poi la sua chiusura algebrica $\mathbb{Q}^{\text{alg cl}}$ e si completa quest'ultima rispetto a $|\ |_\infty$ per ottenere $\mathbb{C}$ e rispetto a $|\ |_p$ per ottenere $\mathbb{C}_p$. Il problema di questa costruzione è la notevole difficoltà che si incontra nello studio di $\mathbb{Q}^{\text{alg cl}}$.

Nel capitolo 4 viene introdotta la nozione di funzione analitica su $\mathbb{C}_p$, funzione definita come una serie di potenze (dove esssa converge). Viene provato poi che la stessa formula classica per trovare il raggio di convergenza di una serie di potenze vale anche nel caso p-adico (sostituendo chiaramente il valore assoluto p-adico a quello classico). Viene anche introdotta le definizione di differenziabilità (e stretta differenziabilità) e viene provato che le funzioni analitiche sono differenziabili nel modo standard (termine a termine). Vengono poi definite le funzioni $\exp_p(X)$ e $\log_p(1+X)$ (usando le serie di MacLaurin note dal caso classico) e viene provato che, a differenza del caso reale, la funzione esponenziale converge solo su un piccolo disco aperto centrato in 0 (di raggio $r_p = p^{-1/(p-1)}$). Le proprietà classiche di esponenziale e logaritmo, però, si conservano anche nel caso p-adico e, restringendo in maniera appropriata dominio e codominio, si mostra che esponenziale e logaritmo sono funzioni l'una inversa dell'altra. Infine si introducono due nuove funzioni: il logaritmo di Iwasawa e l'esponenziale di Artin-Hasse. La prima è una funzione localmente analitica, definita su tutto $\mathbb{C}_p$, che estende il logaritmo precedentemente definito e ha derivata $x \mapsto 1/x$. L'esponenziale di Artin-Hasse, invece, è ricavato togliendo i termini "problematici" dall'esponenziale, ottenendo così una più estesa regione di convergenza (più specificamente viene prima mostrato un modo per scrivere $\exp_p(X)$ come prodotto infinito di serie di potenze e viene poi notato che sono solo alcuni di questi termini a imporre una minore regione di convergenza: togliendoli si ottiene l'esponenziale di Artin-Hasse). Nonostante il nome che potrebbe trarre in inganno, esso non è un'estensione dell'esponenziale: infatti vale $\mathrm{E}_p(X) = \exp_p\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots\right)$.

Nell'ultimo capitolo viene introdotta la definizione di poligono di Newton prima per i polinomi e poi per le serie di potenze. Viene poi presentato l'importante teorema che lega gli zeri di un polinomio al suo poligono di Newton: infatti per ogni segmento di pendenza λ e di lunghezza M (qui per lunghezza si intende quella della proiezione sull'asse orizzontale) vi sono esattamente M zeri, contati con molteplicità, di ordine p-adico $-\lambda$ e tutti gli zeri sono ottenuti in questo modo. Dopo aver mostrato che il raggio di convergenza di una serie è esattamente il sup delle pendenze del suo poligono di Newton si mostrano dei lemmi tecnici per arrivare a dimostrare il teorema di separazione di Weierstrass. Esso ha, tra i suoi corollari, la generalizzazione alle serie di potenze del teorema precedentemente enunciato solo per i polinomi, ossia per ogni segmento di lunghezza $N < +\infty$ e di pendenza λ si hanno N zeri della serie di ordine p-adico $-\lambda$. L'ultimo risultato mostrato è che ogni serie di potenze $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ convergente su tutto $\mathbb{C}_p$ ha un insieme di zeri numerabile, sia $(r_n)_{n\in\mathbb{N}}$, e vale $f(X) = \prod_{n\in\mathbb{N}}\left(1 - \frac{X}{r_n}\right)$. Possiamo pensare a tale risultato come ad una generalizzazione del teorema fondamentale dell'algebra (esiste una versione di tale teorema anche su $\mathbb{C}$, ma si ottiene un prodotto con fattori più complicati). Tra le conseguenze di quest'ultimo vi è ad esempio il fatto che non può esistere, su $\mathbb{C}_p$, un esponenziale come nel caso classico, ossia ovunque convergente e mai nullo: infatti qualunque serie del genere deve essere una costante.

Contents

1 Analytic Approach

1.1 Basic concepts

Here we'll define some basic concepts about norms and metrics.

Definition 1.1. Let X be a non-empty set, a function $d\colon X \times X \to \mathbb{R}_{\geq 0}$ is a *metric* if, for every $x, y, z \in X$, we have:

1. $d(x,y) = 0 \iff x = y$;
2. $d(x,y) = d(y,x)$;
3. $d(x,y) \leq d(x,z) + d(z,y)$.

Definition 1.2. Let F be a field, a function $\| \ \|\colon F \to \mathbb{R}_{\geq 0}$ is a *field norm*[1](or an *absolute value*) if, for every $x, y \in F$, we have:

1. $\|x\| = 0 \iff x = 0$;
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$;
3. $\|x + y\| \leq \|x\| + \|y\|$.

Definition 1.3. Let V be a vector space over the field F, which has its norm $\| \ \|_F$. A function $\| \ \|\colon V \to \mathbb{R}_{\geq 0}$ is a *norm* if, for every $v, w \in V, \alpha \in F$, we have:

1. $\|v\| = 0 \iff v = 0$;
2. $\|\alpha \cdot v\| = \|\alpha\|_F \cdot \|v\|$;
3. $\|v + w\| \leq \|v\| + \|w\|$.

Beginning from a (field) norm $\| \ \|$ there's a natural metric defined as $d(x,y) = \|x - y\|$.

1.2 Metrics on $\mathbb{Q}$

The metric we normally equip $\mathbb{Q}$ with is the euclidean one, which comes from the usual absolute value $| \ |$ (denoted also by $| \ |_\infty$).

Definition 1.4. Let p a fixed prime. We can define a function $\operatorname{ord}_p : \mathbb{Z} \to \mathbb{N} \cup \{+\infty\}$ as follows:

$$\operatorname{ord}_p a := \begin{cases} +\infty, & \text{if } a = 0; \\ n_a, & \text{otherwise;} \end{cases}$$

where $n_a \in \mathbb{N}$ is such that $p^{n_a} | a$ and $p^{n_a+1} \nmid a$. It's easy to prove that $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$ (using the usual convention $\infty + n = n + \infty = +\infty$).

[1] Although usually the term "field norm" has a different definition in field theory, we choose to use this terminology, to distinguish between norms on fields and norms on vectorial spaces.

We can extend this function to $\mathbb{Q}$:

$$\operatorname{ord}_p\left(\frac{a}{b}\right) := \begin{cases} +\infty, & \text{if } \frac{a}{b}=0; \\ \operatorname{ord}_p a - \operatorname{ord}_p b, & \text{otherwise;} \end{cases} .$$

This is of course well defined: $\operatorname{ord}_p\left(\frac{ac}{bc}\right) = \operatorname{ord}_p ac - \operatorname{ord}_p bc = \operatorname{ord}_p a - \operatorname{ord}_p b = \operatorname{ord}_p\left(\frac{a}{b}\right)$.

Proposition 1.5. $\operatorname{ord}_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ *is a discrete valuation.*

Proof. We have to prove the following properties:

- $\operatorname{ord}_p x = +\infty \iff x = 0$;
- $\operatorname{ord}_p xy = \operatorname{ord}_p x + \operatorname{ord}_p y$;
- $\operatorname{ord}_p (x+y) \geq \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}$.

The first two properties are quite easy, to see why the third one is true it's sufficient to write

$$x = \frac{a}{b} = p^{\operatorname{ord}_p x} \cdot \frac{a'}{b'}, \qquad y = \frac{c}{d} = p^{\operatorname{ord}_p y} \cdot \frac{c'}{d'}$$

with a', b', c', d' coprime with p. Then

$$x + y = p^{\min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}} \cdot q \qquad (q \in \mathbb{Q}).$$

Applying property 2. from Definition 1.2 we obtain

$$\operatorname{ord}_p (x+y) = \operatorname{ord}_p \left(p^{\min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}} \cdot q\right) \geq \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}. \qquad \square$$

Using these functions we can define a field norm $|\ |_p\colon \mathbb{Q} \to \mathbb{Q}$ as follows:

$$|x|_p = \begin{cases} p^{-\operatorname{ord}_p x}, & \text{if } x \neq 0; \\ 0, & \text{otherwise;} \end{cases} .$$

Proposition 1.6. $|\ |_p$ *is a field norm on* $\mathbb{Q}$.

Proof. Property 1. is obvious.
To prove 2., given $x, y \in \mathbb{Q}^\times$ we know that $\operatorname{ord}_p xy = \operatorname{ord}_p x + \operatorname{ord}_p y$ so

$$|xy|_p = p^{-\operatorname{ord}_p xy} = p^{-\operatorname{ord}_p x - \operatorname{ord}_p y} = p^{-\operatorname{ord}_p x} \cdot p^{-\operatorname{ord}_p y} = |x|_p \cdot |y|_p.$$

To prove 3. let $x, y \in \mathbb{Q}^\times$; $\operatorname{ord}_p (x+y) \geq \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}$ so

$$\begin{aligned} |x+y|_p &= p^{-\operatorname{ord}_p (x+y)} \leq p^{-\min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}} = p^{\max\{-\operatorname{ord}_p x, -\operatorname{ord}_p y\}} \\ &= \max\left\{p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}\right\} = \max\left\{|x|_p, |y|_p\right\} \leq |x|_p + |y|_p. \end{aligned}$$

We actually proved a stronger inequality than 3., which is one of the key ingredients of p-adic analysis. □

Definition 1.7. A norm on X is called *non-Archimedean* if $\|x+y\| \leq \max\{\|x\|, \|y\|\}$ holds for every $x, y \in X$.

If $\|\ \|$ is a non-Archimedean norm on X, it's immediate to see that

$$\|n \cdot x\| \leq \|x\| \text{ for every } n \in \mathbb{N}, x \in X$$

which explains the name. We have already proved that $|\ |_p$ is a non-Archimedean norm on $\mathbb{Q}$ in Proposition 1.6.

Proposition 1.8. *If $\| \ \|$ is a non-Archimedean norm on X then*

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

Proof. We can assume that $\|x\| < \|y\|$. Then

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

but since $\|x\| < \|y\|$ we must have $\|x+y\| = \|y\|$. □

Definition 1.9. If (X,d) is a metric space, a sequence $(a_n)_{n\in\mathbb{N}}$ is a *Cauchy sequence* if $\forall \varepsilon > 0$ $\exists n_0 \in \mathbb{N}$ such that $n, m > n_0 \implies d(a_n, a_m) < \varepsilon$.

Definition 1.10. Two metrics d_1, d_2 on X are *equivalent* if every Cauchy sequence for d_1 is Cauchy for d_2 and vice-versa. Two norms are equivalent if they induce equivalent metrics.

Now we present a technical lemma we're going to need.

Lemma 1.11. *If $\alpha \in (0,1]$ the function on $\mathbb{Q}$ defined by $x \mapsto |x|^\alpha$ is a norm equivalent to $| \ |_\infty$.*

Proof. First of all we show $| \ |^\alpha$ is actually a norm; property 1. and 2. are easily verified. To prove 3. we have to show that $|x+y|^\alpha \leq |x|^\alpha + |y|^\alpha$ for every $x, y \in \mathbb{Q}^\times$. We can assume $0 < x < y$ and, dividing both sides by $|y|^\alpha$, we just need to prove $(1+t)^\alpha \leq 1 + t^\alpha$ for $t \in [0,1]$. This easily follows studying the first derivative of $[0,1] \ni t \mapsto 1 + t^\alpha - (1+t)^\alpha$ (always non negative if $0 \leq \alpha \leq 1$).
The equivalence of the two norms is easy to see if we use the above definition: let $(a_n)_n$ be Cauchy for $| \ |$; fixed $\varepsilon > 0$ we can find $n_0 \in \mathbb{N}$ such that $n, m > n_0 \implies |a_n - a_m| < \varepsilon^{\frac{1}{\alpha}}$ i.e. $|a_n - a_m|^\alpha < \varepsilon$ $\forall n, m > n_0$ so $(a_n)_n$ is also Cauchy for $| \ |^\alpha$ (and vice-versa). □

Generalizing a little bit the previous lemma we can prove that if $\| \ \|_1$ and $\| \ \|_2$ are two field norms on F which satisfy $\|x\|_1 = \|x\|_2^\alpha$ $\forall x \in F$ for a fixed $\alpha > 0$ then they're equivalent. For example, instead of defining $| \ |_p$ using $p^{-\operatorname{ord}_p a}$, we could have used $\rho \in (0,1)$ in place of $1/p$ and we would have obtained an equivalent norm because $p^{-\operatorname{ord}_p a} = \left(\rho^{\operatorname{ord}_p a}\right)^{-\log_\rho p}$.

Definition 1.12. The norm $\| \ \|$ such that $\|x\| = 1 - \delta_0^x$ is called *trivial*.

Finally we can prove the main theorem of this section.

Theorem 1.13 (Ostrowski)**.** *Every non-trivial norm $\| \ \|$ on $\mathbb{Q}$ is equivalent to $| \ |_p$ for some prime $p \in \mathbb{N}$ or for $p = \infty$.*

Proof. We distinguish two cases.
Case (1). There exists a positive integer n such that $\|n\| > 1$. Let n_0 be the minimum among those (for every field norm $\|\pm 1\| = 1$ so $n_0 > 1$). Since $\|n_0\| > 1$ there exists $\alpha = \log_{n_0}\|n_0\| > 0$ such that $\|n_0\| = n_0^\alpha$. Now if $n \in \mathbb{N}^\times$ then, using base n_0, we can write

$$n = a_0 + a_1 n + \cdots + a_s n_0^s, \qquad a_i \in \{0, 1, \ldots, n_0 - 1\}, a_s \neq 0.$$

Then, since norms are subadditive and multiplicative

$$\begin{aligned} \|n\| &\leq \|a_0\| + \|a_1 n_0\| + \cdots + \|a_s n_0^s\| = \\ &= \|a_0\| + \|a_1\| n_0^\alpha + \cdots + \|a_s\| n_0^{s\alpha}. \end{aligned}$$

Being n_0 the minimum positive integer with $\|n_0\| > 1$ we have $\|a_i\| \leq 1$ so

$$\|n\| \leq 1 + n_0^\alpha + \cdots + n_0^{s\alpha} \leq n_0^{s\alpha}(1 + n_0^{-\alpha} + \cdots + n_0^{-s\alpha}) \leq n^\alpha \left[\sum_{i=0}^{\infty} n_0^{-i\alpha}\right].$$

The last inequality is true because $n \geq n_0^s$. The series at the right side is a geometric one which converges to a certain $C < +\infty$ (since $0 < \frac{1}{n_0} < 1$). Now we have obtained

$$\|n\| \leq Cn^\alpha.$$

Using n^N, for some large $N \in \mathbb{N}$, in place of N in the last inequality, and then extracting Nth roots, leads us to

$$\|n\| \leq \sqrt[N]{C}n^\alpha.$$

Letting $N \to +\infty$ we get $\|n\| \leq n^\alpha$ (obviously this is valid for every $n \in \mathbb{N}$). To get the other verse of the inequality, using n written as above, we have $n_0^{s+1} > n \geq n_0^s$. Using reverse triangular inequality and the one we obtained above, we get

$$\|n\| \geq \left\|n_0^{s+1}\right\| - \left\|n_0^{s+1} - n\right\| \geq n_0^{(s+1)\alpha} - \left(n_0^{s+1} - n\right)^\alpha.$$

Since $n > n_0^s$

$$\|n\| \geq n_0^{(s+1)\alpha} - \left(n_0^{s+1} - n_0^s\right)^\alpha = n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right] \geq C'n^\alpha$$

with $C' := \left[1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right]$ that doesn't depend on n. As before, using n^N and taking Nth roots and letting $N \to +\infty$ gives $\|n\| \geq n^\alpha$. So we proved that $\|n\| = n^\alpha$ for every $n \in \mathbb{N}$. Using property 2. of norms and $\|-1\| = 1$ we get $\|q\| = |q|^\alpha$ for every $q \in \mathbb{Q}$. Now, using Lemma 1.11, we conclude that $\| \ \|$ is equivalent to $| \ |_\infty$.

Case (2). For every $n \in \mathbb{N}$, $\|n\| \leq 1$. Since $\| \ \|$ is non-trivial by hypothesis we can find the minimum $\mathbb{N} \ni n_0 > 1$ such that $\|n_0\| < 1$. Easily n_0 is a prime number: if not, $n_0 = a \cdot b$ with $1 < a, b < n_0$ and $1 > \|n_0\| = \|ab\| = \|a\|\|b\|$ so at least one from $\|a\|$ and $\|b\|$ must be strictly less than 1, absurd because $a, b < n_0$ and n_0 is the minimum positive integer with this property. Let $p = n_0$ and we claim that if q is a different prime from p $\|q\| = 1$. If this is not true then $\|q\| < 1$ and we can find some large $N \in \mathbb{N}$ such that $\left\|p^N\right\|, \left\|q^N\right\| < 1/2$. Since p^N and q^N are coprime, from Bézout identity there are $n, m \in \mathbb{Z}$ such that $np^N + mq^N = 1$, but this leads to a contradiction:

$$1 = \|1\| = \left\|np^N + mq^N\right\| \leq \|n\|\left\|p^N\right\| + \|m\|\left\|q^N\right\| \leq \left\|p^N\right\| + \left\|q^N\right\| < \frac{1}{2} + \frac{1}{2} < 1.$$

Now, given $n \in N$ we can factorize it in a unique way into prime divisors $n = p_1^{b_1} \cdots p_r^{b_r}$. At most one from the p_i-s is equal to p so if, wlog, $p_1 = p$ then $b_1 = \operatorname{ord}_p n$ and $\|p_i\| = 1$ if $i > 1$ so

$$\|n\| = \left\|p_1^{b_1} \cdot \dots \cdot p_r^{b_r}\right\| = \|p_1\|^{b_1} \cdot \dots \cdot \|p_r\|^{b_r} = \|p\|^{\operatorname{ord}_p n}.$$

Letting $\rho := \|p\| \in (0, 1)$ we obtain $\|a\| = \rho^{\operatorname{ord}_p a}$ for $a \in \mathbb{N}^\times$. Using property 2. of norms we can show this holds also if $a \in \mathbb{Q}^\times$. We conclude that $\| \ \|$ is equivalent to $| \ |_p$, using the general version of Lemma 1.11. □

The standard topology of $\mathbb{Q}$, induced by the euclidean metric, is very different from the p-adic topology, induced by the p-adic ultrametric. With the former, $\mathbb{Z} \subset \mathbb{Q}$ is a discrete set while, in p-adic environment, $\mathbb{Z}$ isn't discrete: 0 is an accumulation point, $\lim_{n\to+\infty} p^n = 0$. There are also some interesting algebraic properties, which we haven't in the standard topology, for example the one described in the following lemma.

Lemma 1.14. *For every $r > 0$ the set $B_{<r}(0) \cap \mathbb{Z} = \{x \in \mathbb{Z} \mid |x|_p < r\}$ is an ideal of the ring $\mathbb{Z}$, in the p-adic topology.*

Proof. It's clear that we can only consider the case $r = p^k$ with $k \in \mathbb{Z}$. If $k \geq 0$ the property is trivial since $\mathbb{Z} \subseteq B_{\leq 1}(0) = \{x \in \mathbb{Q} \mid |x|_p \leq 1\}$. Let's consider $x, y \in \mathbb{Z} \cap B_{<p^k}(0)$, i.e. $|x|_p, |y|_p < p^k$. We must show that $|x - y|_p < p^k$ and that for every $z \in \mathbb{Z}$ we have $z \cdot x \in B_{<p^k}(0) \cap \mathbb{Z}$. For the first property we have

$$|x - y|_p \leq \max\left\{|x|_p, |-y|_p\right\} = \max\left\{|x|_p, |y|_p\right\} < p^k$$

and for the second one, recalling that $\mathbb{Z} \ni z \implies |z|_p \leq 1$, we have

$$|z \cdot x|_p = |z|_p \cdot |x|_p \leq |x|_p < p^k. \qquad \square$$

These non-Archimedean norms $|\ |_p$ have some very strange properties, far from our intuition (which is based on euclidean norms). We'll explore them in detail in Section 3.1.

1.3 Construction of $\mathbb{Q}_p$

Definition 1.15. A metric space (X, d) is *complete* if every Cauchy sequence in X converges to some element in X.

Definition 1.16. If (X, d) is a metric space, $(\overline{X}, \overline{d})$ is its completion if it is a complete metric space which contains X as a dense subspace and satisfies this universal property: if Y is a complete metric space and $f\colon X \to Y$ is uniformly continuous then there exists a unique $f'\colon \overline{X} \to Y$ such that f' is uniformly continuous and $f'|_X = f$.

It's clear from the definition that the completion of a space is unique up to isometry.

Proposition 1.17. $(\mathbb{Q}, |\ |_p)$ *is not complete.*

Proof. This proof will heavily rely on the definition of $\mathbb{Z}_p$ proposed in Section 2.1, and on Hensel's lemma (Theorem 2.22). Obviously we don't need any result depending on this statement to build $\mathbb{Z}_p$ and prove the Hensel's lemma (in other words: this proof does not create any logical loop). We have to show that there exists a Cauchy sequence in $(\mathbb{Q}, |\ |_p)$ which has no limit in $\mathbb{Q}$. To do this, we'll use a polynomial $P(X) \in \mathbb{Z}[X] \subset \mathbb{Z}_p[X]$ which has no roots in $\mathbb{Q}$ but admits a root in $\mathbb{Z}/p\mathbb{Z}$. We'll then use Hensel's lemma to obtain $\xi \in \mathbb{Z}_p$ such that $P(\xi) = 0$. We'll then have a Cauchy sequence in $\mathbb{Z} \subset \mathbb{Q}$ (we can consider truncated sums of ξ) which converges to $\xi \notin \mathbb{Q}$. Let's distinguish four cases.

- $p = 2$:
  Let's consider the polynomial $P(X) = X^3 - 7 \in \mathbb{Z}[X]$: obviously there are no rational roots of P but $x_0 = 1$ is such that $P(x_0) \equiv 0 \mod 2$. We immediately see that $P'(X) = 3X^2$ so $2 \nmid 3 = P'(1)$ and, applying Hensel's lemma, we infer there is a unique $\xi \in \mathbb{Z}_2$ such that $P(\xi) = 0$.

- $p = 3$:
  Let's consider the polynomial $P(X) = X^2 - 7 \in \mathbb{Z}[X]$: obviously there are no rational roots of P but $x_0 = 1$ is such that $P(x_0) \equiv 0 \mod 3$. We immediately see that $P'(1) = 2 \not\equiv 0$ mod 3 and, applying Hensel's lemma, we infer there is a unique $\xi \in \mathbb{Z}_3$ such that $P(\xi) = 0$.

- $p \equiv 1 \mod 4$:
  Let's consider the polynomial $P(X) = X^2 - (p+1) \in \mathbb{Z}[X]$. We observe that P has no rational roots; writing $p + 1 = 4k + 2$ we immediately see that $p + 1$ is not a perfect square, because $2 \mid p + 1$ but $4 \nmid p + 1$. Clearly, $p + 1$ can't either be a square of some rational number: if it were, then we would have

$$p + 1 = \left(\frac{a}{b}\right)^2 \implies b^2 \cdot (p + 1) = a^2$$

which is an absurd, since $p+1$ is not a perfect square. So P has no roots in $\mathbb{Q}$, but we easily see that $P(1) \equiv 0 \mod p$ and $P'(1) = 2 \not\equiv 0 \mod p$. Applying Hensel's lemma we find $\xi \in \mathbb{Z}_p$ such that $P(\xi) = 0$.

- $p \equiv 3 \mod 4$:
  Let's consider $\left(\frac{p-1}{2}\right)^2 \equiv 4^{-1} \mod p$ and let $t \in \{0, \dots, p-1\}$ such that $4t \equiv 1 \mod p$. Obviously $0 \neq t$ is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$; we claim that $\sqrt{t} \notin \mathbb{Q}$. We just need to show that t is not a perfect square (then we can use the same reasoning of the previous point). First of all, with a little abuse of notation, we observe that
  $$\mathbb{F}_p^2 = \left\{ x^2 \,\middle|\, 0 \leq x \leq \frac{p-1}{2}, x \in \mathbb{N} \right\}.$$
  Since the only perfect squares less than p are exactly $\left\{ x^2 \,\middle|\, 0 \leq x \leq \lfloor \sqrt{p} \rfloor, x \in \mathbb{N} \right\}$ and $\frac{p-1}{2} \geq \sqrt{p}$ for $p \geq 7$, we infer that t cannot be a perfect square.
  Now we can consider the polynomial $P(X) = X^2 - t \in \mathbb{Z}[X]$: we know that it has no rational root but $x_0 = -2^{-1}$ is a root of P in $\mathbb{Z}/p\mathbb{Z}$, by construction. Obviously $P'(X) = 2X$ so $P'(x_0) = 2x_0 \not\equiv 0 \mod p$. Then we can apply Hensel's lemma and obtain $\xi \in \mathbb{Z}_p$ such that $P(\xi) = 0$. □

Actually, if $p \neq 2$, there is an easier way to prove $(\mathbb{Q}, |\ |_p)$ is not complete, using the Cauchy sequence $(a^{p^n})_{n \in \mathbb{N}}$, where $a \in \{1, \dots, p-2\}$. The proof can be found at [7, p. 3]. Anyway the proof we gave is indeed a nice application of the Hensel's lemma.

The goal of this section is to build $\mathbb{Q}_p$, the completion field of $(\mathbb{Q}, |\ |_p)$ with p a fixed prime. The building process is analogue to the construction of $\mathbb{R}$, the completion of $(\mathbb{Q}, |\ |_\infty)$ and it's actually the "standard" way to complete a metric space. This process is actually necessary, because $(\mathbb{Q}, |\ |_p)$ is not complete, so it's a very unfriendly setting to perform analysis.

Definition 1.18. Let $\mathcal{S} := \left\{ (a_n)_{n \in \mathbb{N}} \subseteq \mathbb{Q} \,\middle|\, (a_n)_{n \in \mathbb{N}} \text{ Cauchy for } |\ |_p \right\}$. Then
$$\mathbb{Q}_p := \mathcal{S}/\sim$$
where $\sim$ is a relation on $\mathcal{S}$: $(a_n)_n \sim (b_n)_n$ if $|a_i - b_i|_p \to 0$ as $i \to +\infty$.

Proposition 1.19. *$\mathbb{Q}_p$ is well defined and there's a natural sum and product on $\mathbb{Q}_p$ which makes $(\mathbb{Q}_p, +, \cdot)$ a field.*

Proof. $\mathbb{Q}_p$ is well defined, in the sense that $\sim$ is an equivalence relation on $\mathcal{S}$ (easy to verify). First of all we can immerge $\mathbb{Q}$ in $\mathcal{S}$ (and then in $\mathbb{Q}_p$) sending x to $\{x\}$, the constant sequence (it's immediate that $\{x'\} \sim \{x\} \iff x = x'$ so this is really an immersion). From now on we'll do a little abuse of notation, not to result too pedantic: 0 will denote both $\{0\}$ (the constant sequence) and $[\{0\}]$ (its equivalence class), context will clarify which is the right meaning.
There's a natural extension of the classical sum and product on $\mathbb{Q}$ to $\mathbb{Q}_p$, which makes it a field. Let $a, b \in \mathbb{Q}_p$, we define $a + b := [(a_n + b_n)_n]$ where $(a_n)_n, (b_n)_n$ are two representatives of a and b respectively. It is easy to see that this is well defined: the sum of two Cauchy is still a Cauchy and $a + b$ doesn't depend on the choice of the representatives. Similarly the product of $a \cdot b := [(a_n \cdot b_n)_n]$ is well defined: product of two Cauchy is Cauchy and given $(a'_n)_n \sim (a_n)_n$ and $(b'_n)_n \sim (b_n)_n$ we have
$$0 \leq \lim_{i \to +\infty} \left| a_i b_i - a'_i b'_i \right|_p = \lim_{i \to +\infty} \left| a_i (b_i - b'_i) + b'_i (a_i - a'_i) \right|_p \leq$$
$$\leq \lim_{i \to +\infty} |a_i|_p \left| b_i - b'_i \right|_p + \lim_{i \to +\infty} \left| b'_i \right|_p \left| a_i - a'_i \right|_p = 0$$

where we used that if $(a_n)_n$ is Cauchy then it is bounded in norm. Then the definition doesn't depend on the choice of the representatives (the first claim above can be proved in the exact same way).
It's easy to see $(\mathbb{Q}_p, +)$ is a group, because 0 is the neutral element and additive inverses are defined in the trivial way. To see that also $(\mathbb{Q}_p^\times, \cdot)$ is a group let's first note that every sequence $(a_n)_n$ is equivalent to $(a'_n)_n$ where $a'_i = p^i$ if $a_i = 0$ and $a'_i = a_i$ otherwise. Associativity holds and the neutral element is $1 = [\{1\}] \neq 0$. The only non-trivial property to prove is the existence of multiplicative inverses: if $a \neq 0$ then if $a = [(a_n)_n]$ (where $(a_n)_n$ is chosen without zeros) then $1/a = [(1/a_n)_n]$. We have to show that $(1/a_n)_n$ is Cauchy: let $N \in \mathbb{N}$ large enough such that $\exists \varepsilon > 0$ and $|a_n|_p > \varepsilon \ \forall n > N$ (see proof of Proposition 1.20) and that $n, m > N \implies |a_n - a_m|_p < \varepsilon^3$; if $n, m > N$ we obtain

$$\left|\frac{1}{a_n} - \frac{1}{a_m}\right|_p = \left|\frac{a_m - a_n}{a_n a_m}\right|_p = \frac{1}{|a_n a_m|_p}|a_m - a_n|_p \leq \frac{1}{\varepsilon^2}\varepsilon^3 = \varepsilon.$$

Using the same exact technique we can prove that $1/a$ is well defined, i.e. if $(a_n)_n$ and $(a'_n)_n$ are both non-zero representatives of a then $(1/a_n)_n \sim (1/a'_n)_n$. Obviously this product is abelian. It is also easy to prove that distributivity holds, i.e. given $a, b, c \in \mathbb{Q}_p$ $a \cdot (b + c) = a \cdot b + a \cdot c$ (it's sufficient to note that $a \cdot (b + c) = [(a_n \cdot (b_n + c_n))_n] = [(a_n \cdot b_n + a_n \cdot c_n)_n]$). So we have finally proved that $(\mathbb{Q}_p, +, \cdot)$ is a field, containing $\mathbb{Q}$ as a subfield (the immersion defined at the beginning is in-fact a ring morphism between $\mathbb{Q}$ and $\mathbb{Q}_p$, representing the natural identification of $\mathbb{Q}$ in $\mathbb{Q}_p$). □

We have then to extend the norm $|\ |_p$ to $\mathbb{Q}_p$: if $a \in \mathbb{Q}_p$ then $|a|_p := \lim_{i\to+\infty}|a_i|_p$ where $(a_n)_n$ is any representative of a.

Proposition 1.20. $|\ |_p$ *is a norm on* $\mathbb{Q}_p$.

Proof. First of all we prove that, chosen a representative $(a_n)_n$ of a, $\exists \lim_{i\to+\infty}|a_i|_p$. We have two cases:

1. if $a = 0$, by definition, $\lim_{i\to+\infty}|a_i|_p = 0$;

2. if $a \neq 0$ then $(a_n)_n \nsim 0$ so $\exists \varepsilon > 0$ and for every $N \in \mathbb{N}$ there exists $i_N > N$ such that $|a_{i_N}|_p > \varepsilon$. Since $(a_n)_n$ is Cauchy, choosing N large enough such that $|a_i - a_j|_p < \varepsilon$ $\forall i, j > N$ we have that $|a_i - a_{i_N}|_p < \varepsilon \ \forall i > N$. Using the isosceles triangle principle we get $|a_i|_p = |a_{i_N}|_p$ for every $i > N$, so trivially the limit exists.

Now we prove that this is well defined, i.e. $|a|_p$ doesn't depend on the choice of the representative of a. Let $(a_n)_n, (b_n)_n$ two representatives of a, then $(a_n)_n \sim (b_n)_n$ which means $\lim_{i\to+\infty}|a_i - b_i|_p = 0$. Now by the reverse triangular inequality

$$0 \leq \lim_{i\to+\infty}\left||a_i|_p - |b_i|_p\right| \leq \lim_{i\to+\infty}|a_i - b_i|_p = 0 \implies \lim_{i\to+\infty}|a_i|_p = \lim_{i\to+\infty}|b_i|_p.$$

The property 1. of norms is proved in the case above. Property 2. and 3. immediately follows from the ones of $|\ |_p$ on $\mathbb{Q}$ and basic limit rules. □

Proposition 1.21. $(\mathbb{Q}_p, |\ |_p)$ *is complete.*

Proof. We have to prove that if $(a_n)_n$ is a Cauchy sequence in $\mathbb{Q}_p$ for $|\ |_p$ then there exists $a \in \mathbb{Q}_p$ such that $a = \lim_{i\to+\infty} a_i$. Let $a_n = [(a_{n,m})_{m\in\mathbb{N}}]$ where $(a_{n,m})_m$ is a Cauchy sequence in $\mathbb{Q}$. Let $N_j \in \mathbb{N}$ such that $\forall\ n, m > N_j$ $|a_{j,m} - a_{j,n}|_p < 1/j$. Now, choosing $k_j > \max\{N_j, k_{j-1}\}$, we claim that $[(a_{n,k_n})_n] \in \mathbb{Q}_p$ is the limit of the sequence at the beginning. First of all we prove that $(a_{n,k_n})_n$ is a Cauchy sequence in $\mathbb{Q}$:

$$\begin{aligned} |a_{n,k_n} - a_{m,k_m}|_p &= |a_{n,k_n} - a_{n,j} + a_{n,j} - a_{m,j} + a_{m,j} - a_{m,k_m}|_p \leq \\ &\leq \max\left\{|a_{n,k_n} - a_{n,j}|_p, |a_{n,j} - a_{m,j}|_p, |a_{m,j} - a_{m,k_m}|_p\right\}. \end{aligned}$$

Choosing a large enough $j \in \mathbb{N}$ we obtain $|a_{n,k_n} - a_{n,j}|_p < 1/n$ and $|a_{m,j} - a_{m,k_m}|_p < 1/m$. Since $(a_n)_n \subseteq \mathbb{Q}_p$ is a Cauchy sequence, for every $\varepsilon > 0$ $\exists N \in N$ such that $n, m > N \implies |a_n - a_m|_p < \varepsilon$, meaning $\lim_{j\to+\infty}|a_{n,j} - a_{m,j}|_p < \varepsilon$. From here we can see that $\exists N' \in \mathbb{N}$ such that $j > N' \implies |a_{n,j} - a_{m,j}|_p < \varepsilon$ so we can also control the other term above. We proved that $(a_{n,k_n})_n$ is a Cauchy sequence.
Now we show that its equivalence class, let it be $a \in \mathbb{Q}_p$, is actually the limit of $(a_n)_n$, i.e.

$$0 = \lim_{n\to+\infty}|a_n - a|_p = \lim_{n\to+\infty}\left(\lim_{j\to+\infty}\left|a_{n,j} - a_{j,k_j}\right|_p\right).$$

Fixed $\varepsilon > 0$ we know that $\exists N \in \mathbb{N}$ such that $n, m > N \implies |a_{n,k_n} - a_{m,k_m}|_p < \varepsilon$. Choosing $\mathbb{N} \ni n > \max\{N, 1/\varepsilon\}$ we have

$$\left|a_{n,j} - a_{j,k_j}\right|_p \leq \max\left\{|a_{n,j} - a_{n,k_n}|_p, \left|a_{n,k_n} - a_{j,k_j}\right|_p\right\}.$$

If $j > \max\{k_n, N\}$ then $|a_{n,j} - a_{n,k_n}|_p < 1/n < \varepsilon$ and $\left|a_{n,k_n} - a_{j,k_j}\right|_p < \varepsilon$ so

$$\lim_{j\to+\infty}\left|a_{n,j} - a_{j,k_j}\right|_p \leq \varepsilon.$$

Thesis easily follows from the fact that ε is arbitrary. □

Proposition 1.22. *$\mathbb{Q}$ is dense in $\mathbb{Q}_p$.*

Proof. Chosen $a = [(a_n)_n] \in \mathbb{Q}_p$ and $\varepsilon > 0$ we know that $\exists N \in \mathbb{N}$ such that $n > m > N \implies |a_n - a_m|_p < \varepsilon$. Now, fixed $n \in \mathbb{N}$ we have that $a_n \in \mathbb{Q}$ is identified with $a' = \{a_n\} \in \mathbb{Q}_p$, the equivalence class of the constant sequence $(a_n, a_n, a_n, \dots)$. Now $|a - a'|_p = \lim_{j\to+\infty}|a_j - a_n|_p$ which is clearly no bigger than ε (we can consider $j > N$). □

Up to now we have proved that $(\mathbb{Q}_p, |\ |_p)$ is actually the completion of $(\mathbb{Q}, |\ |_p)$. Obviously we're not going to work using this abstract construction, thanks to the following result.
First we'll need a technical lemma.

Lemma 1.23. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$ then $\forall i \in \mathbb{N}$ $\exists \alpha \in \mathbb{Z}$ such that $|\alpha - x|_p \leq p^{-i}$. The integer α can be chosen in $\{0, 1, \dots, p^i - 1\}$.*

Proof. Let $x = a/b$ written in lowest terms. The fact that $|x|_p \leq 1$ means exactly $p \nmid b$ so, since p is a prime number, p^i and b are coprime; thanks to Bézout identity $\exists m, n \in \mathbb{Z}$ $mb + np^i = 1$. Letting $\mathbb{Z} \ni \alpha := am$ we get

$$|\alpha - x|_p = \left|am - \frac{a}{b}\right|_p = \left|\frac{a}{b}\right|_p |mb - 1|_p \leq |mb - 1|_p = \left|np^i\right|_p = \frac{|n|_p}{p^i} \leq \frac{1}{p^i}$$

since $|x|_p = |a/b|_p \leq 1$ and $|n|_p \leq 1$ if $n \in \mathbb{Z}$. Adding the right multiple of p^i to α we can get an integer between 0 and $p^i - 1$ still satisfying the above inequality. □

Theorem 1.24. *Every $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$ has exactly one representative $(a_i)_{i\in\mathbb{N}}$ such that for every $i \in \mathbb{N}$:*

1. $a_i \in \{0, 1, \dots, p^{i+1} - 1\}$*;*

2. $a_i \equiv a_{i+1} \mod p^{i+1}$.

Proof. We first prove uniqueness: let $(a'_i)_i$ a different sequence satisfying *1.* and *2.* If $a_{i_0} \neq a'_{i_0}$ then $a_{i_0} \not\equiv a'_{i_0} \mod p^{i_0+1}$ since they are both between 0 and p^{i_0+1}. Now if $i \geq i_0$ we have

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \mod p^{i_0+1} \implies \left|a_i - a'_i\right|_p > \frac{1}{p^{i_0+1}},$$

meaning $(a'_i)_i \nsim (a_i)_i$.
Now we prove existence. Let $(b_i)_i$ be any of the representatives of a and let $N(j) \in \mathbb{N}$ such that $n, m \geq N(j) \implies |b_n - b_m|_p \leq p^{-j-1}$ for every $j \in \mathbb{N}$. We can choose the sequence $(N(j))_{j\in\mathbb{N}} \subseteq \mathbb{N}$ strictly increasing with j, in particular with $N(j) > \max\{j, N(j-1)\}$. We immediately note that if $i \geq N(0)$ then $|b_i|_p \leq 1$ because for every $j \geq N(0)$

$$|b_i|_p \leq \max\left\{|b_j|_p, |b_i - b_j|_p\right\} \leq \max\left\{|b_j|_p, \frac{1}{p}\right\}$$

and $\lim_{j\to+\infty}|b_j|_p = |a|_p \leq 1$. Using Lemma 1.23 we can find $a_j \in \mathbb{Z}$ such that $0 \leq a_j < p^{j+1}$ and $\left|a_j - b_{N(j)}\right|_p \leq 1/p^{j+1}$, because $\left|b_{N(j)}\right|_p \leq 1$. We'll show that $(a_n)_n$ is the desired sequence. Obviously it's Cauchy because

$$|a_n - a_m|_p \leq \max\left\{\left|a_n - b_{N(n)}\right|_p, \left|b_{N(n)} - b_{N(m)}\right|_p, \left|b_{N(m)} - a_m\right|_p\right\}$$

and, choosing n, m large enough, we can control all those three terms. Property *1.* is already verified by construction so we have only to prove that $a_{j+1} \equiv a_j \mod p^{j+1}$ and that $(a_n)_n \sim (b_n)_n$. The former follows from

$$\begin{aligned}|a_{j+1} - a_j|_p \leq \max\left\{\left|a_{j+1} - b_{N(j+1)}\right|_p, \left|b_{N(j+1)} - b_{N(j)}\right|_p, \left|b_{N(j)} - a_j\right|_p\right\} \leq \\ \leq \max\left\{\frac{1}{p^{j+2}}, \frac{1}{p^{j+1}}, \frac{1}{p^{j+1}}\right\} \leq \frac{1}{p^{j+1}}.\end{aligned}$$

To prove the latter, for every j, if $i > N(j)$ we have

$$\begin{aligned}|a_i - b_i|_p \leq \max\left\{|a_i - a_j|_p, \left|a_j - b_{N(j)}\right|_p, \left|b_{N(j)} - b_i\right|_p\right\} \leq \\ \leq \max\left\{\frac{1}{p^{j+1}}, \frac{1}{p^{j+1}}, \frac{1}{p^{j+1}}\right\} = \frac{1}{p^{j+1}}\end{aligned}$$

because $a_i \equiv a_{i+1} \equiv a_{i+2} \equiv \cdots \equiv a_j \mod p^{i+1}$. So $\lim_{j\to+\infty}|a_j - b_j|_p = 0$, i.e. $(a_i)_i \sim (b_i)_i$. □

So we have a "canonical" representative for every $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$, let it be $(a_n)_n$. Since $a_i \in \{0, 1, \dots, p^{i+1} - 1\}$ we can write it using base p, i.e.,

$$a_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_i p^i$$

where $b_i \in \{0, 1, \dots, p-1\}$. Property *2.* of Theorem 1.24 tells us exactly that

$$a_{i+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_i p^i + b_{i+1} p^{i+1}$$

i.e. the first $i+1$ digits (from b_0 to b_i) are the same, because $|a_{i+1} - a_i|_p \leq 1/p^{i+1}$. So we can write, just as a notation,

$$a = \sum_{i=0}^{+\infty} b_i p^i = b_0 + b_1 p + b_2 p^2 + \dots$$

the so called p-adic expansion of a. It's easy to see that $|a|_p = p^{-k}$ where k is the minimum integer such that $b_k \neq 0$ ($k = +\infty$ if $a = 0$). This notation makes sense only if $|a|_p \leq 1$ but it can be used for every element of $\mathbb{Q}_p$ with a little refinement: let $a' \in \mathbb{Q}_p$ with $|a'|_p = p^m > 1$ ($m \in \mathbb{N}^\times$); then $|p^m a'|_p = |p^m|_p |a'|_p = 1$ so we can expand it like before

$$p^m a' = \sum_{i=0}^{+\infty} b_i p^i$$

and multiplying both sides by p^{-m} we obtain

$$a' = p^{-m} \sum_{i=0}^{+\infty} b_i p^i = \sum_{i=0}^{+\infty} b_i p^{i-m} = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + \ldots$$

which can be thought as a p-adic expansion with a finite number of decimal digits. So we have a unique canonical way to write every element of $\mathbb{Q}_p$, which is way more practical than the abstract description. For example it is now easy to actually perform arithmetic operations: sum, difference, multiplication and division can be done applying the exact same algorithm that we use to perform them between integers, except that now we have to proceed with infinite digits (and actions like "carrying" or "borrowing" work from left to right).

Definition 1.25. Given $a, b \in \mathbb{Q}_p$ and $n \in \mathbb{N}^\times$ we say that $a \equiv b \mod p^n$ if $|a - b|_p \leq 1/p^n$.

It's easy to check that if $a, b \in \mathbb{Z}$ this definition is exactly the old-fashioned congruence.

Definition 1.26. $\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \;\middle|\; |x|_p \leq 1 \right\}$ is called the set of *p-adic integers*.

It's easy to verify that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$ (immediate from properties of $|\ |_p$). Its invertible elements are exactly

$$\mathbb{Z}_p^\times = \left\{ x \in \mathbb{Z}_p \;\middle|\; \frac{1}{x} \in \mathbb{Z}_p \right\} = \{ x \in \mathbb{Z}_p \mid x \not\equiv 0 \mod p \} = \left\{ x \in \mathbb{Z}_p \;\middle|\; |x|_p = 1 \right\}.$$

We can now justify our initial notations, which is actually a "real" equality and not just a way to write things, thanks to the following lemma.

Lemma 1.27. *Let $(c_i)_i \subseteq \mathbb{Q}_p$ such that $\lim_{i \to +\infty} c_i = 0$. Then the series*

$$\sum_{i=0}^{+\infty} c_i$$

converges in $\mathbb{Q}_p$.

Proof. We need to show that the sequence of partial sums converge, i.e. $(S_n)_n \subseteq \mathbb{Q}_p$ has limit, where $S_n := c_0 + c_1 + \cdots + c_n$. Since $\mathbb{Q}_p$ is complete it's sufficient to prove $(S_n)_n$ is Cauchy. Fixed $\varepsilon > 0$ $\exists N \in \mathbb{N}$ such that $i > N \implies |c_i|_p < \varepsilon$; so if $n, m > N$ we have

$$|S_n - S_m|_p = |c_{n+1} + \cdots + c_m|_p \leq \max\left\{ |c_{n+1}|_p, \ldots, |c_m|_p \right\} < \varepsilon$$

so $(S_n)_n$ is Cauchy. □

We can use this lemma with $c_i = b_i p^{i-m}$, for $m \in \mathbb{N}$ and $b_i \in \{0, 1, \ldots, p^i - 1\}$, because $|c_i|_p = |b_i|_p |p^{i-m}|_p \leq 1 \cdot p^{m-i} \to 0$ as $i \to +\infty$. We conclude that every p-adic expansion

$$\sum_{i=0}^{+\infty} b_i p^{i-m}$$

actually converges to some element in $\mathbb{Q}_p$ (and, clearly, our notation is coherent). This lemma is also a much cleaner results on series: they converge if and only if the general term approaches zero, unlike in $(\mathbb{R}, | \ |_\infty)$ where there are divergent series like $1 + \frac{1}{2} + \frac{1}{3} + \cdots = \sum_{n=1}^{+\infty} 1/n$. There is a very nice result about p-adic expansions: while the writing of rational numbers using base 10 is not unique ($0.99999\ldots = 1$), in $\mathbb{Q}_p$ p-adic expansions are unique, i.e. if two expansions have different digits they converge to totally different numbers.

Lemma 1.28. *Given $a = p^k \sum_{i=0}^{+\infty} a_i p^i \in \mathbb{Q}_p$, its p-adic expansion is periodic, i.e. $\exists r, N \in \mathbb{N}$ such that $a_i = a_{i+r}$ for every $i > N$, if and only if $a \in \mathbb{Q}$.*

Proof. To see that every periodic p-adic number is rational we can write

$$a = \sum_{i=-k}^{+\infty} a_i p^i = (a_{-k}p^{-k} + \cdots + a_{m-1}p^{m-1}) + p^m \sum_{i=0}^{+\infty} (b_0 + b_1 p + \cdots + b_{n-1}p^{n-1})p^{in}$$

with the obvious meaning: $\mathbb{Q} \ni q := a_{-k}p^{-k} + \cdots + a_{m-1}p^{m-1}$ is the anti-period and $(b_0, \ldots, b_{n-1})$ is the period. It is an easy calculation to verify that if $\alpha \in \mathbb{N}^\times$

$$\sum_{i=0}^{+\infty} p^{i\alpha} = \frac{1}{1 - p^\alpha}.$$

Using this identity we get

$$a = q + (b_0 + b_1 p + \cdots + b_{n-1}p^{n-1}) \cdot p^m \cdot \sum_{i=0}^{+\infty} p^{in} = q + (b_0 + b_1 p + \cdots + b_{n-1}p^{n-1}) \cdot \frac{p^m}{1 - p^n}$$

which is clearly in $\mathbb{Q}$.
To prove that every $q \in \mathbb{Q}$ has a periodic p-adic expansion we'll need a little more work. First of all let's note that if $a \in \mathbb{Q}_p$ admits a periodic representation also $-a$ admits one: given

$$a = \sum_{i=-k}^{+\infty} a_i p^i = (a_{-k}p^{-k} + \cdots + a_{m-1}p^{m-1}) + p^m \sum_{i=0}^{+\infty} (b_0 + b_1 p + \cdots + b_{n-1}p^{n-1})p^{in}$$

we have

$$\begin{aligned} -a = {} & (p - a_{-k})p^{-k} + (p - 1 - a_{-k+1})p^{-k+1} + \cdots + (p - 1 - a_{m-1})p^{m-1} + \\ & + p^m \sum_{i=0}^{+\infty} \left[(p - 1 - b_0) + (p - 1 - b_1)p + \cdots + (p - 1 - b_{n-1})p^{n-1} \right] p^{in} \end{aligned}$$

i.e. the period is $(p - 1 - b_0, p - 1 - b_1, \ldots, p - 1 - b_n)$ (the relation above is true if a admits a non zero anti-period, but it's almost the same if it does not).
Now let $\mathbb{Q} \ni a/b = p^k \cdot (t/s)$ with $p \nmid ts$. We'll show that t/s admits a periodic expansion (then we can conclude immediately). Since p is prime $p \nmid ts \implies p \nmid s$ so p and s are coprime and, thanks to Euler's theorem, $1 - p^{\varphi(s)} = \alpha s$ with $\alpha \in \mathbb{Z}_{\leq 0}$ (where φ is the Euler's totient function). So we have

$$\frac{t}{s} = \frac{\alpha t}{1 - p^{\varphi(s)}} = \alpha t \cdot \left(\frac{1}{1 - p^{\varphi(s)}} \right).$$

Now it's sufficient to prove that $|\alpha t|/(1 - p^{\varphi(s)})$ is periodic (because sign doesn't matter). As said before we know that $(1 - p^{\varphi(s)})^{-1} = \sum_{i=0}^{+\infty} p^{\varphi(s)i}$ and that $|\alpha t| \in \mathbb{N}$ has a finite p-adic expansion (i.e. definitively zero). It's easy to see that also their product is periodic. □

Using this characterization of $\mathbb{Q}$ in $\mathbb{Q}_p$ we can give another proof (a posteriori) of the non-completeness of $(\mathbb{Q}, | \ |_p)$. Obviously, this proof is much easier than the proof of Proposition 1.17, because it already uses the structure of $\mathbb{Q}_p$.

Proposition 1.29. $(\mathbb{Q}, |\ |_p)$ *is not complete.*

Proof. Using the density of $\mathbb{Q}$ in $\mathbb{Q}_p$, proved in Proposition 1.22, we just need to find some element $e \in \mathbb{Q}_p \setminus \mathbb{Q}$, because then we'll have a Cauchy sequence in $(\mathbb{Q}, |\ |_p)$ which doesn't converge to any rational. Thanks to Lemma 1.28 we know that every element of $\mathbb{Q}$ corresponds to a periodic expansion in $\mathbb{Q}_p$ and vice-versa, so e can be every infinite p-adic expansion which is not periodic, like for example

$$e = 1 + p^2 + p^4 + p^8 + \cdots = \sum_{i=0}^{+\infty} p^{2^i}. \qquad \square$$

2 Algebraic Approach

In this chapter we present some different approaches to the construction of $\mathbb{Z}_p$ and $\mathbb{Q}_p$, definitely with a more algebraic flavour.

2.1 Definition and algebraic properties of $\mathbb{Z}_p$

Definition 2.1. A p-adic integer is a formal series $\sum_{i\geq 0} a_i p^i$ with integral coefficients $0 \leq a_i \leq p-1$.

The set $\mathbb{Z}_p$ contains all the so called p-adic integers and is easily identified with

$$\prod_{i\geq 0}\{0,1,\dots,p-1\} = \{0,1,\dots,p-1\}^{\mathbb{N}}$$

which is clearly not countable. We have a natural embedding $\mathbb{N} \hookrightarrow \mathbb{Z}_p$ just writing every number in base p.
We can define addition between two p-adic integer in a component-wise way with a carry system: given $a, b \in \mathbb{Z}_p$ the first component of the sum is $a_0 + b_0$ if it's less than p, or $a_0 + b_0 - p$ otherwise and, in this case, we add a carry to the component of p and so on. Here's a quick example:

$$\begin{gathered}
1 = 1 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \dots \\
x = (p-1) \cdot p^0 + (p-1) \cdot p^1 + (p-1) \cdot p^2 + \dots = \sum_{i\geq 0}(p-1)p^i \\
1 + x = 0 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \dots = 0 \\
\implies -1 = \sum_{i\geq 0}(p-1)p^i.
\end{gathered}$$

This sum admits inverse in $\mathbb{Z}_p$, given $a = \sum_{i\geq 0} a_i p^i$ we define $b := \sigma(a) = \sum_{i\geq 0}(p-1-a_i)p^i \in \mathbb{Z}_p$ so $a + b + 1 = 0$, i.e. $-a = \sigma(a) + 1$. So $(\mathbb{Z}_p, +)$ is an abelian group (easy to verify) and with an involution $\sigma\colon \mathbb{Z}_p \to \mathbb{Z}_p$ ($\sigma^2 = id$).
We can also define a product on $\mathbb{Z}_p$, multiplying the two expansions in a Cauchy way (exactly like the multiplication between polynomials) and using a system of carries to keep the digits in $\{0,1,\dots,p-1\}$. This procedure is simply the classical multiplication of natural integers written in base p, pursued indefinitely. For example

$$-1 = (p-1)\sum_{i\geq 0} p^i \ , \ -(p-1)\sum_{i\geq 0} p^i = 1 \ , \ \sum_{i\geq 0} p^i = \frac{1}{1-p}$$

which shows that $1 - p \in \mathbb{Z}_p$ is invertible. Not every element of $\mathbb{Z}_p$ admits inverse, for example p is not invertible because

$$p \cdot \sum_{i\geq 0} a_i p^i = a_0 p + a_1 p^2 + \dots \neq 1 + 0p + 0p^2 + \dots = 1.$$

Then $\mathbb{Z}_p$ equipped with these two operations is a commutative ring. We can now extend $\mathbb{N} \hookrightarrow \mathbb{Z}_p$ to $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, which is a ring injective homomorphism so we immediately deduct that $\mathrm{char}(\mathbb{Z}_p) = 0$.

Proposition 2.2. *The ring $\mathbb{Z}_p$ is an integral domain.*

Proof. Given $a = \sum_{i\geq 0} a_i p^i \neq 0, b = \sum_{i\geq 0} b_i p^i \neq 0$ we have that $ab = \sum_{i\geq 0} c_i p^i \neq 0$: infact if a_v, b_w are the first non zero coefficients of a and b then $p \nmid a_v, p \nmid b_w \implies p \nmid a_v b_w$ which means that $c_{v+w} = a_v b_w \neq 0$. □

Let us emphasize the importance of p being a prime number: in the last proposition we used the fact that $\mathbb{Z}/p\mathbb{Z}$ is a domain and this is obviously false if p isn't a prime. If we choose to work with n-adic integers, with n being a composite integer, then, since $\mathbb{Z}/n\mathbb{Z}$ is not a domain, we obtain that also $\mathbb{Z}_n$ is not a domain, i.e. there are divisors of zero, so we can't even talk about the quotient field.

Example 2.3. Here's an example with $n = 10$, using the definition of $\mathbb{Z}_p$ given in Theorem 2.17:

$$u = (u_n)_n \in \varprojlim \mathbb{Z}/10^n\mathbb{Z} \qquad u_n := 2^{5^n} \mod 10^n,$$
$$v = (v_n)_n \in \varprojlim \mathbb{Z}/10^n\mathbb{Z} \qquad v_n := 5^{2^n} \mod 10^n.$$

It can be proved by induction that

$$u_n = 2^{5^n} \equiv 2^{5^{n-1}} = u_{n-1}, \qquad v_n = 5^{2^n} \equiv 5^{2^{n-1}} = v_{n-1} \mod 10^{n-1}$$

so our definitions are coherent. Obviously $u, v \neq 0$ but it's easily seen that $u \cdot v = 0$: infact $u_n \cdot v_n \equiv 0 \mod 10^n$ (we recall that products in the projective limit are done component-wise). More facts about 10-adic integers can be found at [5].

We can define $\operatorname{ord}_p : \mathbb{Z}_p \to \mathbb{N} \cup \{\infty\}$ as follows

$$\operatorname{ord}_p a := \begin{cases} +\infty, & \text{if } a = 0; \\ v, & \text{otherwise}; \end{cases}$$

where v is the minimum integer such that $a_v > 0$. It's easily seen that ord_p behaves exactly like a discrete valuation.
Called $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the field with p elements, the map $a = \sum_{i\geq 0} a_i p^i \mapsto a_0 \mod p$ is a ring homomorphism $\varepsilon\colon \mathbb{Z}_p \to \mathbb{F}_p$, which is obviously surjective and with kernel $p\mathbb{Z}_p = \{\, a \in \mathbb{Z}_p \mid a_0 = 0 \,\}$. Then $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{F}_p$ so $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$.

Proposition 2.4. *The group of invertible elements in $\mathbb{Z}_p$ is $\mathbb{Z}_p^\times = \left\{ \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p \,\middle|\, a_0 \neq 0 \right\}$.*

Proof. If $a \in \mathbb{Z}_p$ is invertible also its reduction $\varepsilon(a) \in \mathbb{F}_p$ must be, so we obtain

$$\mathbb{Z}_p^\times \subseteq \left\{ \sum_{i\geq 0} a_i p^i \in \mathbb{Z}_p \,\middle|\, a_0 \neq 0 \right\}.$$

The other inclusion can be proved, but, for brevity, we'll show it using an equivalent definition of $\mathbb{Z}_p$. □

Corollary 2.4.1. *Every non-zero p-adic integer $a \in \mathbb{Z}_p$ has a canonical representation $a = p^v u$ where $v = ord_p a$ and $u \in \mathbb{Z}_p^\times$ is a p-adic unit.*

Proposition 2.5. *The ring $\mathbb{Z}_p$ is a principal ideal domain whose ideals are $\{0\}$ and $p^k\mathbb{Z}_p := \{\, x \in \mathbb{Z}_p \mid \operatorname{ord}_p x \geq k \,\}$ for $k \in \mathbb{N}$.*

Proof. Let $I \neq 0$ be a nonzero ideal a $\mathbb{Z}_p$. Chosen $0 \neq a \in I$ an element of minimal order, we have $a = p^k u$ with $u \in \mathbb{Z}_p^\times$ so $p^k = a \cdot u^{-1} \in I$ which implies $p^k\mathbb{Z}_p = (p^k) \subseteq I$. Conversely if $b \in I$ then $w = \operatorname{ord}_p b \geq k$ so $b = p^w u' = p^k p^{w-k} u' \in p^k\mathbb{Z}_p$, which proves $I \subseteq p^k\mathbb{Z}_p$. □

Lastly, we note that $\mathbb{Z}_p$ is a local ring, i.e. a commutative ring with a maximal ideal $p\mathbb{Z}_p$.

2.2 Topological properties of $\mathbb{Z}_p$

Now we are ready to add a topological structure to the ring of p-adic integers. Since we can identify every element of $\mathbb{Z}_p$ with the sequence of its coefficients $(a_n)_{n\in\mathbb{N}} \in \{0, 1, \dots, p-1\}^{\mathbb{N}} =: X_p$ it's a natural choice to assign to $\mathbb{Z}_p$ the product topology of X_p, where each factor is a discrete set.
By Tychonoff theorem we immediately get that $\mathbb{Z}_p$ is compact and it's also easy to see that its connected components are points, i.e. it's totally disconnected. Since the discrete topology is metrizable (using the trivial metric) also $\mathbb{Z}_p$ is metrizable, being product of a countable number of metric spaces. Given $x = (a_n)_n, y = (b_n)_n \in X_p \leftrightarrow \mathbb{Z}_p$ we can define their distance as

$$d(x, y) := \sup_{i\geq 0} \frac{\delta_{a_i,b_i}}{p^i} = \frac{1}{p^{\operatorname{ord}_p(x-y)}}.$$

This is exactly the metric induced by the p-adic absolute value $|\ |_p$ introduced above (and satisfies all of its properties)!

Definition 2.6. A topological group is a group G equipped with a topology such that the map $(x, y) \mapsto xy^{-1}$ is continuous. A topological ring is a ring A with a topology such that addition $(x, y) \mapsto x + y$ and multiplication $(x, y) \mapsto xy$ are continuous.

Proposition 2.7. *$\mathbb{Z}_p$ is a topological ring.*

Proof. First of all we prove that $(x, y) \mapsto x - y$ is a continuous map, i.e. $(\mathbb{Z}_p, +)$ is a topological group. Using the p-adic metric, given $a, b \in \mathbb{Z}_p$ we have

$$\begin{gathered} |x-a|_p \leq p^{-n}, \qquad |y-b|_p \leq p^{-n} \\ \implies |(x-y)-(a-b)|_p \leq \max\Big\{|x-a|_p, |y-b|_p\Big\} \leq p^{-n} \end{gathered}$$

so the map is continuous at every point $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Now we have to prove the continuity of multiplication. Fixed $a, b \in \mathbb{Z}_p$ if $x = a + h, y = b + k \in \mathbb{Z}_p$ we have

$$\begin{gathered} |xy-ab|_p = |(a+h)(b+k)-ab|_p = |ak+hb+hk|_p \leq \\ \leq \max\Big\{|a|_p, |b|_p\Big\} \cdot \Big(|h|_p + |k|_p\Big) + |h|_p|k|_p \to 0, \qquad \text{as } |h|_p, |k|_p \to 0, \end{gathered}$$

proving the continuity of the multiplication at any point. These two conditions are equivalent to the ones given in the definition of topological ring: infact the map $(x, y) \mapsto x+y$ can be obtained by composing the map $(x, y) \mapsto (x, -y)$ (continuous thanks to product topology and continuity of multiplication) and the map $(x, y) \mapsto x - y$. □

Definition 2.8. A completion of a topological metrizable group G is a pair $(\widehat{G}, j)$ where $\widehat{G}$ is a Cauchy-complete group and $j \colon G \to \widehat{G}$ is a homomorphism such that

- $j(G)$ is dense in $\widehat{G}$;
- j is a homeomorphism $G \to j(G)$;
- any continuous homomorphism $f \colon G \to G'$, where G' is a complete group, can be uniquely factorized as $f = g \circ j \colon G \to \widehat{G} \to G'$ with a continuous homomorphism $g \colon \widehat{G} \to G'$.

It's clear that if G admits a completion $\widehat{G}$ then every other completion $\widehat{G}'$ is isomorphic to $\widehat{G}$ (from the definition we have a continuous bijective homomorphism $g \colon \widehat{G} \to \widehat{G}'$). Our aim is now to prove that $\mathbb{Z}_p$ is a complete space and $(\mathbb{Z}_p, +)$ is the completion of $(\mathbb{Z}, +)$ equipped with the p-adic metric. We'll now show (and prove) some general results on topological groups which will help us.

Lemma 2.9. *Let G be a topological group. G is metrizable (i.e. there exists a metric which induces the topology) if and only if G is Hausdorff and first countable (i.e. every point has a countable fundamental system of neighbourhoods).*

Proof. The $\Longrightarrow$ part is trivial. For the converse statement, check [1, Chap. XI]. □

A metrizable group G always admits a metric d invariant under left translations, i.e. $d(x, y) = d(gx, gy)$ for every $g \in G$. A metrizable group can always be completed.

Lemma 2.10. *If G is a topological group and H is a subgroup of G then the closure $\overline{H}$ of H is a subgroup of G.*

Proof. Let $\varphi\colon G \times G \to G$ be the continuous map $(x, y) \to xy^{-1}$. Since $H \leq G$ we have $\varphi(H \times H) \subseteq H$ hence

$$\varphi(\overline{H} \times \overline{H}) = \varphi(\overline{H \times H}) \subseteq \overline{\varphi(H \times H)} \subseteq \overline{H}$$

which proves $\overline{H} \leq G$. □

Proposition 2.11. *Let G be a topological group and $H \leq G$. If H contains a neighbourhood of the neutral element of G then H is a clopen of G.*

Proof. Let V be such neighbourhood; then $\forall h \in H$, hV is a neighbourhood of h in G which is fully contained in H. This proves H is open in G. Since maps like $x \mapsto gx$ are homeomorphisms for every g in G, we have that every coset gH of H in G is open. Now $G \backslash H = \bigcup_{g \notin H} gH$ is open, i.e. H is closed in G. □

For example the subgroups $p^n\mathbb{Z}_p$ of $(\mathbb{Z}_p, +)$ are open and closed.

Definition 2.12. A subspace Y of a topological space X is *locally closed* (in X) when each point $y \in Y$ has an open neighbourhood V in X such that $Y \cap V$ is closed in V.

It can be proved that $Y \subseteq X$ is locally closed if and only if Y is open in its closure $\overline{Y}$.

Theorem 2.13. *Let G be a topological group and H a locally closed subgroup. Then H is closed.*

Proof. If H is locally closed then it's open in its closure $\overline{H}$. In particular, if e is the neutral element of G then $e \in H$ and $\exists V \subseteq H$, which is a neighbourhood of e in $\overline{H}$. By Lemma 2.10, $\overline{H} \leq G$ so, applying Proposition 2.11 with $H \leq \overline{H}$, we get that H is closed in $\overline{H}$, i.e. $H = \overline{H}$, which clearly implies H is closed in G. □

If we consider only Hausdorff spaces we immediately get that locally compact subsets are locally closed, because a compact set is closed in a Hausdorff space. We recall that a topological group is locally compact exactly when one of its points has a fundamental system of compact neighbourhoods (then by translation every point admits one).

Corollary 2.13.1. *Let H be a locally compact subgroup of a Hausdorff topological group G. Then H is closed.*

Let G be a topological metrizable group which has $\widehat{G}$ as its completion. If G is locally compact then it must be closed in its completion (we identify G with its image in $\widehat{G}$). But since G is dense in $\widehat{G}$ we get $\widehat{G} = G$.

Corollary 2.13.2. *A locally compact metrizable group is complete.*

Now we can prove the following

Proposition 2.14. *$\mathbb{Z}_p$ is a compact, complete metrizable space. More precisely, the topological group $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$, equipped with the p-adic metric.*

Proof. We have already proved that $\mathbb{Z}_p$ is compact and metrizable. To see that it's complete we can just apply Corollary 2.13.2, because $\mathbb{Z}_p$ is locally compact (from general topology we know that Hausdorff and compact implies that every point has a fundamental system of compact neighbourhoods).
Let's consider $j\colon \mathbb{Z} \hookrightarrow \mathbb{Z}_p$ the natural embedding: it is a continuous homomorphism ($\mathbb{Z}$ with the p-adic metric has the topology induced by $\mathbb{Z}_p$) and $j(\mathbb{Z})$ is dense in $\mathbb{Z}_p$. Given $\mathbb{Z}_p \ni x = \sum_{i\geq 0} a_i p^i$ if

$$x_n := \sum_{0\leq i<n} a_i p^i \in \mathbb{N}$$

then $(x_n)_n \subseteq \mathbb{Z}$ is a Cauchy sequence converging to x. To verify the universal property, given a continuous homomorphism $f\colon \mathbb{Z} \to X$, where X is a complete group, we can define $\widetilde{f}\colon \mathbb{Z}_p \to X$ as follows: given $x \in \mathbb{Z}_p$ and $(x_n)_n \subseteq \mathbb{Z}$ a sequence convergent to x then

$$\widetilde{f}(x) := \lim_{n\to+\infty} f(x_n)$$

where the limit is taken in X. This is well defined: if $(y_n)_n \subseteq \mathbb{Z}$ is another sequence convergent to x we have that $|x_n - y_n|_p \to 0$ as $n \to +\infty$ so

$$\lim_{n\to+\infty} (f(x_n) - f(y_n)) = \lim_{n\to+\infty} f(x_n - y_n) = f\left(\lim_{n\to+\infty}(x_n - y_n)\right) = f(0) = 0$$

where we exploited the fact that f is continuous and a homomorphism. The fact that $\widetilde{f}$ is a continuous homomorphism is easy to prove. □

Corollary 2.14.1. *The addition and multiplication of p-adic integers are the only continuous operations on $\mathbb{Z}_p$ extending the classic addition and multiplication on $\mathbb{Z}$.*

2.3 $\mathbb{Z}_p$ as a projective limit

We now want to give another definition of $\mathbb{Z}_p$, using projective limits.

Definition 2.15. A sequence $(E_n, \varphi_n)_{n\in\mathbb{N}}$ of sets and maps $\varphi_n\colon E_{n+1} \to E_n$ is called a *projective system.*
A set E together with maps $\psi_n\colon E \to E_n$ such that $\psi_n = \varphi_n \circ \psi_{n+1}$ $\forall n \in \mathbb{N}$ is called a *projective limit* of the sequence $(E_n, \varphi_n)_n$ if the following holds: for each set X and maps $f_n\colon X \to E_n$ satisfying $f_n = \varphi_n \circ f_{n+1}$ $\forall n \in \mathbb{N}$ there is a unique $f\colon X \to E$ such that $f_n = \psi_n \circ f$ for every $n \in \mathbb{N}$ (universal factorization property).

The maps $\varphi_n\colon E_{n+1} \to E_n$ are called transition maps and the whole system, which is often called *inverse system*, can be represented by

$$E_0 \xleftarrow{\varphi_0} E_1 \xleftarrow{\varphi_1} E_2 \xleftarrow{\varphi_2} \dots \xleftarrow{\varphi_n} E_{n+1} \longleftarrow \dots$$

and denoting E as $\varprojlim E_n$, the complete scheme would look like this:

$$\begin{tikzcd}
 & & & & \varprojlim E_n \arrow[llld, "\psi_n"'] \arrow[lld, "\psi_{n+1}"] \\
\cdots & E_n \arrow[l] & E_{n+1} \arrow[l, "\varphi_n"] & \cdots \arrow[l] & \\
 & & & & X \arrow[uu, dashed, "f"] \arrow[lllu, "f_n"] \arrow[llu, "f_{n+1}"']
\end{tikzcd}$$

Theorem 2.16. *For every projective system $(E_n, \varphi_n)_{n\in\mathbb{N}}$ there exists a projective limit $E = \varprojlim E_n \subset \prod_n E_n$ with maps $\psi_n \colon E \to E_n$ given by (restriction of) projections.*
Moreover, given (E', ψ'_n) another projective limit of the system, there's a unique bijection $f\colon E' \to E$ such that $\psi'_n = \psi_n \circ f$.

Proof. First we prove existence. Let

$$E := \{(x_n)_n : \varphi_n(x_{n+1}) = x_n \ \forall n \geq 0\} \subset \prod_{n\geq 0} E_n$$

be the set of *coherent sequences* (with respect to the transition maps φ_n). If $p_n\colon \prod_{i\geq 0} E_i \to E_n$ is the canonical projection then we have

$$\varphi_n(p_{n+1}(x)) = p_n(x) \qquad \forall x \in E.$$

So, if we define $\psi_n := p_n|_E : E \to E_n$ we have $\varphi_n \circ \psi_{n+1} = \psi_n$. We'll now show that (E, ψ_n) is a projective limit of the system. If (E', ψ'_n) is another set equipped with maps satisfying $\varphi_n \circ \psi'_{n+1} = \psi'_n$ (for every $n \geq 0$) then we need to prove that there's a unique factorization of ψ'_n by ψ_n. We can define a vector map

$$(\psi'_n)\colon E' \to \prod_{n\geq 0} E_n, \qquad y \mapsto (\psi'_n(y))_n.$$

Since $\varphi_n(\psi'_{n+1}(y)) = \psi'_n(y)$, the image of this map is fully contained in E (i.e. $(\psi'_n(y))_n$ is a coherent sequence). Thus there's a unique map $f\colon E' \to E$ such that $\psi'_n = \psi_n \circ f$, and it's exactly the map (ψ'_n) considered with E as target (uniqueness is easy to see, recalling that ψ_n is just the restrictions to E of the canonical projection p_n).
Now we have to prove uniqueness. If (E, ψ_n) and (E', ψ'_n) are both projective limits then, by the universal factorization property, there's a unique map $f'\colon E \to E'$ with $\psi_n = \psi'_n \circ f'$. Using the same $f\colon E' \to E$ defined before and substituting in $\psi'_n = \psi_n \circ f$ we obtain

$$\psi'_n = \psi_n \circ f = \psi'_n \circ f' \circ f$$

which means that $f' \circ f$ is a factorization of $\mathrm{id}_{E'}$ (identity map). Since (E', ψ'_n) has also, by definition of projective limit, the unique factorization property we must have $f' \circ f = \mathrm{id}_{E'}$. Similarly we can prove $f \circ f' = \mathrm{id}_E$, so f is the searched bijection. □

The projective limit can be defined for a lot of structures, like topological spaces, groups or vector spaces. For example, given $(G_n, \varphi_n)_n$ a projective system of groups and homomorphisms $\varphi_n\colon G_{n+1} \to G_n$, the projective limit $G = \varprojlim G_n$ is a group and the projections $\psi_n\colon G \to G_n$ are group homomorphisms. Likewise, a projective system of topological spaces and continuous maps will have a projective limit which is itself a topological space, equipped with continuous projections.

We can now give another definition of $\mathbb{Z}_p$. Let's consider the ring $\mathbb{Z}$ and the decreasing sequence $(p^n\mathbb{Z})_n$ of ideals. The inclusion $p^{n+1}\mathbb{Z} \subset p^n\mathbb{Z}$ gives us the canonical transition homomorphism

$$\varphi_n\colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}, \qquad x + p^{n+1}\mathbb{Z} \mapsto x + p^n\mathbb{Z}.$$

If we consider $\mathbb{Z}/p^n\mathbb{Z}$ as a topological ring (equipped with discrete topology) then we have the following theorem.

Theorem 2.17. *The map $\Phi\colon \mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ which associates to the p-adic integer $x = \sum_{i\geq 0} a_i p^i$ the sequence of its partial sums $x_n = \sum_{i<n} a_i p^i \mod p^n$ is an isomorphism of topological rings.*

Proof. The map is well defined. In-fact, since the transition maps φ_n are given by

$$\sum_{i\leq n} a_ip^i \mod p^{n+1} \quad \mapsto \quad \sum_{i<n} a_ip^i \mod p^n$$

the set of coherent sequences in $\prod \mathbb{Z}/p^n\mathbb{Z}$ is exactly the set of partial sums of a p-adic expansion. From the relations

$$x_1 = a_0, \quad x_2 = a_0 + a_1p, \quad x_3 = a_0 + a_1p + a_2p^2, \dots$$
$$a_0 = x_1, \quad a_1 = \frac{x_2 - x_1}{p}, \quad a_2 = \frac{x_3 - x_2}{p^2}, \dots$$

we infer that Φ is bijective. It's easily proved that it is a ring homomorphism (sum and product are done component-wise on $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$), so Φ is a ring isomorphism. Finally, this map is continuous since for every $n \in \mathbb{N}$, if $\pi\colon \prod_i \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the canonical projection, we have

$$\mathbb{Z}_p \xrightarrow{\Phi} \varprojlim \mathbb{Z}/p^k\mathbb{Z} \hookrightarrow \prod_k \mathbb{Z}/p^k\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p^n\mathbb{Z}, \qquad \sum_{i\geq 0} a_ip^i \mapsto \sum_{i<n} a_ip^i \mod p^n$$

which is continuous (we recall how product topology is defined). Now Φ is a continuous invertible map between two compact spaces so it's a homeomorphism. □

So we can also think $\mathbb{Z}_p$ as the projective limit of $\mathbb{Z}/p^n\mathbb{Z}$, with canonical projection maps. Let us observe that we can choose any system of representatives $\mathcal{S}$ for $\mathbb{Z}/p\mathbb{Z}$ and write any p-adic integer as $x = \sum s_ip^i$ with $s_i \in \mathcal{S}$. For example, if p is odd we can choose to use $\mathcal{S} = \{-\frac{p-1}{2}, \dots, 0, \dots, \frac{p-1}{2}\}$. Although we are only working with $\mathbb{Z}_p$, where p is a prime number, this theorem also gives us a factorization of $\mathbb{Z}_n$, for each $n \in \mathbb{N}$. In-fact, since the projective limit of a cartesian product is exactly the cartesian product of the projective limits of the factors, if $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ we have

$$\mathbb{Z}/m^n\mathbb{Z} = \mathbb{Z}/p_1^{\alpha_1 \cdot n}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r \cdot n}\mathbb{Z}$$
$$\implies \mathbb{Z}_m = \varprojlim (\mathbb{Z}/p_1^{\alpha_1 \cdot n}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r \cdot n}\mathbb{Z}) = \prod_{i=1}^r \varprojlim \mathbb{Z}/p_i^{\alpha_i \cdot n}\mathbb{Z} = \prod_{i=1}^r \mathbb{Z}_{p_i^{\alpha_i}}.$$

In particular, for the already seen example $m = 10$, we obtain $\mathbb{Z}_{10} = \mathbb{Z}_2 \times \mathbb{Z}_5$.

Lastly, we can give another description of $\mathbb{Z}_p$ using formal power series $\mathbb{Z}[\![X]\!]$. We recall that on $\mathbb{Z}[\![X]\!]$ sum is defined component-wise (obviously here there's no carry system, unlike in $\mathbb{Z}_p$) and product is done in a Cauchy way (there's a natural inclusion $\mathbb{Z}[X] \hookrightarrow \mathbb{Z}[\![X]\!]$).

Theorem 2.18. *The map*

$$\Phi\colon \mathbb{Z}[\![X]\!] \to \mathbb{Z}_p \qquad \sum a_iX^i \mapsto \sum a_ip^i$$

is a ring homomorphism, which defines a canonical isomorphism

$$\frac{\mathbb{Z}[\![X]\!]}{(X-p)} \xrightarrow{\sim} \mathbb{Z}_p$$

where $(X - p)$ is the principal ideal of $\mathbb{Z}[\![X]\!]$ generated by $X - p$.

Proof. To prove this theorem we exploit the universal factorization property of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, i.e. $\mathbb{Z}_p$. Let's consider this sequence of maps

$$\Phi_n\colon \mathbb{Z}[\![X]\!] \to \mathbb{Z}/p^n\mathbb{Z}, \qquad \sum a_iX^i \mapsto \sum_{i<n} a_ip^i \mod p^n.$$

They're actually ring homomorphisms; the condition $\Phi_n(x+y) = \Phi_n(x) + \Phi_n(y)$ is immediate, to check $\Phi_n(x \cdot y) = \Phi_n(x) \cdot \Phi_n(y)$ we write

$$\begin{aligned}\Phi_n\left(\sum_i a_i X^i \cdot \sum_j b_j X^j\right) &= \Phi_n\left(\sum_k c_k X^k\right) = \sum_{k<n} c_k p^k \mod p^n = \\ &= \sum_{k<2n} c_k p^k \mod p^n = \left(\sum_{i<n} a_i p^i\right) \cdot \left(\sum_{j<n} b_j p^j\right) \mod p^n = \\ &= \Phi_n\left(\sum_i a_i X^i\right) \cdot \Phi_n\left(\sum_j b_j X^j\right).\end{aligned}$$

It's immediate that these maps are all compatible with the transition homomorphisms

$$\varphi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}, \qquad x + p^{n+1}\mathbb{Z} \mapsto x + p^n\mathbb{Z}$$

and so we infer there exists a unique homomorphism

$$\Phi \colon \mathbb{Z}[\![X]\!] \to \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$$

compatible with the Φ_n (i.e. such that $\psi_n \circ \Phi = \Phi_n$, where $\psi_n \colon \varprojlim \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the canonical projection). This map is surjective: if $x = \sum a_i p^i$ is a p-adic integer then $\Phi\left(\sum a_i X^i\right) = x$. Thanks to the first theorem of isomorphism for ring homomorphisms now we just need to prove $\ker \Phi = (X - p)$ (then we'll have $\mathbb{Z}[\![X]\!]/\ker\Phi = \mathbb{Z}[\![X]\!]/(X-p) \simeq \operatorname{Im}\Phi = \mathbb{Z}_p$). In other words we need to show that if the formal power series $\sum_{i\geq 0} a_i X^i$ is such that $\sum_{i<n} a_i p^i \in p^n\mathbb{Z}$ for every $n \geq 1$, then it is divisible by $X - p$. For $n = 1$ the condition is $a_0 \equiv 0 \mod p$ so we find $\alpha_0 \in \mathbb{Z}$ such that $a_0 = p\alpha_0$. For $n = 2$ we get

$$a_0 + a_1 p = \alpha_0 p + a_1 p \equiv 0 \mod p^2 \implies \alpha_0 + a_1 \equiv 0 \mod p$$

so we find $\alpha_1 \in \mathbb{Z}$ such that $\alpha_0 + a_1 = p\alpha_1$ so $a_1 = p\alpha_1 - \alpha_0$. For a general $n \geq 1$ the condition is

$$a_0 + a_1 p + \cdots + a_n p^n = p^n \alpha_{n-1} + a_n p^n \equiv 0 \mod p^{n+1}$$

and it furnishes an integer α_n such that $\alpha_{n-1} + a_n = p\alpha_n$, which can be written as $a_n = p\alpha_n - \alpha_{n-1}$. These relations between the coefficients a_n and α_n are exactly the ones expressed by

$$\sum a_i X^i = -(X - p) \cdot \sum \alpha_i X^i$$

which concludes our proof. □

2.4 The field $\mathbb{Q}_p$

We have proved that $\mathbb{Z}_p$ is an integral domain hence we can define the field

$$\mathbb{Q}_p = \operatorname{Frac}(\mathbb{Z}_p).$$

To understand its structure, we recall that any p-adic integer can be written as $x = p^m u$ where $u \in \mathbb{Z}_p^\times$. Then, $1/x = p^{-m}u^{-1}$, with $u^{-1} \in \mathbb{Z}_p$. So we can write

$$\mathbb{Q}_p = \mathbb{Z}_p[1/p] = \bigcup_{m\geq 0} p^{-m}\mathbb{Z}_p.$$

Since a non-zero element of $\mathbb{Q}_p$ admits a unique such writing, $\mathbb{Q}_p^\times = \coprod_{m\in\mathbb{Z}} p^m\mathbb{Z}_p^\times$. Similarly to Laurent expansions of meromorphic functions around a pole, we can write every non-zero element of $\mathbb{Q}_p$ as

$$x = p^m \cdot \sum_{i\geq 0} a_i p^i = \sum_{i\geq m} a_{i-m} p^i, \qquad m \in \mathbb{Z}, a_0 \neq 0.$$

We can extend the function ord_p to $\mathbb{Q}_p$ as follows:

$$\operatorname{ord}_p x = \begin{cases} m, & \text{if } x = p^m u, u \in \mathbb{Z}_p^\times; \\ +\infty, & \text{otherwise;} \end{cases}.$$

Given $x = a/b$ with $a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^\times$ it's easy to see that $\operatorname{ord}_p x = \operatorname{ord}_p a - \operatorname{ord}_p b$ and, writing every number as above, we immediately get $\operatorname{ord}_p xy = \operatorname{ord}_p x + \operatorname{ord}_p y$ (this holds also when $xy = 0$, with the usual convention $m + \infty = \infty + m = \infty$), i.e. $\operatorname{ord}_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ is a group homomorphism. Finally we see that $\operatorname{ord}_p (x+y) \geq \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}$, with the equality holding when $\operatorname{ord}_p x \neq \operatorname{ord}_p y$. These properties tell us exactly that ord_p is a discrete valuation on the field $\mathbb{Q}_p$, and that $\mathbb{Z}_p$ is the ring of valuation of $(\mathbb{Q}_p, \operatorname{ord}_p)$ because $x \in \mathbb{Z}_p$ if and only if $\operatorname{ord}_p x \geq 0$ and $\operatorname{ord}_p 1/x = -\operatorname{ord}_p x$.

We recall that

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \nmid b, b \neq 0 \right\}.$$

The relations between $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are similar to the ones between $\mathbb{Z}_{(p)}$ and $\mathbb{Q}$. In-fact we have

$$\mathbb{Q} = \bigcup_{m\geq 0} p^{-m}\mathbb{Z}_{(p)}, \qquad \mathbb{Q}^\times = \coprod_{p\in\mathbb{Z}} p^m \mathbb{Z}_{(p)}^\times$$

where $\mathbb{Z}_{(p)}^\times$ consists of all the fractions with both numerator and denominator prime to p.

We can see that the definition of $\mathbb{Q}_p$ introduced here represents exactly the same object described in chapter 1. So we can introduce the p-adic absolute value, and its induced metric, in the exact same way and all properties proved before will be valid. So $\mathbb{Q}_p$ is a metric field equipped with a discrete valuation, which implies that $\mathbb{Q}_p$ is a topological field (i.e. a topological ring where the inverse map $\mathbb{Q}_p^\times \to \mathbb{Q}_p^\times : x \mapsto x^{-1}$ is continuous).

Proposition 2.19. *The field $\mathbb{Q}_p$ is a locally compact field of characteristic 0 which induces on $\mathbb{Z}_p$ the p-adic topology. It can be identified with the completion of $\mathbb{Z}_p[1/p]$ or of $\mathbb{Q}$, for the p-adic metric.*

Proof. We have already observed that $\mathbb{Z}_p = B_{\leq 1}(0) = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ and, for every $k \geq 0$ the ideal $p^k\mathbb{Z}_p$ is exactly $B_{\leq p^{-k}}(0)$. Since $\mathbb{Z}_p$ is a compact neighbourhood of 0, the topological field $\mathbb{Q}_p$ is locally compact ($x + \mathbb{Z}_p$ is a compact neighbourhood of x). From Corollary 2.13.2 we obtain that $\mathbb{Q}_p$ is complete. We now show that $\mathbb{Z}[1/p]$ is dense in $\mathbb{Q}_p$; given

$$x = \sum_{i\geq v}^{+\infty} x_i p^i \qquad (v = \operatorname{ord}_p x \in \mathbb{Z})$$

we immediately find that the sequence of truncated sums $x_n = \sum_{v\leq i<n} x_i p^i$ is a Cauchy sequence in $\mathbb{Z}[1/p] \subset \mathbb{Q}$ which converges to x. Finally, we have already seen that $\mathbb{Q}_p$ is a field of characteristic 0, since we have an immersion $\mathbb{Z} \hookrightarrow \mathbb{Q}_p$. □

Here we have proved that $\mathbb{Q}_p$ is a complete field, a fact we already knew, in a very different way than before, by just using algebraic properties of topological groups.

Given a non-zero element $\mathbb{Q}_p \ni x = \sum_{i \geq m} x_i p^i$ we can define

$$[x] := \sum_{i \geq 0} x_i p^i \in \mathbb{Z}_p : \textit{ integral part } \text{of } x \; ;$$

$$\langle x \rangle := \sum_{i<0} x_i p^i \in \mathbb{Z}[1/p] = \{ap^v \mid a, v \in \mathbb{Z}\} \subset \mathbb{Q} : \textit{ fractional part } \text{of } x.$$

Hence we obtain the decomposition $\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p]$, which is not canonical, because it depends on the choice of the representatives of $\mathbb{Z}/p\mathbb{Z}$ chosen for digits (here we have always chosen to use $\mathcal{S} = \{0, 1, \ldots, p-1\}$). This sum is not a direct sum since $\mathbb{Z}_p \cap \mathbb{Z}[1/p] = \mathbb{Z}$, so there's not a unique factorization of any $x \in \mathbb{Q}_p$. If we consider the map $\mathbb{Z} \to \mathbb{Z}_p \oplus \mathbb{Z}[1/p] : m \mapsto (m, -m)$ and the addition homomorphism $\mathbb{Z}_p \oplus \mathbb{Z}[1/p] \to \mathbb{Z}_p + \mathbb{Z}[1/p] = \mathbb{Q}_p : (a, b) \mapsto a + b$ we obtain the short exact sequence:

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \oplus \mathbb{Z}[1/p] \twoheadrightarrow \mathbb{Q}_p$$

where the image of the first map is exactly the kernel of the second one.

2.5 Hensel's Lemma

In this section we present the important Hensel's lemma, a principle which gives us a method to find roots of polynomials in $\mathbb{Z}_p[X]$.

Proposition 2.20. *Let $P(X) \in \mathbb{Z}_p[X]$. The following properties are equivalent:*

(i) $P = 0$ admits a solution in $\mathbb{Z}_p$;

(ii) for each $n \geq 0$, $P = 0$ admits a solution in $\mathbb{Z}/p^n\mathbb{Z}$.

Proof. The part *(i)* $\implies$ *(ii)* is trivial: if $x = \sum_{i \geq 0} a_i p^i \in \mathbb{Z}_p$ is a root of P then $x_n = \sum_{i<n} a_i p^i$ is in $\mathbb{Z}/p^n\mathbb{Z}$ and $P(x_n) = P(x) \mod p^n$.
To prove the converse, let's consider the non-empty finite sets

$$X_n = \{x \in \mathbb{Z}/p^n\mathbb{Z} \mid P(x) = 0 \mod p^n\}.$$

It's immediate that if $x \in X_{n+1}$ then $\widetilde{x} = x \mod p^n$ is in X_n, because $P(\widetilde{x}) = P(x) \mod p^n$. So reduction mod p^n furnishes a map $\varphi_n \colon X_{n+1} \to X_n$. We can consider the projective system $(X_n, \varphi_n)_{n \in \mathbb{N}}$: it admits a projective limit $X = \varprojlim X_n \subset \mathbb{Z}_p$. It's now clear that if $x \in X$ then $P(x) = 0$ in $\mathbb{Z}_p$. Since the projective limit of non-empty sets is not empty (it immediately follows from the fact that projective limit of non-empty compact space is non-empty, [6, p. 30]), we can conclude. □

We recall the elementary fact that if A is a commutative ring and $P \in A[X]$ then

$$P(X+h) = P(X) + h \cdot P'(X) + h^2 \cdot Q(X, h)$$

where Q is a polynomial in $A[X, Y]$ (we'll refer to this as the Taylor expansion of P, for obvious reasons). We're now ready to prove this proposition. For brevity, we'll write $v(\zeta) := \operatorname{ord}_p \zeta$, for $\zeta \in \mathbb{Q}_p$.

Proposition 2.21. *Let $P \in \mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$ be such that $P(x) \equiv 0 \mod p^n$. If $k = v(P'(x)) < n/2$, then $\widehat{x} := x - P(x)/P'(x)$ satisfies*

(i) $P(\widehat{x}) \equiv 0 \mod p^{n+1}$;

(ii) $\widehat{x} \equiv x \mod p^{n-k}$;

(iii) $v(P'(\widehat{x})) = v(P'(x))$.

Proof. Let's write $P(x) = p^n y$ for $y \in \mathbb{Z}_p$ and $P'(x) = p^k u$ with $u \in \mathbb{Z}_p^\times$. Then

$$\widehat{x} - x = -\frac{P(x)}{P'(x)} = -p^{n-k} y u^{-1} \in p^{n-k}\mathbb{Z}_p$$

which proves *(ii)*. To prove *(i)* we observe

$$P(\widehat{x}) = P(x + (\widehat{x} - x)) = P(x) - \frac{P(x)}{P'(x)} P'(x) + (\widehat{x} - x)^2 \cdot t$$

where $t \in \mathbb{Z}_p$. Then

$$P(\widehat{x}) = p^{2(n-k)} y^2 u^{-2} t^2 \in p^{n+1}\mathbb{Z}_p \subseteq p^{2(n-k)}\mathbb{Z}_p$$

since $n - k > n/2$. Now it only remains to compute the order of $P'(\widehat{x})$. Let's use Taylor expansion:

$$P'(\widehat{x}) = P'(x) + (\widehat{x} - x) \cdot s = p^k u + p^{n-k} zs = p^k(u + p^{n-2k} zs) = p^k w \quad (z, s \in \mathbb{Z}_p).$$

Since $n - 2k > 0$ and u is a unit of $\mathbb{Z}_p$, we get

$$w = u + p^{n-2k} zs \in u + p^{n-2k}\mathbb{Z}_p \subset \mathbb{Z}_p^\times$$

which proves $v(P'(\widehat{x})) = k$. □

We can finally prove the Hensel's Lemma.

Theorem 2.22 (Hensel's Lemma)**.** *Let P be a polynomial in $\mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$ such that $P(x) \equiv 0 \mod p^n$. If $k = v(P'(x)) < n/2$ then there exists a unique root ξ of P in $\mathbb{Z}_p$ such that $\xi \equiv x \mod p^{n-k}$ and $v(P'(\xi)) = v(P'(x))$.*

Proof. Let's first prove the existence of such ξ. Let $x_0 = x$; we want to find $x_1 \in \mathbb{Z}_p$ such that

$$x_1 \equiv x_0 \mod p^{n-k}, \quad P(x_1) \equiv 0 \mod p^{n+1}, \quad v(P'(x_1)) = k.$$

By Proposition 2.21 we can build such an x_1, which represents an "improved" root of P. Similarly, we can find $x_2 \in \mathbb{Z}_p$ such that

$$x_2 \equiv x_1 \mod p^{n-k+1}, \quad P(x_2) \equiv 0 \mod p^{n+2}, \quad v(P'(x_2)) = k.$$

Iterating this process we get a coherent sequence $(x_m)_{m \in \mathbb{N}} \subset \mathbb{Z}_p$: more specifically, letting $h = n - k$, we obtain

$$x_m \equiv \sum_{i=0}^{h+m} a_i p^i \mod p^{h+m+1}, \quad P(x_m) \equiv 0 \mod p^{n+m}$$

$$x_{m+1} \equiv \sum_{i=0}^{h+m} a_i p^i + a_{h+m+1} p^{h+m+1} \mod p^{h+m+2}, \quad P(x_{m+1}) \equiv 0 \mod p^{n+m+1}$$

so it's clear that this sequence has p-adic limit $\xi = \sum_{i \geq 0} a_i p^i$ satisfying $P(\xi) = 0$ in $\mathbb{Z}_p$, $\xi \equiv x \mod p^{n-k}$ and $v(P'(\xi)) = k$.
Now we prove uniqueness. Let ξ and η be two roots of P in $\mathbb{Z}_p$ satisfying the above constraints. Then

$$0 = P(\eta) = P(\xi) + (\eta - \xi)P'(\xi) + (\eta - \xi)^2 a \quad (a \in \mathbb{Z}_p)$$

so, since $\eta - \xi \in p^{n-k+1}\mathbb{Z}_p$, we have

$$0 = (\eta - \xi)(P'(\xi) + (\eta - \xi)a).$$

Clearly, since $v(P'(\xi)) = k$ and $v((\eta - \xi)a) \geq n - k + 1 > k$, the term $(P'(\xi) + (\eta - \xi)a)$ can't vanish so we must have $\eta = \xi$. □

The Hensel's Lemma is a very important tool in p-adic analysis, so we'll write again a weak version of it.

Corollary 2.22.1 (Weak Hensel's Lemma)**.** *Let P a polynomial in $\mathbb{Z}_p[X]$ and $a_0 \in \mathbb{Z}_p$ such that $P(a_0) \equiv 0 \mod p$ and $P'(a_0) \not\equiv 0 \mod p$. Then there is a unique $a \in \mathbb{Z}_p$ such that $P(a) = 0$ and $a \equiv a_0 \mod p$.*

3 Construction of $\mathbb{C}_p$

3.1 Ultrametric spaces

In this section we'll explore some useful properties of ultrametric spaces.

Definition 3.1. An *ultrametric space* is a metric space (X, d) where

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

for every $x, y, z \in X$.

In these section, to avoid confusion, we'll use different names for open and closed balls:

- $B_{<r}(a)$ is a *stripped ball*;
- $B_{\leq r}(a)$ is a *dressed ball.*

Proposition 3.2. *Let (X, d) be an ultrametric space. The following properties hold:*

(i) any point of a ball is a center;

(ii) ff two balls have a common point, one is contained in the other;

(iii) the diameter of a ball is less or equal than its radius.

Proof. *(i)* If $b \in B_{<r}(a)$ then $d(a, b) < r$ and we have

$$\begin{aligned} x \in B_{<r}(a) \implies d(x, a) < r \implies d(x, b) \leq \max\{d(x, a), d(a, b)\} < r \\ \implies x \in B_{<r}(b) \end{aligned}$$

which implies $B_{<r}(a) \subseteq B_{<r}(b)$. Exchanging the roles of a and b we obtain $B_{<r}(a) = B_{<r}(b)$. The result for dressed balls is identical.

(ii) If $c = B_{<r}(a) \cap B_{\leq r'}(b)$ then we have $B_{<r}(a) = B_{<r}(c)$ and $B_{\leq r'}(b) = B_{\leq r'}(c)$, by *(i)*. Now the result is obvious.

(iii) Direct application of the ultrametric inequality. □

Let $S_r(a) := \{x \in X \mid d(x, a) = r\}$ be the sphere of radius r centered in a.

Proposition 3.3. *Let (X, d) be an ultrametric space. The following properties hold:*

(i) if $d(x, z) > d(z, y)$ then $d(x, y) = d(x, z)$;

(ii) if $x \in S_r(a)$ then $B_{<r}(x) \subset S_r(a)$ and $S_r(a) = \bigcup_{x \in S_r(a)} B_{<r}(x)$.

Proof. *(i)* We have

$$\begin{aligned} d(x, y) &\leq \max\{d(x, z), d(z, y)\} = d(x, z) \\ d(x, z) &\leq \max\{d(x, y), d(y, z)\} \leq d(x, z) \end{aligned}$$

so $\max\{d(x,y),d(y,z)\} = d(x,z)$ which implies $d(x,y) = d(x,z)$. This property is well known as the *isosceles triangle principle*, i.e. every triangle of an ultrametric space is isosceles, with at most one short side.

(ii) We need to prove that $y \in B_{<r}(x) \implies d(a,y) = r$. By *(i)*, since $d(x,y) < d(a,x) = r$, we must have $d(y,a) = d(a,x) = r$. The second part of the statement is obvious. □

We can give a slightly more general version of the isosceles triangle principle. Let $x_1,\dots,x_n \in X$, $x_{n+1} := x_1$ and assume $d(x_1,x_n) = \max_{1\le i\le n} d(x_i,x_{i+1})$. Applying the ultrametric inequality (with a rapid induction) we obtain

$$d(x_1,x_n) \le \max\{d(x_1,x_2),\dots,d(x_{n-1},x_n)\} = d(x_1,x_n)$$

so there exists $i \in \{1,\dots,n-1\}$ such that $d(x_i,x_{i+1}) = d(x_1,x_n)$. We have proved that given a cycle of length n there are always at least two pairs of elements with equal maximal distance.

With the next lemma we'll understand why it is a better choice to use a different nomenclature for balls.

Proposition 3.4. *Let (X,d) be an ultrametric space. The following properties hold:*

(i) the spheres $S_r(a)$ are clopen for every $a \in X, r > 0$;

(ii) the dressed balls are open (and closed);

(iii) the stripped balls are closed (and open);

(iv) if B and B' are disjoint balls then $d(B,B') = d(x,x')$ for every $x \in B, x' \in B'$.

Proof. *(i)* Since the function $x \mapsto d(x,a)$ is continuous, $S_r(a)$ is closed. By Proposition 3.3 $S_r(a)$ is also open (union of stripped balls, which are trivially open).

(ii) If $r > 0$ we have $B_{\le r}(a) = B_{<r}(a) \sqcup S_r(a)$ so $B_{\le r}(a)$ is open.

(iii) If $r > 0$ we have $B_{<r}(a) = B_{\le r}(a) \setminus S_r(a)$ so $B_{<r}(a)$ is closed (intersection of closed sets).

(iv) Given $x, y \in B$ and $x', y' \in B'$ we can consider the 4-cycle x, x', y', y: there must be two pairs with equal maximal distance. Since $B \cap B' = \emptyset$, such distance is $c := d(x,x') = d(y,y')$ and $d(B,B') = \inf_{a\in B, b\in B'} d(a,b) = c$. □

Lemma 3.5. *Let (X,d) be an ultrametric space. The following properties hold:*

(i) $(x_n)_{n\in\mathbb{N}} \subseteq X$ is Cauchy if (and only if) $d(x_n,x_{n+1}) \to 0$ as $n \to +\infty$;

(ii) if $x_n \to x \neq a$ then $\exists N \in \mathbb{N}$ such that $d(x_n,a) = d(x,a)$ for every $n \ge N$.

Proof. *(i)* Fixed $\varepsilon > 0$ if $d(x_n,x_{n+1}) < \varepsilon$ for $n \ge N$ then

$$d(x_n,x_{n+m}) \le \max_{0\le i<m} d(x_{n+i},x_{n+i+1}) < \varepsilon$$

for all $n \ge N$ and $m \ge 0$.

(ii) As soon as $d(x_n,x) < d(x,a)$ we have, by the isosceles triangle principle, $d(x_n,a) = d(x,a)$. □

There are some more interesting properties if the space is an abelian (additive) group G equipped with an *ultrametric norm*, i.e. a function $|\ |: G \to \mathbb{R}_{\ge 0}$ satisfying:

- $|x| > 0 \iff x \neq 0$;
- $|-x| = |x|$;
- $|x+y| \le \max\{|x|,|y|\}$.

These groups are called *abelian ultrametric groups.* Here we can consider finite sums and series and we will see that there are simpler conditions for them to converge than in classic analysis.

Proposition 3.6. *Let G be an abelian ultrametric group. If $a_1 + a_2 + \cdots + a_n = 0$ then $\exists i \neq j$ such that $|a_i| = |a_j| = \max_{1 \leq h \leq n} |a_h|$. This property is called* competitivity.

Proof. It's just the group version of the generalized isosceles triangle principle. □

Proposition 3.7. *Let $(a_n)_{n\in\mathbb{N}}$ a sequence in a complete ultrametric abelian group G. The series $\sum_{n\geq 0} a_n$ converges if and only if $\lim_{n\to+\infty} a_n = 0$.*

If $\sum_{n\geq 0} a_n$ converges and s is its sum then

(i) for any bijection $\sigma\colon \mathbb{N} \to \mathbb{N}$ we have $s = \sum_{n\geq 0} a_{\sigma(n)}$,

(ii) for any partition $\mathbb{N} = \coprod_j I_j$ we have $s = \sum_j \left(\sum_{i\in I_j} a_i\right)$.

Proof. For the first part the only if is trivial. To prove the converse let $s_n = \sum_{0\leq i<n} a_i$. Since G is complete we just need to show $(s_n)_{n\in\mathbb{N}}$ is Cauchy:

$$|s_{n+m} - s_n| = |a_n + \cdots + a_{n+m-1}| \leq \max\{|a_n|, \ldots, |a_{n+m-1}|\} \to 0$$

as $n, m \to +\infty$.

The proof of the second part is not so interesting and can be found at [6, p. 75]. □

This last result is much cleaner than the corresponding one in classical analysis: in an ultrametric group if a series converge we are free to exchange and group its terms without changing the sum, unlike in classical analysis, where there is distinction between absolutely convergent and conditionally convergent series. Anyway, in both contexts, grouping terms of a divergent series can produce a convergent one.

From now on we'll mainly work with *ultrametric fields*, fields equipped with an ultrametric norm. Some of these results will be generalizations of facts proved in Chapter 2 with regards to $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Lemma 3.8. *All balls containing 0 in an ultrametric field K are additive subgroups. The dressed ball $B_{\leq 1}(0)$ is a subring of K and the balls $B_{\leq r}(0)$ and $B_{<r}(0)$ (with $r < 1$) are ideals of $B_{\leq 1}(0)$.*

Proof. All these verifications are trivial using the ultrametric inequality. □

Let K be an ultrametric field and let

$$\begin{aligned} A :=& B_{\leq 1}(0) = \{x \in K \mid |x| \leq 1\}, \\ M :=& B_{<1}(0) = \{x \in K \mid |x| < 1\}. \end{aligned}$$

Proposition 3.9. *A is a maximal subring of K and M is the unique maximal ideal of A.*

Proof. If A' is a subring of K such that $A \subsetneq A'$, there exists $y \in A'$ with $|y| = r > 1$, so $y^n \in A'$ for every $n \in \mathbb{N}$. Hence $B_{\leq r^n}(0) = y^n A \subset A'$ $\forall n \in \mathbb{N}$ which implies $K = \bigcup_{n\geq 1} y^n A = A'$ since $r^n = |y|^n \to +\infty$. So A is a maximal subring of K. To see why M is the unique maximal ideal of A we observe that $A = A^\times \sqcup M$, so every ideal which strictly contains M is the whole ring A, because it must contain a unit. □

We note that A is a local ring (by the previous proposition) and a valuation ring of K, since $x \in A \;\vee\; 1/x \in A$ for every $x \in K^\times$. An example we have already studied is $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$ and $M = p\mathbb{Z}_p$.

Definition 3.10. Let K be an ultrametric field, $A = B_{\leq 1}(0)$, $M = B_{<1}(0)$. The quotient $k := A/M$ is the *residue field* of K.

Finally we are ready to prove the representation theorem.

Theorem 3.11. *Let K be a complete ultrametric field, A its maximal subring defined by $|x| \leq 1$. If $\xi \in A$ with $|\xi| < 1$ and $0 \in S \subset A$ is a set of representatives for the classes $A/\xi A$, then every $x \in K^\times$ is a sum*

$$x = \sum_{i \geq m} a_i \xi^i \quad (m \in \mathbb{Z}, a_i \in S, a_m \neq 0)$$

with $m \geq 0$ precisely when $x \in A$. There's an isomorphism $A \cong \varprojlim A/\xi^n A$ defined by $x \mapsto (s_n)$ where $s_n = \sum_{m \leq i < n} a_i \xi^i$.

Proof. If $x \in A$ we can find a unique $a_0 \in S$ such that $x - a_0 \in \xi A$, so we can write

$$x = a_0 + \xi x_1 \quad (x_1 \in A).$$

By induction we obtain

$$x = a_0 + a_1 \xi + a_2 \xi^2 + \cdots + \xi^n x_n \quad (a_i \in S, x_n \in A).$$

Using the same notation of the theorem we have $x = s_n + \xi^n x_n$ and we immediately note that $(s_n)_n$ converges, because it is a Cauchy sequence since $|\xi^n x_n| \leq |\xi|^n \to 0$ as $n \to +\infty$. It can be easily checked that $s_n \to x$, so $x = \sum_{i \geq 0} a_i \xi^i$. Since for every $x \in K^\times$ there exists $k \in \mathbb{Z}$ such that $\left|\xi^k x\right| \leq 1$ we can repeat this reasoning for x starting at index $i = k$. It's now easy to see that the ring morphism $A \to \varprojlim A/\xi^n A$ is an isomorphism, since it is clearly injective and surjective (by completeness of K). □

If K is not complete we could anyway represent every $x \in K$ as $x = \sum_{i \geq m} a_i \xi^i$, but we would only have an injection $A \hookrightarrow \varprojlim A/\xi^n A$. Applying this theorem to $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$ and $\xi = p$ we obtain exactly how p-adic numbers are represented and the fact that $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

3.2 Extension of norms

Let V be a vector space over the field $\mathbb{Q}_p$, equipped with a norm. For example $V = \mathbb{Q}_p$ with norm $\|x\| := c|x|_p$ $(c > 0)$ is a $\mathbb{Q}_p$-vector space; we immediately note that the set $\{\, \|v\| \mid v \in V \,\}$ can be different from the set of the absolute values of scalars (in this case $|\mathbb{Q}_p|_p = p^{\mathbb{Z}} \cup \{0\}$). From now on, to have a lighter notation, we'll omit the pedix p in the p-adic absolute value. We recall that two norms $\| \,\|, \| \,\|'$ on a vector space are equivalent if we can find $0 < c \leq C < +\infty$ such that

$$c\|x\| \leq \|x\|' \leq C\|x\| \quad \forall x \in V.$$

Now we are ready to state and prove the following theorem.

Theorem 3.12. *Let V be a finite-dimensional $\mathbb{Q}_p$-vector space. Then all norms on V are equivalent.*

Proof. Let $n = \dim V$ and $(e_i)_{1 \leq i \leq n}$ be a basis. It's clear that there is an isomorphism $\varphi \colon \mathbb{Q}_p^n \xrightarrow{\sim} V$ sending $(x_i)_{1 \leq i \leq n} \mapsto \sum_i x_i e_i$. We consider $\mathbb{Q}_p^n$ equipped with the sup-norm $\|x\|_\infty := \sup|x_i|_p$. We only need to prove that φ is a homeomorphism.
It's easy to prove that φ is continuous:

$$\|\varphi(x)\| = \left\|\sum x_i e_i\right\| \leq \sum |x_i|_p \|e_i\| \leq \max\|e_i\| \cdot \sum |x_i|_p \leq C\|x\|_\infty$$

where $C := n \cdot \max\|e_i\|$ is a fixed constant. We'll conclude showing that φ is an open map (any continue invertible open map is a homeomorphism). Let $B := \{x \in \mathbb{Q}_p^n \mid \|x\|_\infty \le 1\}$ be the unit ball in $\mathbb{Q}_p^n$: we have to show that $\varphi(B)$ contains an open ball of positive radius centered in $0 \in V$. We firstly note that $B \subset \mathbb{Q}_p^n$ is a compact set: it's possible to extract a convergent subsequence from any sequence, exploiting the fact that $(\mathbb{Q}_p, |\ |_p)$ is a locally compact field. Let's consider the unit sphere in $\mathbb{Q}_p^n$:

$$S_1 := \left\{ x \in \mathbb{Q}_p^n \mid \|x\|_\infty = 1 \right\}.$$

This is a closed subset of B and, since B is compact, S_1 is a compact set hence $\varphi(S_1)$ is also compact. Since φ is bijective we have $0 \notin \varphi(S_1)$ so $0 < \operatorname{dist}(\{0\}, \varphi(S_1))$ and, by Weierstrass theorem, we find a point $\varphi(x_0)$ such that

$$x \in S_1 \implies \|\varphi(x)\| \ge \|\varphi(x_0)\| = \varepsilon > 0.$$

Let $v \in V \setminus \{0\}$ and observe that

$$\|v\| < \varepsilon, \lambda \in \mathbb{Q}_p, |\lambda|_p \le 1 \implies \|\lambda v\| < \varepsilon \implies \lambda v \notin \varphi(S_1).$$

We can write

$$v = \sum_i v_i e_i = \varphi((v_i)_i).$$

Let's assume without loss of generality that $0 \neq |v_n|_p = \max |v_i|_p = \|(v_i)_i\|_\infty$. If $\lambda = 1/v_n$ then $\lambda v = \varphi((v_i/v_n)_i) \in \varphi(S_1)$ so it must be $|\lambda|_p > 1$ which implies

$$\|(v_i)_i\|_\infty = |v_n|_p = \frac{1}{|\lambda|_p} < 1.$$

This shows that $v = \varphi((v_i)_i) \in \varphi(B)$. We have just proved that $B_{<\varepsilon}(0, V) \subseteq \varphi(B)$. □

This theorem can be generalized: it holds for any finite dimensional F-vector space, where F is a locally compact field.

Corollary 3.12.1. *If V and W are two finite-dimensional $\mathbb{Q}_p$-vector spaces and $\alpha\colon V \to W$ is a linear map, then α is continuous.*

This is an analogue to the classic result on real or complex vectorial spaces of finite dimension.

Now let's consider a finite extension $K/\mathbb{Q}_p$ and let's assume there is at least one absolute value on K extending the p-adic absolute value of $\mathbb{Q}_p$. Then we can see K as a $\mathbb{Q}_p$-vectorial space of finite dimension equipped with a norm (every such absolute value on K is actually also a norm).

Proposition 3.13. *There is at most one absolute value on K extending the p-adic one of $\mathbb{Q}_p$.*

Proof. Let $|\ |$ and $|\ |'$ two such absolute values on K. By Theorem 3.12 they must be equivalent norms so there exist constants $0 < c \le C < \infty$ such that

$$c|x| \le |x|' \le C|x| \quad (x \in K).$$

Replacing x^n with x in the previous inequalities we obtain

$$c|x|^n \le |x|'^n \le C|x|^n \implies c^{1/n}|x| \le |x|' \le C^{1/n}|x|.$$

Letting $n \to +\infty$ we have $c^{1/n}, C^{1/n} \to 1$ so $|x| = |x|'$. □

We now know that if $K/\mathbb{Q}_p$ is a finite extension and K admits an absolute value extending the p-adic one, there can only be one such absolute value. Anyway, if $K/\mathbb{Q}_p$ is a generic finite extension we don't know if there is an absolute value on K compatible with the p-adic one. The next theorem will give us an answer (yes, there always is such a field norm) and also a method to define this (unique) absolute value. First we quickly present two technical lemmas we'll need.

Definition 3.14. A *generalized absolute value* on a field K is a group morphism $f\colon K^\times \to \mathbb{R}_{>0}$ extended by $f(0) = 0$ which satisfies $f(x + y) \leq C \max\{f(x), f(y)\}$, where $C > 0$ is a fixed constant. If $C = 1$, f is a classical ultrametric absolute value.

Lemma 3.15. *Let f be a generalized absolute value on a field K. If f is bounded on $\mathbb{N}$ (thought as a subset of K) then f is an ultrametric absolute value.*

Proof. See [6, p. 88]. □

Lemma 3.16. *If V is a locally compact normed space over $\mathbb{Q}_p$ then its dimension is finite. In a locally compact normed $\mathbb{Q}_p$-vector space the compact subsets are the closed bounded subsets.*

Proof. See [6, p. 93]. □

Definition 3.17. Let $K/\mathbb{Q}_p$ be a finite extension, $\alpha \in K$ and ℓ_α be the $\mathbb{Q}_p$-linear map $K \to K : x \mapsto \alpha x$. We define the "Norm"[1] of α on K as

$$\mathbf{N}_{K/\mathbb{Q}_p}(\alpha) := \det \ell_\alpha .$$

Now we are ready to prove the following. Let's recall that $\|K\| = \{\, \|k\| \mid k \in K \,\}$.

Theorem 3.18. *Let K be a field extension of $\mathbb{Q}_p$ of degree $d < \infty$. For each $x \in K$ let $\ell_x\colon K \to K$ the $\mathbb{Q}_p$-linear map $y \mapsto xy$. Then*

$$f(x) := \left|\mathbf{N}_{K/\mathbb{Q}_p}(x)\right|_p^{1/d} = \left|\det \ell_x\right|_p^{1/d}$$

defines an absolute value on K that extends the p-adic one. This is the unique such absolute value.

Proof. First of all it's clear that if $a \in \mathbb{Q}_p$ then $\left|\mathbf{N}_{K/\mathbb{Q}_p}(a)\right|_p^{1/d} = |a|_p$, so the formula correspond to the p-adic absolute value on $\mathbb{Q}_p$. It's also clear that $f(x) = 0 \iff x = 0$ (every $y \mapsto xy$ is invertible if $x \neq 0$) and $f(x \cdot y) = f(x) \cdot f(y)$, thanks to the Binet's formula for det. We only need to check the ultrametric inequality. Let's choose any ultrametric norm $x \mapsto \|x\|$ on K such that $\|K\| = |\mathbb{Q}_p|$ (for example we could choose the sup-norm). Since K is a $\mathbb{Q}_p$-vector space with $\dim K = d$ we know, from Theorem 3.12, that K is homeomorphic to $(\mathbb{Q}_p^d, \| \ \|_\infty)$ so it is locally compact. By Lemma 3.16 we know that the unit sphere $S_1 = \{x \in K \mid \|x\| = 1\}$ is compact so the continuous function f, by Weierstrass theorem, is bounded on S_1, namely

$$0 < \varepsilon \leq f(x) \leq A < +\infty \quad (\|x\| = 1).$$

For $x \in K^\times$ we can find $\lambda \in \mathbb{Q}_p$ such that $\|x/\lambda\| = 1$ so $\varepsilon \leq f(x/\lambda) \leq A$. Since $f(x/\lambda) = f(x)/|\lambda|_p = f(x)/\|x\|$ we get

$$\begin{gathered}\varepsilon\|x\| \leq f(x) \leq A\|x\| \\ \implies \|x\| \leq \varepsilon^{-1} f(x), \quad f(x) \leq A\|x\| \quad (x \in K).\end{gathered}$$

[1] We'll write "Norm" to avoid confusion: we're talking about the field norm in field theory, not about an absolute value on K.

If $f(x) \leq 1$ we have that $\|x\| \leq \varepsilon^{-1}$ and

$$\begin{aligned} f(1+x) &\leq A\|1+x\| \leq A\max\{\|1\|, \|x\|\} \leq \\ &\leq A\max\{\|1\|, \varepsilon^{-1}\} =: C \cdot 1 = C\max\{f(1), f(x)\}. \end{aligned}$$

More generally, if $f(y) \geq f(x)$ then $f(x/y) = f(x)/f(y) \leq 1$ so we can apply our previous results. Multiplying both sides by $f(y)$ we obtain

$$f(x+y) \leq C\max\{f(x), f(y)\}.$$

This proves that f is a generalized absolute value on K. Since f is bounded on $\mathbb{N} \subset \mathbb{Q}_p \subset K$, being an extension of the p-adic absolute value, by Lemma 3.15 we obtain that f is an ultrametric absolute value. □

Corollary 3.18.1. *Let $K/\mathbb{Q}_p$ be a finite Galois extension and $\alpha \in K$. Then the norm of α equals the norm of each of his conjugates, i.e. Galois automorphisms are isometric.*

Proof. Let α' be a conjugate of α and σ a $\mathbb{Q}_p$-automorphism such that $\sigma(\alpha) = \alpha'$ (from Galois theory we know it actually exists). Thanks to Theorem 3.18, we know there exists a unique p-adic norm $\| \ \|$ on K. The map $\| \ \|' \colon K \to \mathbb{R}$ defined by $\|x\|' := \|\sigma(x)\|$ is clearly a field norm on K which extends $| \ |_p$. Hence $\| \ \|' = \| \ \|$ so $\|\alpha\| = \|\alpha'\|$. □

We have proved that for every finite extension $K/\mathbb{Q}_p$ there's a unique norm which extends the p-adic one. We'll now give a more practical method to calculate this norm.

Proposition 3.19. *Let $K/\mathbb{Q}_p$ be a finite extension of degree d. Then*

$$|\alpha|_p = |a_n|_p^{1/n}$$

where $\alpha \in K$ and $a_n \in \mathbb{Q}_p$ is the constant term of the minimal polynomial of α over $\mathbb{Q}_p$ (which has degree n).

Proof. First of all, let's consider the simple case where $K = \mathbb{Q}_p(\alpha)$ (the smallest field containing $\mathbb{Q}_p$ and α), where the minimal polynomial of α on $\mathbb{Q}_p$ is

$$\lambda_{\mathbb{Q}_p}(\alpha) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Q}_p[X].$$

If we use $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ as a $\mathbb{Q}_p$-basis for K then ℓ_α has matrix

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_n \\ 1 & 0 & 0 & \ldots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \ldots & 0 & -a_{n-2} \\ 0 & 0 & 1 & \ldots & 0 & -a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix}$$

where we used $\alpha^n = -a_1\alpha^{n-1} - a_2\alpha^{n-2} - \cdots - a_{n-1}\alpha - a_n$. It's easy to see that $\det \ell_\alpha = (-1)^n a_n$, expanding using the first row. If $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = \prod_{i=1}^n (x - \alpha_i)$, where α_i are the conjugates of $\alpha = \alpha_1$ in $\mathbb{Q}_p$, then $\det \ell_\alpha = \prod_{i=1}^n \alpha_i$.
Now let's consider an arbitrary element $\beta \in K$. It's immediate that

$$\mathbf{N}_{K/\mathbb{Q}_p}(\beta) = \left(\mathbf{N}_{\mathbb{Q}_p(\beta)/\mathbb{Q}_p}(\beta)\right)^{[K:\mathbb{Q}_p(\beta)]}$$

because if we consider $\mathbb{Q}_p \leq \mathbb{Q}_p(\beta) \leq K$ and we first choose a basis for $\mathbb{Q}_p(\beta)$ over $\mathbb{Q}_p$ and then a basis for K over $\mathbb{Q}_p(\beta)$, we can then take all products of elements of these two basis and obtain a basis for K over $\mathbb{Q}_p$ (this is exactly the idea used to prove $[K:\mathbb{Q}_p]=[K:\mathbb{Q}_p(\beta)]\cdot[\mathbb{Q}_p(\beta):\mathbb{Q}_p]$). In this basis the matrix of ℓ_β has form

$$\begin{pmatrix} A_\beta & 0 & & \\ 0 & A_\beta & & \\ & & \ddots & \\ & & & A_\beta \end{pmatrix}$$

where A_β is the matrix of the multiplication by β in $\mathbb{Q}_p(\beta)$. The determinant of this matrix is clearly $(\det A_\beta)^{[K:\mathbb{Q}_p(\beta)]}$, since there are exactly $[K:\mathbb{Q}_p(\beta)]$ blocks. Finally, if $\alpha\in K$ has minimal polynomial $\lambda_{\mathbb{Q}_p}(\alpha)=x^n+\cdots+a_{n-1}x+a_0$ we obtain

$$|\alpha|_p=\left|\mathbf{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p^{1/d}=\left|\mathbf{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|_p^{[K:\mathbb{Q}_p(\alpha)]/d}=\left|\mathbf{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|_p^{1/n}=|a_n|_p^{1/n}$$

where we used $d=[K:\mathbb{Q}_p(\alpha)]\cdot n$. □

3.3 Field extensions of $\mathbb{Q}_p$

Definition 3.20. Let $K/\mathbb{Q}_p$ be a finite extension. The set

$$A:=\{\alpha\in K\mid \exists(a_i)\subset\mathbb{Z}_p \text{ such that } \alpha^n+a_1\alpha^{n-1}+\cdots+a_{n-1}\alpha+a_n=0\}$$

is called the *integral closure* of $\mathbb{Z}_p$ in K.

It can be shown that if $\alpha\in A$ then its minimal polynomial over $\mathbb{Q}_p$ has the above form, i.e. coefficients in $\mathbb{Z}_p$. Moreover, the integral closure is always a ring. We'll prove it only in our special case.

Proposition 3.21. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n and let*

$$A=\{x\in K\mid |x|_p\le 1\},$$
$$M=\{x\in K\mid |x|_p<1\}.$$

Then A is a ring, which is exactly the integral closure of $\mathbb{Z}_p$ in K. M is the maximal ideal of A and A/M is a finite extension of $\mathbb{F}_p$ of degree at most n.

Proof. Thanks to Theorem 3.18 we know that there exists a p-adic absolute value on K, which makes it an ultrametric field. Then we can apply Proposition 3.9, which states that A is the maximal subring of K and M is its maximal ideal.
Now let $\alpha\in K$ have degree m over $\mathbb{Q}_p$ and suppose it is integral over $\mathbb{Z}_p$, i.e.

$$\alpha^m+a_1\alpha^{m-1}+\ldots a_{m-1}\alpha+a_m=0\quad(a_i\in\mathbb{Z}_p).$$

If $|\alpha|_p>1$ then we would have

$$|\alpha|_p^m=\left|a_1\alpha^{m-1}+\cdots+a_m\right|_p\le\max_{1\le i\le m}\left|a_i\alpha^{m-i}\right|_p\le\max_{1\le i\le m}\left|\alpha^{m-i}\right|_p=|\alpha|_p^{m-1}$$

which is a contradiction. Conversely, let $\alpha\in K$ with $|\alpha|_p\le 1$. Then, thanks to Corollary 3.18.1, all the conjugates of $\alpha=\alpha_1$ over $\mathbb{Q}_p$ have the same norm

$$|\alpha_i|_p=\prod_{j=1}^m|\alpha_j|_p^{1/m}=|\alpha|_p\le 1.$$

Since all coefficients in $\lambda_{\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p[X]$ are sums or differences of products of α_i (more exactly they're the symmetric polynomials evaluated in (α_i)) it follows that they also have $|\ |_p \leq 1$ so they're in $\mathbb{Z}_p$. We have proved that A is exactly the integral closure of $\mathbb{Z}_p$ in K.
To prove that A/M is a finite extension of $\mathbb{F}_p$ let's consider the map

$$\mathbb{Z}_p/p\mathbb{Z}_p \to A/M : a + p\mathbb{Z}_p \mapsto a + M \quad (a \in \mathbb{Z}_p).$$

It's well defined, since if $a - b \in p\mathbb{Z}_p \subset M$ then $a - b \in M$ so $a + M = b + M$. It is also injective, thanks to the fact that $M \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Then we have an inclusion $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow A/M$, which proves that A/M is an extension of $\mathbb{F}_p$. Finally, to prove that $[A/M : \mathbb{F}_p] \leq n$ we just need to show that any $n+1$ elements $\overline{a_1}, \overline{a_2}, \dots, \overline{a_{n+1}} \in A/M$ are linearly dependent on $\mathbb{F}_p$. Let $a_i \in A$ be any element such that $\overline{a_i} = a_i + M$, for $i = 1, 2, \dots, n+1$. By hypothesis $n = [K : \mathbb{Q}_p]$ so the elements $a_1, \dots, a_{n+1}$ are linearly dependent on $\mathbb{Q}_p$, i.e.

$$a_1 b_1 + a_2 b_2 + \cdots + a_{n+1} b_{n+1} = 0 \qquad (b_i \in \mathbb{Q}_p, \exists j : b_j \neq 0).$$

We can assume that every coefficient is in $\mathbb{Z}_p \subset A$ but at least one b_i is not in $p\mathbb{Z}_p$ (we can multiply by a suitable power of p). Then the image of this expression in A/M is

$$\overline{a_1} \cdot \overline{b_1} + \overline{a_2} \cdot \overline{b_2} + \cdots + \overline{a_{n+1}} \cdot \overline{b_{n+1}} = 0$$

where $\overline{b_i}$ is the image of b_i in $\mathbb{Z}_p/p\mathbb{Z}_p$ by the standard projection. Since at least one b_i is not in $p\mathbb{Z}_p$ we have that at least one $\overline{b_i}$ is not 0, so $\overline{a_1}, \overline{a_2}, \dots, \overline{a_{n+1}}$ are linearly dependent on $\mathbb{F}_p$. □

Let's denote $|K^\times|_p := \left\{ |x|_p \,\middle|\, x \in K^\times \right\} \leq \mathbb{R}_{>0}$ and $p^{\mathbb{Z}} = \{ p^z \mid z \in \mathbb{Z} \} = \left|\mathbb{Q}_p^\times\right|_p$. They're clearly two multiplicative groups and $\left|\mathbb{Q}_p^\times\right|_p \leq |K^\times|_p$.

Definition 3.22. Let $K/\mathbb{Q}_p$ be a finite extension. Using the same notations as above for A and M, $k := A/M$ is called the *residue field* of K, $f := [k : \mathbb{F}_p] = \dim_{\mathbb{Q}_p} k$ is called the *residue degree* and $e := \left(|K^\times|_p : \left|\mathbb{Q}_p^\times\right|_p\right)$ is called the *ramification index.*

If $K/\mathbb{Q}_p$ is an extension of degree n, we can extend to K the function $\operatorname{ord}_p : \mathbb{Q}_p \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ defined in Section 2.4: if $\alpha \in K$ then

$$\operatorname{ord}_p \alpha := -\log_p |\alpha|_p = -\log_p \left|\mathbf{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p^{1/n} = -\frac{1}{n} \log_p \left|\mathbf{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p$$

with the usual convention $\log_p 0 = -\infty$. Clearly this definition agrees with the old one when $\alpha \in \mathbb{Q}_p$ and has the usual property $\operatorname{ord}_p \alpha\beta = \operatorname{ord}_p \alpha + \operatorname{ord}_p \beta$. Let's observe that fixed $\alpha \in K$, the number $\operatorname{ord}_p \alpha$ doesn't depend on the choice of K: for every field J such that $\alpha \in J$ and $[J : \mathbb{Q}_p] < +\infty$, $\operatorname{ord}_p \alpha$ is the same. The image of $K^\times$ under the map ord_p is a non-trivial additive subgroup of $(1/n)\mathbb{Z} = \{ x \in \mathbb{Q} \mid nx \in \mathbb{Z} \}$ which contains $\mathbb{Z}$: it must be of the form $(1/e)\mathbb{Z}$ for some positive integer e dividing n. The name e is not randomly chosen: it is exactly the ramification index of $K/\mathbb{Q}_p$.

Proposition 3.23. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. Then $n = e \cdot f$.*

Proof. Let's choose $\pi \in K$ such that $\operatorname{ord}_p \pi = 1/e$ and a family $(s_i)_{1 \leq i \leq f}$ in A such that the images $\widetilde{s_i} \in k$ make up a basis of k over $\mathbb{F}_p$. We claim that

$$\left\{ s_i \pi^j \,\middle|\, 1 \leq i \leq f, 0 \leq j < e \right\}$$

is a basis for K over $\mathbb{Q}_p$. Let's first prove independence over $\mathbb{Q}_p$. Let's consider a non-trivial linear combination

$$\sum_{i,j} c_{ij} s_i \pi^j = \sum_j x_j \pi^j \qquad (c_{ij} \in \mathbb{Q}_p)$$

where $x_j = \sum_i c_{ij} s_i$. For every j there's an index $\ell = \ell(j)$ such that

$$|c_{\ell j}|_p \geq |c_{ij}|_p \quad \text{for all } i$$

so $x_j / c_{\ell j} = \sum_i (c_{ij}/c_{\ell j}) s_i = \sum_i \gamma_i s_i$ is a non trivial linear combination with coefficients in A and $\gamma_\ell = 1$ (clearly we're considering only the cases in which $c_{\ell j} \neq 0$ and there is at least one such case by assumption). We can consider this relation in the residue field k. Let $\widetilde{\gamma_i}$ be the image of γ_i in k; since by hypothesis $(\widetilde{s_i})_i$ is a basis for k over $\mathbb{F}_p$ we have

$$0 \neq \sum_i \widetilde{\gamma_i} \widetilde{s_i} \in A/M$$

simply because $\widetilde{\gamma_\ell} = 1$. Hence

$$\sum_i \gamma_i s_i \notin M \implies \left| \sum_i \gamma_i s_i \right|_p = 1$$

and $|x_j|_p = |c_{\ell j}|_p \in \left|\mathbb{Q}_p^\times\right|_p$ is an integer power of p. There is no competition among the absolute values of the distinct terms $x_j \pi^j$, so, by Proposition 3.6, we obtain

$$\sum_{i,j} c_{ij} s_i \pi^j = \sum_j x_j \pi^j \neq 0$$

and this proves the linear independence.
Now we have to show that the family $(s_i \pi^j)_{i,j}$ generates the $\mathbb{Q}_p$-vector space K. We recall that every finite extension of $\mathbb{Q}_p$ is complete, since $(\mathbb{Q}_p^n, \| \, \|_\infty)$ is complete for each $n \in \mathbb{N}$ and all norms on it are equivalent (see Theorem 3.12). To do this we'll use the Representation Theorem 3.11 for the complete field K and the element $\xi = p \in M \subset A$. In this case $A/pA = A/\pi^e A$ (which is of course different from $A/M = A/\pi A$) is finite with representatives

$$\mathcal{S} = \left\{ \sum_{1 \leq i \leq f, 0 \leq j < e} c_{ij} s_i \pi^j \;\middle|\; c_{ij} \in \{0, 1, \ldots, p-1\} \right\}.$$

Hence every element $x \in A$ can be written as a series

$$x = \sum_{h \geq 0} c_h p^h \quad (c_h \in \mathcal{S}).$$

If we write explicit expressions for the coefficients

$$c_h = \sum_{\substack{1 \leq i \leq f \\ 0 \leq j < e}} c_{ijh} s_i \pi^j \in \mathcal{S}$$

we obtain

$$x = \sum_{h \geq 0} \sum_{\substack{1 \leq i \leq f \\ 0 \leq j < e}} c_{ijh} s_i \pi^j p^h.$$

Since $\lim_{h \to +\infty} p^h = 0$, thanks to Proposition 3.7, this family is summable and we can re-arrange its terms to obtain

$$x = \sum_{\substack{1 \leq i \leq f \\ 0 \leq j < e}} \left(\sum_{h \geq 0} c_{ijh} p^h \right) \cdot s_i \pi^j$$

but $c_{ij} := \sum_{h \geq 0} c_{ijh} p^h \in \mathbb{Z}_p$ and $x = \sum_{i,j} c_{ij} s_i \pi^j$. This proves that the ef elements $(s_i \pi^j)$ generates K: if $x \notin A$ there exists $\ell \in \mathbb{N}$ such that $p^\ell x \in A$ so can repeat the process above and then multiply every c_{ij} by $p^{-\ell}$, obtaining $c_{ij} \in \mathbb{Q}_p$. □

Definition 3.24. Let $K/\mathbb{Q}_p$ be a finite extension. $K/\mathbb{Q}_p$ is said to be

- *unramified* when $e = 1$, i.e. $[K : \mathbb{Q}_p] = f$;
- *totally ramified* when $f = 1$, i.e. $[K : \mathbb{Q}_p] = e$.

We'll now study some properties of finite extensions of $\mathbb{Q}_p$, focusing on these two particular cases. We now need an analogue of the famous Eisenstein's criterion, but on $\mathbb{Z}_p$.

Proposition 3.25. *Let $f(X) \in \mathbb{Z}_p[X]$ be a polynomial satisfying*

$$\begin{gathered} f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \\ a_0 \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p, \\ a_i \in p\mathbb{Z}_p \qquad (1 \leq i \leq n-1). \end{gathered}$$

Then f is irreducible in $\mathbb{Z}_p[X]$ and in $\mathbb{Q}_p[X]$.

Proof. By Gauss's lemma we just need to prove that f is irreducible in $\mathbb{Z}_p[X]$. Let's consider a factorization $f = g \cdot h$ in $\mathbb{Z}_p[X]$ with

$$g = b_l X^l + \cdots + b_0, \qquad h = c_m X^m + \cdots + c_0.$$

Hence

$$l + m = n, \qquad b_l c_m = 1, \qquad b_0 c_0 = a_0.$$

Since $a_0 \in p\mathbb{Z}_p$ is not divisible by p^2 we can assume without loss of generality that $p \mid c_0$ and $p \nmid b_0$. Let's consider these polynomials in $\mathbb{Z}_p/p\mathbb{Z}_p[X]$: by assumption $\widetilde{f} = X^n$ so its factorization $\widetilde{f} = \widetilde{g} \cdot \widetilde{h}$ must also be a product of monomials. Hence $\widetilde{g} = b_0$ is a constant and, since $b_l c_m = 1$, we obtain $m = 0$. We have proved that every factorization of f in $\mathbb{Z}_p[X]$ is trivial, hence f is irreducible. □

This criterion can be easily generalized: if $K/\mathbb{Q}_p$ is a finite extension of degree $n = e \cdot f$ then we can replace $\mathbb{Z}_p$ with A, $p\mathbb{Z}_p$ with πA (where $\pi \in K$ is such that $\operatorname{ord}_p \pi = 1/e$) and $p^2\mathbb{Z}_p$ with $\pi^2 A$ (here A is the maximal subring of K, as in the usual notation).

Definition 3.26. A monic polynomial $f(X) \in \mathbb{Z}_p[X]$ of degree $n \geq 1$ satisfying

$$f(X) \equiv X^n \mod p, \qquad f(0) \not\equiv 0 \mod p^2.$$

is called an *Eisenstein polynomial.*

Proposition 3.27. *If $K/\mathbb{Q}_p$ is a totally ramified finite extension and $\pi \in K$ is such that* $\operatorname{ord}_p \pi = 1/e$ *then π is root of an Eisenstein polynomial*

$$f(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0, \qquad a_i \in \mathbb{Z}_p$$

and $K = \mathbb{Q}_p(\pi)$. Conversely, if α is a root of an Eisenstein polynomial of degree e then $\mathbb{Q}_p(\alpha)$ is totally ramified over $\mathbb{Q}_p$ and $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = e$.

Proof. For the first implication let's consider the minimal polynomial of π over $\mathbb{Q}_p$

$$\lambda_{\mathbb{Q}_p}(\pi) = X^h + b_{h-1}X^{h-1} + \cdots + b_1 X + b_0.$$

Its degree h must be equal to e: obviously $h \leq e$ since $[\mathbb{Q}_p(\pi) : \mathbb{Q}_p] \leq [K : \mathbb{Q}_p] = e$; we'll see why it cannot be strictly less then e. Let's observe that its coefficients b_i are the symmetric polynomials evaluated in the conjugates of π, all of which have $|\ |_p = |\pi|_p = p^{-1/e}$, so $|b_i|_p < 1$, which means $b_i \in p\mathbb{Z}_p$. As for b_0, we have

$$|b_0|_p = |\pi|_p^h = p^{-h/e}$$

and since $b_0 \in \mathbb{Q}_p$ we must have $|b_0|_p \in p^{\mathbb{Z}}$ so $e|h \implies h = e$. Then $|b_0|_p = 1/p$ so $b_0 \in p\mathbb{Z}_p \backslash p^2\mathbb{Z}_p$. We have proved that $K = \mathbb{Q}_p(\pi)$ and $\lambda_{\mathbb{Q}_p}(\pi) \in \mathbb{Z}_p[X]$ is an Eisenstein polynomial.
Conversely, if $\mathbb{Z}_p[X] \ni f(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$ is an Eisenstein polynomial, we know it is irreducible by Proposition 3.25, so if we adjoin a root α to $\mathbb{Q}_p$ we obtain an extension of degree $e = \deg f$. Since, by assumption, $\operatorname{ord}_p a_0 = 1$ we obtain $\operatorname{ord}_p \alpha = (1/e)\operatorname{ord}_p a_0 = 1/e$ hence $\mathbb{Q}_p(\alpha)$ is totally ramified over $\mathbb{Q}_p$. □

Proposition 3.28. *There is exactly one unramified extension K_f^{unram} of $\mathbb{Q}_p$ of degree f and it can be obtained by adjoining a primitive $(p^f - 1)$th root of 1. If K is an extension of $\mathbb{Q}_p$ of degree n, index of ramification e and residue degree f, then $K = K_f^{unram}(\pi)$, where π satisfies an Eisenstein polynomial with coefficients in K_f^{unram}.*

Proof. Let's first prove that there exists at least one unramified extension of $\mathbb{Q}_p$ of degree f. Let $\overline{\alpha}$ be a generator of the cyclic group $\mathbb{F}_{p^f}^\times$ and let $\overline{P}(X) = X^f + \overline{a_1}X^{f-1} + \cdots + \overline{a_f} \in \mathbb{F}_p[X]$ be its minimal polynomial. For every $i = 1, \ldots, f$ let's consider $a_i \in \mathbb{Z}_p$ which reduces to $\overline{a_i}$ mod p and let $P(X) = X^f + a_1X^{f-1} + \cdots + a_f \in \mathbb{Z}_p[X]$. This polynomial is clearly irreducible in $\mathbb{Z}_p[X]$ (otherwise its reduction $\overline{P}(X)$ could be factorized in $\mathbb{F}_p[X]$) so, by Gauss's lemma, $P(X)$ is irreducible in $\mathbb{Q}_p[X]$. Let $\alpha \in \mathbb{Q}_p^{\text{alg cl}}$ be a root of $P(X)$ (clearly $\alpha \notin \mathbb{Q}_p$) and let $\widetilde{K} := \mathbb{Q}_p(\alpha)$, $\widetilde{A} := \{x \in \widetilde{K} \mid |x|_p \leq 1\}$, $\widetilde{M} := \{x \in \widetilde{K} \mid |x|_p < 1\}$. Then $[\widetilde{K} : \mathbb{Q}_p] = f$ and the coset $\alpha + \widetilde{M} \in \widetilde{A}/\widetilde{M}$ is a root of the irreducible polynomial $\overline{P}(X)$ over $\mathbb{F}_p$. Hence $[\widetilde{A}/\widetilde{M} : \mathbb{F}_p] = f$ which implies $\widetilde{K}$ is an unramified extension of $\mathbb{Q}_p$ of degree f.
Now we prove uniqueness. Let K be as in the statement, let A be the valuation ring of $| \;|_p$ in K and let M be the maximal ideal of A. Since f is the residue degree of K we have $A/M = \mathbb{F}_{p^f}$. We'll now prove that any $\beta \in \mathbb{F}_{p^f}^\times$ admits a *Teichmüller representative*, i.e. an $\omega(\beta) \in A$ such that it is a solution of $X^{p^f} - X = 0$ congruent to β mod M. We'll focus on the case in which β is a generator of $\mathbb{F}_{p^f}^\times$ (so some properties we'll find will be valid only in this case).
Let $\overline{\alpha}$ be a generator of $\mathbb{F}_{p^f}^\times$ and let $\alpha_0 \in A$ be any element which reduces to $\overline{\alpha}$ mod M. Finally, let $\pi \in K$ be any element with $\operatorname{ord}_p \pi = 1/e$; thus $M = \pi A$. We claim that there exists $A \ni \alpha \equiv \alpha_0$ mod M such that $\alpha^{p^f-1} - 1 = 0$ (now we only know that $\alpha_0^{p^f-1} - 1 \equiv 0 \mod \pi$). The proof is an Hensel's lemma type argument. First of all we write $\alpha \equiv \alpha_0 + \alpha_1\pi \mod \pi^2$ and we want to find $\alpha_1 \in A$ such that $(\alpha_0 + \alpha_1\pi)^{p^f-1} - 1 \equiv 0 \mod \pi^2$. Using Newton's binomial and recalling that we're operating in a ring of characteristic p, namely A/π^2A, we obtain

$$0 \equiv (\alpha_0 + \alpha_1\pi)^{p^f-1} - 1 \equiv \alpha_0^{p^f-1} - 1 - \alpha_1\pi\alpha_0^{p^f-2} \mod \pi^2.$$

Since $\alpha_0^{p^f-1} \equiv 1 \mod \pi$ we can set

$$\alpha_1 \equiv \frac{\alpha_0^{p^f-1} - 1}{\pi\alpha_0^{p^f-2}} \equiv \alpha_0 \cdot \frac{\alpha_0^{p^f-1} - 1}{\pi} \mod \pi$$

and we obtain the desired congruence mod π^2, which represents a better approximation of the solution. Continuing in this way, just as in Hensel's lemma, we find $A \ni \alpha = \alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \ldots$ such that $\alpha^{p^f-1} = 1$. We immediately note that α is a primitive $(p^f - 1)$th root of 1 because $\alpha, \alpha^2, \ldots, \alpha^{p^f-1}$ are all distinct (their reductions mod M $\overline{\alpha}, \overline{\alpha}^2, \ldots, \overline{\alpha}^{p^f-1}$ are all distinct by assumption). We also observe that $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geq f$. In-fact, let $G(X) := \lambda_{\mathbb{Q}_p}(\alpha)$ be the minimal polynomial of α on $\mathbb{Q}_p$ and consider $0 \neq \overline{G}(X) \in \mathbb{F}_p[X]$, its reduction mod p (recall that $|\alpha|_p = 1$ so $G(X) \in \mathbb{Z}_p[X]$); by assumption $\alpha + M = \overline{\alpha}$ so $G(\alpha) = 0 \implies \overline{G}(\overline{\alpha}) = 0$. By hypothesis the minimal polynomial of $\overline{\alpha}$ in $\mathbb{F}_p$ is $\overline{P}(X)$ so

$$\overline{P}(X) \mid \overline{G}(X) \implies \deg \overline{G}(X) \geq \deg \overline{P}(X) = f \implies \deg G(X) \geq f$$

so $[\mathbb{Q}_p(\alpha):\mathbb{Q}_p] = \deg G(X) \geq f$. We can apply this discussion to any $\widetilde{K}$ unramified extension of $\mathbb{Q}_p$ of degree f (for example the one we have built at the beginning). Hence, $\mathbb{Q}_p(\alpha) \subseteq \widetilde{K}$, where $\widetilde{K} \ni \alpha$ is a primitive (p^f-1)th root of 1. We have

$$f = [\widetilde{K}:\mathbb{Q}_p] \geq [\mathbb{Q}_p(\alpha):\mathbb{Q}_p] \geq f$$

so $\widetilde{K} = \mathbb{Q}_p(\alpha)$. This implies that the unramified extension of degree f is unique, let's call it K_f^{unram}.

Now let $K/\mathbb{Q}_p$ be a generic finite extension of degree $n = ef$, as in the statement. Let $E(X)$ be the minimal polynomial of π over $K_f^{\text{unram}} \leq K$. Let $\{\pi_j\}_j$ be the conjugates of π over K_f^{unram} (in a suitable extension of K). Then

$$E(X) = \prod_j (X - \pi_j) = X^d + b_{d-1}X^{d-1} + \dots b_1 X + b_0.$$

Let $d = \deg E(X)$ and $c = b_0$ be the constant term of $E(X)$. Every b_i is a symmetric polynomial evaluated in the conjugates of π: by the ultrametric inequality, since $|\pi_j|_p = |\pi|_p = p^{-1/e}$, we obtain $|b_i|_p < 1$ for every $i = 1, \dots, d-1$. Since $b_i \in K_f^{\text{unram}}$ we have $\operatorname{ord}_p b_i \in \mathbb{Z}$ so it must be $\operatorname{ord}_p b_i \geq 1$, i.e. p divides b_i. Instead, the constant term has order $\operatorname{ord}_p c = d \cdot \operatorname{ord}_p \pi = d/e \in \mathbb{Z}$; we recall that $d = [K_f^{\text{unram}}(\pi) : K_f^{\text{unram}}] \leq [K : K_f^{\text{unram}}] = e$ so the only possibility is that $d = e$ and $\operatorname{ord}_p c = 1$, i.e. p divides c but p^2 does not. This proves that $E(X)$ is an Eisenstein polynomial over K_f^{unram} and $K = K_f^{\text{unram}}(\pi)$. □

We have an important "structural" corollary of this proposition.

Corollary 3.28.1. *If K is a finite extension of $\mathbb{Q}_p$ of degree $n = ef$ and $\pi \in K$ is chosen so that $\operatorname{ord}_p \pi = 1/e$, then every $\alpha \in K$ can be written in one and only one way as*

$$\sum_{i=m}^{+\infty} a_i \pi^i$$

where $m = e \cdot \operatorname{ord}_p \alpha$ and every a_i satisfies $a_i^{p^f} = a_i$ (the a_i are called Teichmüller digits*).*

Proof. Let A be the maximal subring of K and M be its maximal ideal; $\pi \in K$ is such that $|\pi|_p = p^{-1/e} < 1$ so $M = \pi A$ and we already know, by definition, that $A/\pi A = \mathbb{F}_{p^f}$. Let's choose p^f representatives $0 = a_1, a_2, \dots, a_{p^f} \in A$ for $A/\pi A$ such that $a_i^{p^f} = a_i$ (we can apply an Hensel's lemma type argument). We can then apply Theorem 3.11 and conclude. □

Let's observe that we could apply this corollary to $\mathbb{Q}_p$ itself but we would not obtain the same representation in power series we used: in-fact we would obtain the so called representation with Teichmüller digits where every a_i is 0 or a $(p-1)$th root of unity (in $\mathbb{Z}_p$). This is the more convenient way to write elements of $\mathbb{Z}_p$ and $\mathbb{Q}_p$: using these digits we have closed formulas for addition and multiplication, which are very hard to find if one uses digits in $\{0, \dots, p-1\} \subset \mathbb{Z}$, due to the problem of carrying. We'll not study these formulas, we'll only try to describe very briefly how to derive the Teichmüller representation beginning with the old one. First, for every $\zeta \in \mathbb{F}_p$ we have to find a solution of $X^p - X = 0$ in $\mathbb{Z}_p$ which is equivalent to $\zeta \mod p$: we can always find such a solution thanks to Hensel's lemma. We have defined the *Teichmüller character* $\omega\colon \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ (clearly a group morphism), which we can extend sending 0 to 0 to define a section of the canonical projection $\pi\colon \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/p\mathbb{Z}_p \equiv \mathbb{F}_p$. Now, given $x \in \mathbb{Z}_p$ such that

$$x = x_0 + x_1 p^1 + x_2 p^2 + \dots \qquad (x_i \in \{0, \dots, p-1\})$$

we consider, with a little abuse of notation, $\omega(x_0) \in \mathbb{Z}_p$; since, by definition, $\omega(x_0) \equiv x_0 \mod p$ we have $x - \omega(x_0) \equiv 0 \mod p$ so

$$x - \omega(x_0) = x'_1 p + x'_2 p^2 + x'_3 p^3 + \dots \qquad (x'_i \in \{0, \dots, p-1\}).$$

Then we can consider $\omega(x_1') \in \mathbb{Z}_p$ and obtain $x - \omega(x_0) - \omega(x_1')p \equiv 0 \mod p^2$ and iterating this process we get the Teichmüller digits of x.

Getting back to the study of algebraic extensions of $\mathbb{Q}_p$, we can conclude that the finite unramified extensions of $\mathbb{Q}_p$ are precisely the extensions obtained by adjoining roots of 1 of order not divisible by p: in-fact if m and p are coprime then there exists $f \in \mathbb{Z}$ such that $p^f - 1 = mm'$ with $m' \in \mathbb{Z}$ (for example we can choose f equal to the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$); adjoining to $\mathbb{Q}_p$ a primitive $(p^f - 1)$th root of 1, let it be α, we obtain that $\alpha^{m'}$ is a primitive m-th root of 1.

3.4 The algebraic closure of $\mathbb{Q}_p$ and its completion $\mathbb{C}_p$

Definition 3.29. The union of all the finite unramified extensions of $\mathbb{Q}_p$ is $\mathbb{Q}_p^{\text{unram}}$ and it's called the *maximal unramified extension of* $\mathbb{Q}_p$.

Obviously $\mathbb{Q}_p^{\text{unram}}$ is well defined: given K_f and $K_{f'}$, two unramified extensions of $\mathbb{Q}_p$ of degree f and f' respectively, there exists a (unique) unramified extension $K_{ff'}$ which contains both of them (because $(p^{ff'} - 1)$ is divided by $(p^{f'} - 1)$ and $(p^f - 1)$). There's an obvious extension of the p-adic absolute value to $\mathbb{Q}_p^{\text{unram}}$ so we can define its valuation ring

$$\mathbb{Z}_p^{\text{unram}} := \{x \in \mathbb{Q}_p^{\text{unram}} \mid |x|_p \leq 1\}.$$

It admits a unique maximal ideal $p\mathbb{Z}_p^{\text{unram}} = \{x \in \mathbb{Q}_p^{\text{unram}} \mid |x|_p < 1\}$. It is easily seen that the residue field $\mathbb{Z}_p^{\text{unram}}/p\mathbb{Z}_p^{\text{unram}}$ is $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. Every $\overline{x} \in \overline{\mathbb{F}}_p$ has a unique Teichmüller representative $x \in \mathbb{Z}_p^{\text{unram}}$ such that x has image $\overline{x}$ in $\overline{\mathbb{F}}_p$ and x is a root of 1 (more precisely if $\overline{x} \in \mathbb{F}_{p^f}$, then $x^{p^f} = x$). For this reason $\mathbb{Z}_p^{\text{unram}}$ is often called the "lifting to characteristic 0 of $\overline{\mathbb{F}}_p$".

Proposition 3.30. *The field $\mathbb{Q}_p$ is not algebraically closed.*

Proof. Using the p-adic Heisenstein's criterion (Proposition 3.25) we can find irreducible polynomials in $\mathbb{Q}_p[X]$ of any degree, for example $X^n - p$. □

Although this fact was already obvious, from the proof we infer that an algebraic closure of $\mathbb{Q}_p$ can't have finite degree over $\mathbb{Q}_p$.

Definition 3.31. The algebraic closure of $\mathbb{Q}_p$ is called $\mathbb{Q}_p^{\text{alg cl}}$.

Clearly, there's a unique extension of the p-adic absolute value to $\mathbb{Q}_p^{\text{alg cl}}$, since we can extend it to every finite extension of $\mathbb{Q}_p$, so $\mathbb{Q}_p^{\text{alg cl}}$ is an ultrametric field. We'll see that it is not complete.

We now state and prove two technical lemmas we'll need in the next theorems.

Lemma 3.32. *Let $K/\mathbb{Q}_p$ be a finite extension and $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in K[X]$. If $C_0 = \max_i |b_i|_p$ then there exists a constant C_1, which depends only on C_0, such that every root β of $g(X)$ satisfies $|\beta|_p < C_1$.*

Proof. We claim that $C_1 = 1 + \max_{0 \leq i < n} C_0^{1/i}$ is a suitable constant. Let β be a root of $g(X)$, i.e.

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_1\beta + b_0 = 0.$$

By the competitivity of the absolute value, Proposition 3.6, we know that there are two distinct terms in this sum which attain maximum absolute value. We can distinguish two cases:

- $|\beta^n|_p \leq |b_0|_p$: then $|\beta|_p \leq C_0^{1/n} < C_1$.
- $|\beta^n|_p \leq |b_i\beta^i|_p$ for some $1 \leq i < n$: then $|\beta|_p \leq C_0^{1/(n-i)} < C_1$.

So we can conclude that the chosen C_1 satisfies the request. □

Let's now generalize the notion of congruence mod p^n: if $K/\mathbb{Q}_p$ is a finite extension and $\alpha, \beta \in K$, the writing $\alpha \equiv \beta \mod p^n$ means $|\alpha - \beta|_p \leq p^{-n}$. It's immediately seen that this is exactly our old definition of congruence when $K = \mathbb{Q}_p$.

Lemma 3.33. *Let ξ be algebraic of degree n over $\mathbb{Q}_p$. Then there exists an integer N such that ξ does not satisfy any congruence*

$$a_{n-1}\xi^{n-1} + a_{n-2}\xi^{n-2} + \cdots + a_1\xi + a_0 \equiv 0 \mod p^N$$

where the a_i are in $\mathbb{Z}_p$ and there is at least one coefficient in $\mathbb{Z}_p^\times$.

Proof. Let's consider the space $\mathbb{Z}_p^n \setminus (p\mathbb{Z}_p)^n \subset \mathbb{Z}_p^n$: it is compact since it's a closed subset of the compact space $\mathbb{Z}_p^n$ ($p\mathbb{Z}_p$ is open in $\mathbb{Z}_p$ and, by definition of product topology, also $(p\mathbb{Z}_p)^n$ is open in $\mathbb{Z}_p^n$). Let's consider the sets

$$X_m := \left\{ \left(a_{n-1}^{(m)}, \ldots, a_0^{(m)}\right) \in \mathbb{Z}_p^n \setminus (p\mathbb{Z}_p)^n \,\middle|\, a_{n-1}^{(m)}\xi^{n-1} + \cdots + a_0^{(m)} \equiv 0 \mod p^m \right\}$$

for every $m \in \mathbb{N}$. We claim that X_m is compact. To prove it, we can just show that X_m is closed. Let's consider the function

$$g \colon \mathbb{Z}_p^n \setminus (p\mathbb{Z}_p)^n \to \mathbb{R}_{\geq 0}, \quad g(x_0, \ldots, x_{n-1}) := \left|x_{n-1}\xi^{n-1} + \cdots + x_0\right|_p.$$

Clearly it is a continuous function and it's easily seen that $X_m = g^{-1}\left([0, p^{-(m+1)}]\right)$ so X_m is closed. Now, let's suppose the thesis is false, which means exactly that $X_m \neq \emptyset$ for every $m \in \mathbb{N}$. Obviously $X_{m+1} \subseteq X_m$ so we have a decreasing sequence of non-empty compact sets and we can consider

$$X := \bigcap_{m \in \mathbb{N}} X_m.$$

This intersection is not empty: it is well known that a decreasing intersection of non-empty compact sets is non-empty (in this case we can choose a sequence $(a_i)_i$ with $a_i \in X_i$ and by a diagonal argument we can extract a convergent subsequence with limit in X). Let $(b_{n-1}, \ldots, b_0) \in X$, then

$$\begin{aligned} b_{n-1}\xi^{n-1} + b_{n-2}\xi^{n-2} + \cdots + b_1\xi + b_0 \equiv 0 \mod p^m \qquad \forall m \in \mathbb{N} \\ \implies b_{n-1}\xi^{n-1} + b_{n-2}\xi^{n-2} + \cdots + b_1\xi + b_0 = 0. \end{aligned}$$

That's a contradiction, since ξ has degree n over $\mathbb{Q}_p$. □

We now present two useful propositions.

Proposition 3.34 (Krasner's Lemma). *Let $a, b \in \mathbb{Q}_p^{\text{alg cl}}$ and assume that for every conjugate a_i of a (i.e. for every root of $\lambda_{\mathbb{Q}_p}(a)$) the following holds*

$$|b - a|_p < |a_i - a|_p.$$

Then $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$.

Proof. Let $K = \mathbb{Q}_p(b)$ and suppose that $a \notin K$. So $[K(a) : K] > 1$ and, since a has exactly $[K(a) : K]$ conjugates over K (K is a field of characteristic 0 so irreducible polynomials can't have multiple roots), it follows that there is at least one $a_i \notin K$. Then we have an isomorphism $\sigma \colon K(a) \to K(a_i)$ which keeps K fixed and sends a to a_i. By Corollary 3.18.1 we know that $|\sigma(x)|_p = |x|_p$ for every $x \in K(a)$. In particular

$$\begin{aligned} |b - a_i|_p = |\sigma(b) - \sigma(a_i)|_p = |b - a|_p \\ \implies |a_i - a|_p \leq \max\left\{|a_i - b|_p, |b - a|_p\right\} = |b - a|_p < |a_i - a|_p \end{aligned}$$

which is clearly a contradiction. □

Let's observe that the Krasner's lemma can be easily generalized to any finite extension K of $\mathbb{Q}_p$: we just need to consider the conjugates of a over K and we the result becomes $K(a) \subseteq K(b)$.

From now on, unless otherwise specified, given a normed field $(K, \| \ \|)$ we'll equip the ring $K[X]$ with the sup-norm, i.e. given $f = \sum a_i X^i$ and $g = \sum b_j X^j$ we define

$$\|f - g\| := \max_i \|a_i - b_i\|.$$

Proposition 3.35. *Let K be a finite extension of $\mathbb{Q}_p$ and $f(X) \in K[X]$ have degree n and distinct roots*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Then for every $\varepsilon > 0$ there exists $\delta > 0$ such that if $K[X] \ni g(X) = \sum b_i X^i$ has degree n and $|f - g|_p < \delta$, then for every root α_i of $f(X)$ there is precisely one root β_i of $g(X)$ such that $|\alpha_i - \beta_i|_p < \varepsilon$.

Proof. Let's fix an $\varepsilon > 0$. For every root β of $g(X)$ we have

$$|f(\beta)|_p = |f(\beta) - g(\beta)|_p = \left| \sum_{i=0}^{n} (a_i - b_i)\beta^i \right|_p \leq \max_i \left\{ |a_i - b_i|_p, |\beta|_p^i \right\} \leq$$

$$\leq |f - g|_p \cdot \max \left\{ 1, |\beta|_p^n \right\} < \delta C_1^n$$

where δ will be chosen later and C_1 is a suitable constant which dominates the norm of all the roots of $g(X)$. We can find such a constant which only depends on $f(X)$: in-fact for every i we have

$$|b_i|_p \leq \max \left\{ |b_i - a_i|_p, |a_i|_p \right\} \leq \max \left\{ \delta, |a_i|_p \right\} \leq \max_i |a_i|_p$$

if we choose a small enough δ. Then $\max_i |b_i|_p \leq \max_i |a_i|_p$ and, recalling Lemma 3.32, we conclude that we can set $C_1 = C$, where C is the constant we obtain applying the lemma to $f(X)$. Let's define

$$C_2 := \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|_p.$$

Since by assumption the α_i are distinct, $C_2 > 0$. We immediately see that there can be at most one α_i satisfying $|\beta - \alpha_i|_p < C_2$: in-fact if it held for another $\alpha_j \neq \alpha_i$ we'd have $|\alpha_i - \alpha_j|_p < C_2$ by the ultrametric inequality. Since

$$C_1^n \delta > |f(\beta)|_p = |a_n|_p \prod |\beta - \alpha_i|_p$$

it's clear that if δ is sufficiently small there exists an α_i such that $|\beta - \alpha_i|_p < C_2$. For that α_i we have

$$|\beta - \alpha_i|_p < \frac{C_1^n \delta}{|a_n|_p \prod_{j \neq i} |\beta - \alpha_j|_p} \leq \frac{C_1^n \delta}{|a_n|_p C_2^{n-1}}$$

and it's clear that we can make $|\beta - \alpha_i|_p$ less than ε choosing a sufficiently small δ. □

Finally we prove the already mentioned non-completeness of $\mathbb{Q}_p^{\text{alg cl}}$.

Theorem 3.36. *$\mathbb{Q}_p^{\text{alg cl}}$ is not complete.*

Proof. We must show a Cauchy sequence $(a_i)_{i \in \mathbb{N}} \subseteq \mathbb{Q}_p^{\text{alg cl}}$ which doesn't converge in $\mathbb{Q}_p^{\text{alg cl}}$. Let $b_i \in \mathbb{Q}_p^{\text{alg cl}}$ be a primitive $(p^{i!} - 1)$th root of 1. If $j > i$ then $(p^{i!} - 1) \mid (p^{j!} - 1)$ so $b_i^{p^{j!}-1} = 1$. Thus if $j > i$, b_i is a power of b_j so $\mathbb{Q}_p(b_i) \subset \mathbb{Q}_p(b_j)$. Let

$$a_i := \sum_{j=0}^{i} b_j p^{N_j}$$

where $0 = N_0 < N_1 < N_2 < \dots$ is an increasing sequence of integers we'll choose later. We immediately note that the b_j, for $j = 0, \dots, i$, are the Teichmüller digits of the p-adic expansion of a_i in the unramified extension $\mathbb{Q}_p(b_i)$, since $b_j^{p^{i!}} = b_j$. It's clear that the sequence $(a_i)_i$ is Cauchy:

$$|a_{i+1} - a_i|_p = \left|b_{i+1}p^{N_{i+1}}\right|_p = 1 \cdot \left|p^{N_{i+1}}\right|_p \to 0 \qquad \text{as } i \to +\infty.$$

We choose the integers N_i by induction. We have already set $N_0 = 0$ and suppose that we have defined N_j for $j \leq i$, so that we have $a_i = \sum_{j=0}^{i} b_j p^{N_j}$. Let $K = \mathbb{Q}_p(b_i)$: K is a Galois unramified extension of $\mathbb{Q}_p$ of degree $i!$ and $\mathbb{Q}_p(a_i) = K$. In-fact, if $\mathbb{Q}_p(a_i) \subsetneq K$ there would be a non trivial $\mathbb{Q}_p$-automorphism of K which leaves a_i fixed, let it be σ. By assumption $\sigma(b_i) \neq b_i$ and

$$\sigma(a_i) = \sum_{j=0}^{i} \sigma(b_j)p^{N_j} \qquad (\sigma(b_j)^{p^{i!}} = \sigma(b_j) \quad \forall j = 0, \dots, i).$$

We see that $\sigma(a_i)$ can't be equal to a_i because it has a different p-adic expansion (see Corollary 3.28.1) so it must be $K = \mathbb{Q}_p(a_i)$ and a_i is algebraic over $\mathbb{Q}_p$ of degree $i!$. Thanks to Lemma 3.33 we can find $N_{i+1} > N_i$ such that a_i does not satisfy any congruence

$$\alpha_n a_i^n + \alpha_{n-1}a_i^{n-1} + \dots + \alpha_1 a_i + \alpha_0 \equiv 0 \mod p^{N_{i+1}}$$

for $n < i!$ and $\alpha_j \in \mathbb{Z}_p$ not all divisible by p. We have now completely determined our sequence $(a_i)_i$. Now, suppose that $a \in \mathbb{Q}_p^{\text{alg cl}}$ is the limit of $(a_i)_i$. By definition, a is algebraic over $\mathbb{Q}_p$ so it satisfies a polynomial equation in $\mathbb{Q}_p$

$$\beta_n a^n + \beta_{n-1}a^{n-1} + \dots + \beta_1 a + \beta_0 = 0$$

and, multiplying by a suitable power of p, we can assume that $\beta_i \in \mathbb{Z}_p$ and that there is at least a coefficient in $\mathbb{Z}_p^\times$. Let's choose i such that $i! > n$. We have

$$|a_j - a_i|_p \leq \left|p^{N_{i+1}}\right|_p \quad \forall j > i \implies |a - a_i|_p = \lim_{j \to +\infty} |a_j - a_i|_p \leq \left|p^{N_{i+1}}\right|_p$$

so $a \equiv a_i \mod p^{N_{i+1}}$. This implies

$$\beta_n a_i^n + \beta_{n-1}a_i^{n-1} + \dots + \beta_1 a_i + \beta_0 \equiv 0 \mod p^{N_{i+1}}$$

which is a contradiction. Then $(a_i)_i$ cannot have limit in $\mathbb{Q}_p^{\text{alg cl}}$ and this proves the theorem. □

We can then complete $\mathbb{Q}_p^{\text{alg cl}}$ exactly in the same way we completed $(\mathbb{Q}, |\ |_p)$ in Section 1.3 (this is the standard way to complete a metric space).

Definition 3.37. The completion of $\mathbb{Q}_p^{\text{alg cl}}$ is called $\mathbb{C}_p$.

We can extend the p-adic absolute value to this new field $\mathbb{C}_p$ just as we extended it from $\mathbb{Q}$ to $\mathbb{Q}_p$: given $x \in \mathbb{C}_p$, we choose a representative Cauchy sequence $(x_i)_i$ in $\mathbb{Q}_p^{\text{alg cl}}$ (recall that $\mathbb{C}_p$ is the set of equivalence classes of Cauchy sequences), and we define

$$|x|_p := \lim_{i \to +\infty} |x_i|_p.$$

It can be proved that $|x|_p$ is well defined and that the limit exists: if $x \neq 0$ then from a sufficiently large i all norms $|x_i|_p$ are equal. We can also extend ord_p to $\mathbb{C}_p$:

$$\operatorname{ord}_p x := -\log_p |x|_p.$$

Let $A = \{x \in \mathbb{C}_p \mid |x|_p \leq 1\}$ be the valuation ring of $\mathbb{C}_p$ and $M = \{x \in \mathbb{C}_p \mid |x|_p < 1\}$ its maximal ideal.

Definition 3.38. Let $r = a/b \in \mathbb{Q}$ with $a \in \mathbb{Z}, b \in \mathbb{N}^\times$ and $P(X) = X^b - p^a \in \mathbb{Q}_p[X]$. Any root of $P(X)$ in $\mathbb{Q}_p^{\text{alg cl}}$ is called a *fractional power* of p to r and can be denoted by p^r.

Using fractional powers we can immediately prove an interesting result.

Proposition 3.39. *For any $q \in \mathbb{Q}$ there exists $x \in \mathbb{Q}_p^{\text{alg cl}}$ with $\operatorname{ord}_p x = q$.*

Proof. Let's write $q = a/b$ with $a \in \mathbb{Z}, b \in \mathbb{N}^\times$ and let $\mathbb{Q}_p^{\text{alg cl}} \ni x = p^q$ be any fractional power. We claim that $\operatorname{ord}_p x = q$, i.e. $|x|_p = p^{-q}$. In-fact, by definition of fractional power, we have $x^b = p^a$, which implies $|x|_p = p^{-a/b}$. □

With the next proposition we'll dig deeper into the structure of $\mathbb{C}_p$, to understand how its elements can be represented (working with equivalence classes of Cauchy sequences is not very practical).

Proposition 3.40. *Any non-zero element of $\mathbb{C}_p$ is a product of a fractional power of p, a root of unity and an element in the open unit disc about 1 (in $\mathbb{C}_p$).*

Proof. Let's first consider the case of $x \in A^\times$, i.e. $|x|_p = 1$. Since $\mathbb{Q}_p^{\text{alg cl}}$ is dense in $\mathbb{C}_p$ we can find an algebraic x' such that $|x - x'|_p < 1$, i.e. $x - x' \in M$. By the isosceles triangle principle we obtain $|x'|_p = 1$ so it follows that x' is integral over $\mathbb{Z}_p$ (see Proposition 3.21), i.e. it satisfies a monic polynomial in $\mathbb{Z}_p[X]$. Reducing this polynomial mod p we find that $x + M = x' + M$ is algebraic over $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ so it lies in some $\mathbb{F}_{p^f}$. We can consider $\omega(x)$, the Teichmüller representative of $x + M \in \mathbb{F}_{p^f}$, which is a $(p^f - 1)$th root of 1 (i.e. it is an element of $K_f^{\text{unram}} \subset \mathbb{Q}_p^{\text{alg cl}}$ which is a solution of $X^{p^f} - X = 0$ and is congruent to $x + M$ mod p, see proof of Proposition 3.28). If we set $\langle x \rangle := x/\omega(x)$, then $\langle x \rangle \in 1 + M$. We have proved that any element of $A^\times$ is the product of a root of unity $\omega(x)$ and an element $\langle x \rangle$ which is in the open unit disc about 1.

Finally, any $x \in \mathbb{C}_p$ can be written as a product of a fractional power of p and an element of absolute value 1. Namely, if $\operatorname{ord}_p x = r = a/b$ (observe that $\operatorname{ord}_p(\mathbb{C}_p^\times) \subset \mathbb{Q}$) and $p^r \in \mathbb{Q}_p^{\text{alg cl}}$ is any root of $X^b - p^a$, then $|p^r|_p = |p|_p^{a/b}$ (p^r is a root of $p^{-a}X^b - 1 = 0$) so

$$|x/p^r|_p = |x|_p \cdot \frac{1}{|p^r|_p} = |p|_p^{a/b} \cdot |p|_p^{-a/b} = 1$$

and, called $x_1 := x/p^r \in A^\times$, we know that x_1 is a product of a root of 1 and an element in $1 + M = B_{<1}(1, \mathbb{C}_p)$. □

Obviously, by construction, $\mathbb{C}_p$ is a complete field which contains $\mathbb{Q}_p^{\text{alg cl}}$. It is then an immediate question if $\mathbb{C}_p$ is still algebraically closed and we'll see in the next theorem that it is.

Theorem 3.41. *$\mathbb{C}_p$ is algebraically closed.*

Proof. Let's consider a generic monic polynomial in $\mathbb{C}_p[X]$:

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

We just need to show that f admits a root in $\mathbb{C}_p$. For each $i = 0, 1, \ldots, n-1$, let $(a_{i,j})_{j \in \mathbb{N}}$ be a sequence of elements in $\mathbb{Q}_p^{\text{alg cl}}$ which converges to a_i. Let's consider the sequence $(g_j(X))_{j \in \mathbb{N}} \subset \mathbb{Q}_p^{\text{alg cl}}[X]$ defined by

$$g_j(X) := X^n + a_{n-1,j}X^{n-1} + \cdots + a_{1,j}X + a_{0,j}.$$

Let $\{r_{i,j}\}_{i=1}^n \subset \mathbb{Q}_p^{\text{alg cl}}$ be the roots of $g_j(X)$. We claim that we can find a sequence $(i_j)_{j \in \mathbb{N}} \subset \mathbb{N}$ such that the sequence $(r_{i_j,j})_j$ is Cauchy.

Let's proceed by induction and suppose we have $r_{i_h,h}$ and we want to find $r_{i_{h+1},h+1}$. Let $\delta_h := |g_h - g_{h+1}|_p = \max_i |a_{i,h} - a_{i,h+1}|_p$, which clearly approaches 0 as $j \to +\infty$, and let $A_h := \max\{1, |r_{i_h,h}|_p^n\}$. Now, thanks to Lemma 3.32, we can find C_j, a constant depending only on $\max_i |a_{i,j}|_p$, which dominates the norm of each root of $g_j(X)$ and such that $A_j \leq C_j$. Since $(a_{i,j})_j$ is a convergent sequence in $\mathbb{Q}_p^{\text{alg cl}}$, it is bounded in norm for every $i = 0, \dots, n-1$ so we can find a uniform constant C such that $C_j \leq C$ for every $j \in \mathbb{N}$. Then we have

$$\prod_{i=1}^{n} |r_{i_h,h} - r_{i,h+1}|_p = |g_{h+1}(r_{i_h,h})|_p = |g_{h+1}(r_{i_h,h}) - g_h(r_{i_h,h})|_p \leq \delta_h C$$

hence there is at least one i such that $|r_{i_h,h} - r_{i,h+1}|_p \leq \sqrt[n]{\delta_h C}$. Let i_{h+1} be such i. Since $\delta_j \to 0$ as $j \to +\infty$, it is clear that $(r_{i_j,j})_j$ is Cauchy in $\mathbb{Q}_p^{\text{alg cl}}$. Since $\mathbb{C}_p$ is complete, this sequence converges and if we define

$$r := \lim_{j \to +\infty} r_{i_j,j} \in \mathbb{C}_p$$

we then have

$$f(r) = f\left(\lim_{j \to +\infty} r_{i_j,j}\right) = \lim_{j \to +\infty} f(r_{i_j,j}) = \lim_{j \to +\infty} \lim_{m \to +\infty} g_m(r_{i_j,j})$$

where we used that f is continuous and that $g_j \xrightarrow{\| \ \|_\infty} f$ (which implies punctual convergence). More precisely, since this double limit exists, we can consider the section $m = j$ to obtain

$$\lim_{j \to +\infty} \lim_{m \to +\infty} g_m(r_{i_j,j}) = \lim_{j \to +\infty} g_j(r_{i_j,j}) = 0$$

so we can conclude $f(r) = 0$ and $r \in \mathbb{C}_p$ is a root of f. □

Finally, after all this effort, we have built $\mathbb{C}_p$: the smallest field which contains $\mathbb{Q}$ and is both algebraically closed and complete with respect to $| \ |_p$ (we recall that completion and algebraic closure are unique processes up to isomorphism). Let's observe some basic properties of this field:

1. $|\mathbb{C}_p|_p = \left|\mathbb{Q}_p^{\text{alg cl}}\right|_p = p^{\mathbb{Q}} \cup \{0\}$;
2. $\text{card}(\mathbb{C}_p) = \text{card}(\mathbb{R})$;
3. $\mathbb{C}_p$ is a field isomorphic to $\mathbb{C}$, although not in a canonical way.

While property 1. is evident, the other properties aren't so obvious and we'll have faith in them, i.e. we won't prove them.

Actually, we could have built $\mathbb{C}_p$ in an apparently shorter way:

$$\begin{tikzcd}
 & & \mathbb{C} \\
\mathbb{Q} \arrow[r, "\text{alg cl}"] & \mathbb{Q}^{\text{alg cl}} \arrow[ur, "| \ |_\infty"] \arrow[dr, "| \ |_p"'] & \\
 & & \mathbb{C}_p
\end{tikzcd}$$

namely by first embedding $\mathbb{Q}$ in $\mathbb{Q}^{\text{alg cl}}$, its algebraic closure (clearly it does not depend on the chosen norm), and then completing $\mathbb{Q}^{\text{alg cl}}$ with respect to the euclidean norm (we obtain $\mathbb{C}$) and to the p-adic norm (we obtain $\mathbb{C}_p$). We could have chosen to follow this way, which highlights the similarity between $\mathbb{C}$ and $\mathbb{C}_p$, without even needing the intermediate field $\mathbb{Q}_p$. The problem is that the algebraic closure of $\mathbb{Q}$ is a very complicate field. Instead, the road we decided to follow is this longer one:

$$\begin{tikzcd}
 & \mathbb{R} \arrow[r, "\text{alg cl}"] & \mathbb{C} & \\
\mathbb{Q} \arrow[ur, "|\ |_\infty"] \arrow[dr, "|\ |_p"'] & & & \\
 & \mathbb{Q}_p \arrow[r, "\text{alg cl}"] & \mathbb{Q}_p^{\text{alg cl}} \arrow[r, "|\ |_p"] & \mathbb{C}_p
\end{tikzcd}$$

Here we can see that the "euclidean case" seems simpler and that's because $\mathbb{C}$, the algebraic closure of $\mathbb{R}$, has a finite degree over $\mathbb{R}$ (namely $[\mathbb{C} : \mathbb{R}] = 2$) so it's still complete, while $[\mathbb{Q}_p^{\text{alg cl}} : \mathbb{Q}_p] = +\infty$ and completeness is lost: we have to complete again and we obtain $\mathbb{C}_p$. The following general theorem holds.

Theorem 3.42. *Let $(K, \|\ \|)$ be an algebraically closed non-Archimedean normed field. Then the completion of K is algebraically closed.*

Proof. See [3, p. 2]. □

4 p-adic power series

4.1 Elementary functions

In many of the following reasonings we'll use the next proposition, which will give us the possibility to manipulate formal power series, knowing their behaviour in some neighbourhood of 0.

Proposition 4.1. *Let $f(X_1, \dots, X_n) \in \mathbb{C}[\![X_1, \dots, X_n]\!]$ be a power series and let $\varepsilon > 0$ such that f is absolutely convergent on $[-\varepsilon, \varepsilon]^n$ and $f(x_1, \dots, x_n) = 0$ for every $x_i \in [-\varepsilon, \varepsilon]$. Then $f \equiv 0$, i.e. all terms of f vanishes.*

Proof. We prove the proposition by induction on n.

- $n = 1$: let
$$f(X) = \sum_{i=0}^{+\infty} a_i X^i.$$
Obviously $f(0) = a_0 = 0$ so we can write $f(X) = X \cdot (a_1 + a_2 X + \dots) =: X \cdot f_1(X)$. Now $f_1(X) \in \mathbb{C}[\![X]\!]$ vanishes for every $x \in [-\varepsilon, \varepsilon] \setminus \{0\}$. It is well known from complex analysis that a formal power series in $\mathbb{C}$ defines a holomorphic function where it converges (so, in particular, it's continuous). We then obtain that f_1 is continuous so $f_1(0) = 0$, i.e. $a_1 = 0$. Then we can write $f(X) = X^2 \cdot (a_2 + a_3 X + \dots) =: X^2 \cdot f_2(X)$, where $f_2(x) = 0$ for every $x \in [-\varepsilon, \varepsilon] \setminus \{0\}$. Iterating this process we obtain $a_n = 0$ for each $n \in \mathbb{N}$ so $f \equiv 0$.

- $n > 1$: let's assume that the thesis holds for every $i < n$ and let's prove it for n. For brevity, let $Y = (X_1, \dots, X_{n-1})$. Since f is absolutely convergent we can write
$$f(Y, X_n) = \sum_{i=0}^{+\infty} g_i(Y) X_n^i, \qquad g_i(Y) \in \mathbb{C}[\![Y]\!].$$
For $x_n = 0$ we have $f(y, 0) = g_0(y) = 0$ for $y \in [-\varepsilon, \varepsilon]^{n-1}$. Then, by induction, $g_0 \equiv 0$ so
$$f(Y, X_n) = X_n \cdot (g_1(Y) + g_2(Y) X_n + \dots) =: X_n \cdot f_1(Y, X_n)$$
and by hypothesis $f_1(y, x_n) = 0$ for every $y \in [-\varepsilon, \varepsilon]^{n-1}, x_n \in [-\varepsilon, \varepsilon] \setminus \{0\}$. Clearly, fixed $y \in [-\varepsilon, \varepsilon]^{n-1}$, the function $X \mapsto f_1(y, X)$ is a continuous function so $f_1(y, 0) = \lim_{x \to 0} f_1(y, x) = 0$. We have obtained $0 \equiv f_1(Y, 0) = g_1(Y)$ so, by inductive hypothesis, $g_1(Y) \equiv 0$ and we can write
$$f(Y, X_n) = X_n^2 \cdot (g_2(Y) + g_3(Y) X_n + \dots) =: X_n^2 \cdot f_2(Y, X_n)$$
where $f_2(y, x_n) = 0$ if $y \in [-\varepsilon, \varepsilon]^{n-1}, x_n \in [-\varepsilon, \varepsilon] \setminus \{0\}$. Iterating this process we obtain $g_n(Y) \equiv 0$ for every $n \in \mathbb{N}$, i.e. $f \equiv 0$.

□

Another important lemma about p-adic power series is the Dwork's lemma. It expresses an important phenomenon in p-adic analysis: if we know $F(X^p)/(F(X)^p)$ then we also know something about F. This ratio represents how far off F is from commuting with the p-power map, which is a very important map also in different contexts (e.g. Frobenius morphism for characteristic p fields).

Lemma 4.2 (Dwork's lemma). *Let $F(X) \in 1 + X\mathbb{Q}_p[\![X]\!]$. Then $F(X) \in 1 + X\mathbb{Z}_p[\![X]\!]$ if and only if $\frac{F(X^p)}{F(X)^p} \in 1 + pX\mathbb{Z}_p[\![X]\!]$.*

Proof. If $F(X) \in 1+X\mathbb{Z}_p[\![X]\!]$ then, since $(a+b)^p \equiv a^p + b^p \mod p$ and $a^p \equiv a \mod p$ if $a \in \mathbb{Z}_p$, we have

$$F(X)^p = F(X^p) + pG(X) \qquad \exists G(X) \in X\mathbb{Z}_p[\![X]\!].$$

Then

$$\frac{F(X^p)}{F(X)^p} = 1 - p \cdot \frac{G(X)}{F(X)^p} \in 1 + pX\mathbb{Z}_p[\![X]\!],$$

because $F(X)^p \in 1 + X\mathbb{Z}_p[\![X]\!]$ so it can be inverted.
For the other implication let $F(X) = \sum a_i X^i$; by hypothesis we know that $\exists G(X) = \sum b_i X^i$ such that $G(X) \in 1 + pX\mathbb{Z}_p[\![X]\!]$ and

$$F(X^p) = F(X)^p \cdot G(X)$$

We'll prove by induction that $a_i \in \mathbb{Z}_p$. By assumption $F(X) \in 1 + X\mathbb{Q}_p[\![X]\!]$ so $a_0 = 1$. Let's now suppose that $a_i \in \mathbb{Z}_p$ for every $i < n$. Looking at the coefficients of X^n on both sides of the above equation we obtain

$$\text{coefficient of } X^n \text{ in } \left(\sum_{i=0}^{n} a_i X^i\right)^p \cdot \left(1 + \sum_{i=1}^{n} b_i X^i\right) = \begin{cases} a_{n/p}, & \text{if } p \text{ divides } n; \\ 0, & \text{otherwise;} \end{cases}.$$

Expanding the expression for the coefficient of X^n on the left and subtracting $a_{n/p}$ (recall that $a_{n/p}^p \equiv a_{n/p} \mod p$) we notice that the resulting expression consists of pa_n added to some terms in $p\mathbb{Z}_p$ so we can conclude that $pa_n \in p\mathbb{Z}_p$, i.e. $a_n \in \mathbb{Z}_p$. (To see why this is true it can be convenient to recall the formula $(x_1 + \cdots + x_n)^m = \sum_{i_1+\cdots+i_n=m} \binom{m}{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$). □

We'll also prove here a technical lemma, which we will use to study the p-adic logarithm.

Lemma 4.3. *Let a be a primitive m-th root of 1 in $\mathbb{Q}_p^{\text{alg cl}}$. Then*

(i) if $m = p^n$ for some $n \in \mathbb{N}$ then $|a-1|_p = p^{-1/\varphi(p^n)}$;

(ii) otherwise, $|a-1|_p = 1$.

Proof. Let $\Phi_n(X) \in \mathbb{Z}_p[X]$ be the n-th cyclotomic polynomial.
(i) To prove this case we'll do an induction on n. The case $n = 0$ is trivial, since $a = 1$. If $n = 1$ then a is a primitive p-th root of 1, i.e. $a^p = 1, a \neq 1$, so $\Phi_p(a) = 0$. By Eisenstein criterion (Proposition 3.25) it is easy to prove that $\Phi_p(X)$ is irreducible over $\mathbb{Q}_p$. We consider then

$$f(X) := \Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots + \binom{p}{2} X + p.$$

Clearly $f(X) \in \mathbb{Q}_p[X]$ is irreducible and $f(a-1) = 0$ so, recalling how we extended $|\ |_p$ to $\mathbb{Q}_p^{\text{alg cl}}$, we have

$$|a-1|_p = |p|_p^{1/(p-1)} = p^{-1/(p-1)}$$

which concludes the proof of the case $n = 1$. Now, suppose we know the thesis holds for $m = p^i, i < n$ and let's prove it also holds for $m = p^n$. If we consider the extension $K = \mathbb{Q}_p(a)$

with the usual notation (A is the maximal subring and M is its maximal ideal), it is easy to note that $|a|_p = 1$ and

$$a^{p^n} = 1 \implies a^{p^n} \equiv 1 \mod M$$

and since A/M is a finite field of characteristic p we obtain

$$a \equiv 1 \mod M$$

which means exactly $a = 1 + b$ for some $b \in K, |b|_p < 1$. We recall the easy facts

$$\deg \Phi_{p^n}(X) = \varphi(p^n) = p^n - p^{n-1}, \qquad \Phi_{p^n}(X) = \Phi_p\left(X^{p^{n-1}}\right)$$

which imply $\Phi_{p^n}(1) = \Phi_p(1) = p$. Since a is a primitive p^n-th root of 1, every other primitive p^n-th root of 1 is a^j, with $p \nmid j$, so

$$\Phi_{p^n}(X) = \prod_{1 \le j < p^n, p \nmid j} (X - a^j).$$

Evaluating at $X = 1$ we obtain

$$|p|_p = \prod_{1 \le j < p^n, p \nmid j} \left|1 - a^j\right|_p.$$

Using the fact $a \equiv 1 \mod M$ we can see that

$$\frac{1 - a^j}{1 - a} = 1 + a + \cdots + a^{j-1} \equiv j \mod M$$

and if $p \nmid j$ we obtain

$$\left|\frac{1 - a^j}{1 - a}\right|_p = 1$$

so $\left|1 - a^j\right|_p = |1 - a|_p$, which implies $|1 - a|_p = |p|_p^{1/\varphi(p^n)}$.
(ii) First of all let's consider the basic case $p \nmid m$. Then, $a - 1$ is a root of the polynomial

$$f(X) = \Phi_m(X + 1) = X^{m-1} + \cdots + m = g_1(X) \cdots g_r(X)$$

where $g_i(X) \in \mathbb{Q}_p[X]$ is an irreducible factor of f, and we can assume that every $g_i(X)$ is monic and has coefficients in $\mathbb{Z}_p$. By hypothesis $|m|_p = 1$ and if b_i is the constant term of $g_i(X)$ we have

$$|b_1 b_2 \cdots b_r|_p = |m|_p = 1, b_i \in \mathbb{Z}_p \implies |b_i|_p = 1 \quad \forall\, i = 1, \ldots, r.$$

Since $f(a - 1) = 0$ there is at least one $g_i(X)$ such that $g_i(a - 1) = 0$ so $\lambda_{\mathbb{Q}_p}(a - 1) = g_i(X)$. Then

$$|a - 1|_p^{\deg g_i(X)} = |b_i|_p = 1 \implies |a - 1|_p = 1.$$

Now let $m = p^n q$ with $p \nmid q$ (clearly $q \in \mathbb{N}_{>1}$) and suppose the thesis holds for every $m \in \mathbb{N}$ such that m is not a power of p and $p^n \nmid m$. Then, if a is a primitive m-th root of 1, a^p is a primitive $(p^{n-1}q)$-th root of 1 and, by inductive hypothesis, we know

$$|a - 1|_p \cdot \left|a^{p-1} + a^{p-2} + \cdots + a + 1\right|_p = |a^p - 1|_p = 1.$$

Since $|a|_p = 1$ we have

$$|a - 1|_p \le 1, \qquad \left|a^{p-1} + \cdots + 1\right|_p \le 1$$
$$\implies |a - 1|_p = 1$$

which proves the statement. □

We recall that in an ultrametric space, like $(\mathbb{C}_p, |\ |_p)$, a sequence is Cauchy if and only if the difference between adjacent terms tends to 0, and if the space is also complete, an infinite series converges if and only if its general term tends to 0 (see Lemma 3.5 and Proposition 3.7). Now we are ready to define analytic functions on $\mathbb{C}_p$ and prove some of their basic properties.

Definition 4.4. A function f is an *analytic function* if

$$f(X) = \sum_{n=0}^{+\infty} a_n X^n, \qquad a_n \in \mathbb{C}_p.$$

We can define $f(x)$ for every $x \in \mathbb{C}_p$ such that the series converges, i.e. $|a_n x^n|_p \to 0$ as $n \to +\infty$.

Like in complex analysis, given an analytic function f, we can define its *radius of convergence.* Surprisingly we have the exact same formula as in classic analysis.

Proposition 4.5. *Let $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ be an analytic function. We can define its radius of convergence as*

$$r := \frac{1}{\limsup |a_n|_p^{1/n}},$$

with the usual meaning: f converges if $|x|_p < r$ and diverges if $|x|_p > r$.

Proof. We recall the definition of lim sup: $1/r$ is the least real number such that for any $C > 1/r$ there are only finitely many $|a_n|_p^{1/n} > C$.
Let's first consider the case $|x|_p < r$: we can write $|x|_p = (1-\varepsilon)r$ for some $\varepsilon > 0$. We have

$$|a_n x^n|_p = \left(r|a_n|_p^{1/n}\right)^n \cdot (1-\varepsilon)^n$$

and, if n is big enough, by definition of r we have

$$|a_n|_p^{1/n} \leq \frac{1}{r - \frac{1}{2}\varepsilon r}.$$

Then

$$\lim_{n\to+\infty} |a_n x^n|_p \leq \lim_{n\to+\infty} \left(\frac{(1-\varepsilon)r}{(1-\frac{1}{2}\varepsilon)r}\right)^n = \lim_{n\to+\infty} \left(\frac{1-\varepsilon}{1-\frac{1}{2}\varepsilon}\right)^n = 0,$$

which gives us the desired convergence.
Let's now prove that if $|x|_p > r$ (and $r < +\infty$) the series diverges. Let's choose an element $|x|_p > r$ and an $\varepsilon > 0$ such that $|x|_p \geq (1+\varepsilon)r$. By definition of lim sup we can find a subsequence $(a_{n_k})_k$ such that $|a_{n_k}|_p^{1/n_k} \geq 1/(r + \frac{1}{2}\varepsilon r)$. Then

$$\lim_{k\to+\infty} |a_{n_k} x^{n_k}|_p \geq \lim_{k\to+\infty} \left(\frac{1+\varepsilon}{1+\frac{1}{2}\varepsilon}\right)^{n_k} = +\infty,$$

which implies that f cannot converge.
Finally, if $r = +\infty$, i.e. $\lim_{n\to+\infty} |a_n|_p^{1/n} = 0$, chosen an element $x \in \mathbb{C}_p^\times$ ($x = 0$ is trivial) we have that, if n is big enough, $|a_n|_p \leq 1/(2^n |x|_p^n)$ so

$$\lim_{n\to+\infty} |a_n x^n|_p \leq \lim_{n\to+\infty} 2^{-n} = 0$$

and f converges everywhere. □

This proposition tells us nothing about the case $|x|_p = r$. In classical analysis there isn't a simple answer: for example the well known function

$$\log(1+X) = \sum_{n=1}^{+\infty}(-1)^{n+1}\frac{X^n}{n}$$

has radius of convergence $r = 1$ on $\mathbb{C}$. When $|x| = 1$ this series can diverge (for example if $x = -1$ we obtain the divergent series $-\sum 1/n$) or converge (if $x = 1$ we obtain $\sum(-1)^{n+1}/n$, which converges by Leibniz criterion). This happens because, over $\mathbb{R}$, there are conditionally convergent series that aren't absolutely convergent. In p-adic analysis this cannot happen because convergence only depends on $|x|_p$: a given analytic function behaves exactly in the same way for every $|x|_p = r$. We will study more deeply this formal series in $\mathbb{C}_p$ when we'll talk about p-adic logarithm.
Let's prove two basic facts about analytic functions. For brevity we'll adopt the notation $D_a(r) := B_{\leq r}(a)$ and $D_a(r^-) := B_{<r}(a)$, where we consider the balls in $\mathbb{C}_p$. We'll also omit the subscript a if $a = 0$, for example $D(r) = D_0(r) = B_{\leq r}(0)$.

Proposition 4.6. *Every $f(X) \in \mathbb{Z}_p[\![X]\!]$ converges in $D(1^-)$.*

Proof. Let $f(X) = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{Z}_p[\![X]\!]$ and let $x \in D(1^-)$. Then

$$\begin{aligned} &|x|_p < 1, |a_n|_p \leq 1 \,\forall\, n \in \mathbb{N} \\ \implies &\lim_{n\to+\infty}|a_n x^n|_p \leq \lim_{n\to+\infty}|x|_p^n = 0. \end{aligned}$$

□

Proposition 4.7. *Every $f(X) = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{C}_p[\![X]\!]$ which converges in a disc $D = D(r)$, or $D(r^-)$, is continuous on D.*

Proof. Let's first prove continuity in 0. Let $x \in D$ such that $|x|_p < \delta < r$ ($\delta > 0$ will be chosen later); then, by continuity of absolute value, we have

$$|f(x) - f(0)|_p = \left|\sum_{n=1}^{+\infty} a_n x^n\right|_p \leq \max_{n\in\mathbb{N}^\times} |a_n x^n|_p \leq \max_{n\in\mathbb{N}^\times}\left(|a_n|_p \cdot \delta^n\right).$$

Clearly, since f converges on D, we must have $1/r' > \limsup|a_n|_p^{1/n}$ where $\delta < r' < r$ so, for a large enough N, $|a_n|_p < r'^{-n}$ if $n > N$. Let's introduce

$$C(\delta) := \max_{1\leq n\leq N}\left(|a_n|_p \cdot \delta^n\right);$$

it's obvious that $C(\delta) \to 0^+$ as $\delta \to 0^+$. Instead, if $n > N$, we have

$$|a_n|_p \cdot \delta^n \leq \left(\frac{\delta}{r'}\right)^n \leq \left(\frac{\delta}{r'}\right)^N,$$

since $\delta/r' < 1$. Then

$$|f(x) - f(0)|_p \leq \max\left\{C(\delta), \left(\frac{\delta}{r'}\right)^N\right\}$$

and we can make the right member as small as we want by choosing smaller δ. This proves continuity in 0.
Let's now prove continuity in $0 \neq x \in D$ and consider $y \in D$ such that $|x-y|_p < \delta$, where

$\delta < |x|_p$ will be chosen later, as before. Then, by the isosceles triangle principle, $|x|_p = |y|_p$. We have

$$|f(x) - f(y)|_p = \left| \sum_{n=1}^{+\infty} (a_n x^n - a_n y^n) \right|_p \leq \max_{n \in \mathbb{N}^\times} \left(|a_n|_p \cdot |x^n - y^n|_p \right) \leq$$
$$\leq \max_{n \in \mathbb{N}^\times} \left(|a_n|_p \cdot \left| (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \right|_p \right)$$

but $\left| x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} \right|_p \leq \max_{1 \leq i \leq n} \left| x^{n-i} y^{i-1} \right|_p = |x|_p^{n-1}$ hence

$$|f(x) - f(y)|_p \leq \max_{n \in \mathbb{N}^\times} \left(|x - y|_p \cdot |a_n|_p |x|_p^{n-1} \right) < \frac{\delta}{|x|_p} \cdot \max_{n \in \mathbb{N}^\times} \left(|a_n|_p \cdot |x|_p^n \right).$$

We know that $\lim_{n \to +\infty} |a_n|_p |x|_p^n = 0$ so as $\delta \to 0^+$ we have $|f(x) - f(y)|_p \to 0$, which proves the statement. □

Definition 4.8. The (partial) function $\log_p(1 + X) \colon \mathbb{C}_p \to \mathbb{C}_p$ defined by

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

is the *p-adic logarithm.*

Proposition 4.9. *The function* $\log_p(1 + X)$ *converges on* $D(1^-)$ *and diverges elsewhere.*

Proof. It's immediate to verify that the series converges if $|x|_p < 1$ and diverges if $|x|_p \geq 1$. In-fact $|a_n|_p = p^{\operatorname{ord}_p n}$ so $\lim_{n \to +\infty} |a_n|_p^{1/n} = \lim_{n \to +\infty} p^{(\operatorname{ord}_p n)/n} = 1$ and we obtain the desired radius of convergence. Lastly, if $|x|_p = 1$, we have $|a_n x^n|_p = p^{\operatorname{ord}_p n} \geq 1$ so the series diverges. □

From now on, unless otherwise specified, we'll use $\log_p$ meaning the p-adic logarithm we have just defined. Let's now prove the basic property of logarithms, which also holds in p-adic environment.

Proposition 4.10. *The logarithm of a product is the sum of the logarithms. More precisely, if* $x, y \in D(1^-)$ *then* $\log_p [(1 + x)(1 + y)] = \log_p(1 + x) + \log_p(1 + y)$.

Proof. First of all let's observe that $x, y \in D(1^-) \implies x + y + xy \in D(1^-)$, so we can compute the logarithms. By definition

$$\log_p [(1 + x)(1 + y)] = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(x + y + xy)^n}{n}.$$

If we work in $\mathbb{R}$ with the usual metric we already know that $\log [(1 + x)(1 + y)] = \log(1 + x) + \log(1 + y)$ and, using the Taylor expansion of log, we have

$$\sum_{n=1}^{+\infty} (-1)^{n+1} \frac{x^n}{n} + \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{y^n}{n} = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(x + y + xy)^n}{n}$$

for every $x, y \in \left[-\frac{1}{2}, \frac{1}{2} \right]$. Thanks to Proposition 4.1 we infer that this relation also holds in the ring of formal power series in two variables $\mathbb{Q}[\![X, Y]\!]$. Then, using the fact that if a series converges in $\mathbb{C}_p$ its terms can be rearranged in any order without changing the sum, we can write

$$\log_p [(1 + x)(1 + y)] = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(x + y + xy)^n}{n} =$$
$$= \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{x^n}{n} + \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{y^n}{n} = \log_p(1 + x) + \log_p(1 + y)$$

which concludes the proof. □

Corollary 4.10.1. *If $1+x \in \mathbb{C}_p$ is a root of 1 and $|x|_p < 1$, then $\log_p(1+x) = 0$. In particular if $1+x$ is a p^m-th root of 1 then $\log_p(1+x) = 0$.*

Proof. Let's first observe that we can actually compute the logarithm of $1+x$ since by hypothesis $|x|_p < 1$ (if $1+x$ is a p^m-th root of 1 then automatically $|x|_p < 1$ by Lemma 4.3). Now we have

$$k \cdot \log_p(1+x) = \log_p\left[(1+x)^k\right] = \log_p(1) = 0,$$

which concludes the proof. □

We have obtained a function, defined on a particular disc of $\mathbb{C}_p$, using the Taylor expansion of the classical $\log(1+X)$. Now we would like to define the exponential function, beginning from the classical $\exp(x) = \sum_{n=0}^{+\infty} x^n/n!$, and study its relation with the logarithm.

Definition 4.11. The (partial) function $\exp_p(X)\colon \mathbb{C}_p \to \mathbb{C}_p$ defined by

$$\exp_p(x) := \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

is the *p-adic exponential.*

Looking at this series we immediately see that, unlike in the classical case where the $n!$ in the denominator makes sure the series converges for every $x \in \mathbb{C}$, there can be some problems. In-fact if $n!$ is divisible by a high power of p, its reciprocal will have a big absolute value. More precisely, we can compute exactly $|1/n!|_p = p^{\mathrm{ord}_p(n!)}$.

Lemma 4.12. *Given $n \in \mathbb{N}$,*

$$\mathrm{ord}_p(n!) = \frac{n - S_n}{p-1}$$

where S_n is the sum of digits in n to base p.

Proof. Let's write n in base p:

$$n = a_0 + a_1 p + \cdots + a_r p^r, \qquad a_i \in \{0, \ldots, p-1\},\ a_r \neq 0.$$

Then $S_n = a_0 + a_1 + \cdots + a_n$. By definition, $\mathrm{ord}_p(n!)$ is the maximum t such that $p^t \mid (n!)$. We can use this little formula to compute it:

$$\mathrm{ord}_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right] = \sum_{k=1}^{r} \left[\frac{n}{p^k}\right]$$

where $[x]$ is the integer part of $x \in \mathbb{R}$, i.e. the only integer such that $[x] \leq x < [x]+1$. Using the representation of n in base p we have that $\left[n/p^k\right] = 0$ if $k > r$ and, otherwise,

$$\left[\frac{n}{p^k}\right] = \frac{n - a_0 - \cdots - a_{k-1}p^{k-1}}{p^k}$$

so if we add them together we obtain

$$\sum_{k=1}^{r} \left[\frac{n}{p^k}\right] = \sum_{k=1}^{r} \frac{n - \sum_{j=0}^{k-1} a_j p^j}{p^k}.$$

With a little bit of computation, recalling that $1 + p + \cdots + p^{k-1} = \frac{p^k-1}{p-1}$, we obtain the desired formula. □

Proposition 4.13. *The function* $\exp_p(X)$ *converges on* $D(r_p^-)$ *and diverges elsewhere, where* $r_p := p^{-1/(p-1)}$.

Proof. Using Lemma 4.12 we obtain

$$|1/n!|_p = p^{\frac{n-S_n}{p-1}}$$

and, recalling the formula for the radius of convergence $r = 1/(\limsup |a_n|_p^{1/n})$, we can write

$$\operatorname{ord}_p r = -\operatorname{ord}_p \left(\limsup p^{-(\operatorname{ord}_p a_n)/n}\right) = -\operatorname{ord}_p \left(p^{-\liminf(\operatorname{ord}_p a_n)/n}\right) = \liminf \left(\frac{\operatorname{ord}_p a_n}{n}\right)$$

so, in our case where $a_n = 1/n!$, we obtain

$$\operatorname{ord}_p r = \liminf \left(-\frac{n - S_n}{n(p-1)}\right).$$

We can use the easy upper bound $S_n \leq (p-1) \cdot \operatorname{ord}_p n$ to prove

$$\lim_{n\to+\infty} \frac{S_n - n}{n(p-1)} = -\frac{1}{p-1}$$

so the exponential series $\sum_{n=0}^{+\infty} x^n/n$ converges if $|x|_p < p^{-1/(p-1)} = r_p$ and diverges if $|x|_p > p^{-1/(p-1)} = r_p$. If $|x|_p = r_p$, i.e. $\operatorname{ord}_p x = 1/(p-1)$, we have

$$\operatorname{ord}_p (a_n x^n) = -\frac{n - S_n}{p-1} + \frac{n}{p-1} = \frac{S_n}{p-1}$$

and, choosing $n = p^m$ so $S_n = 1$, we have $\left|a_{p^m} x^{p^m}\right|_p = p^{-1/(p-1)} > 0$; we have found a subsequence of $(|a_n x^n|_p)_n$ which does not converge to zero so we conclude that if $|x|_p = r_p$ the exponential series diverges. □

We immediately note that $D(r_p^-) \subsetneq D(1^-)$, i.e. $\exp_p$ converges in a smaller disc than $\log_p$. We now prove that, like in the classical case, the p-adic exponential transforms sums into products.

Proposition 4.14. *If* $x, y \in D(r_p^-)$ *then* $\exp_p(x+y) = \exp_p(x) \cdot \exp_p(y)$.

Proof. Let's first observe that $x, y \in D(r_p^-) \implies x + y \in D(r_p^-)$ so we can compute $\exp_p(x+y)$. The rest of the proof is completely analogue to the proof of Proposition 4.10, using the fact that $\exp(x+y) = \exp(x) \cdot \exp(y)$ if $x, y \in \mathbb{R}$ (which then can be translated to a relation between power series by Proposition 4.1). □

Finally we have all the tools we need to prove the relation between p-adic exponential and logarithm.

Proposition 4.15. *The functions* $\log_p$*, defined by* $x \mapsto \log_p(1 + (x-1))$*, and* $\exp_p$ *give mutually inverse isomorphisms between the multiplicative group* $(D_1(r_p^-), \cdot)$ *and the additive group* $(D(r_p^-), +)$.

Proof. First of all let's observe that $\exp_p \colon D(r_p^-) \to D_1(r_p^-)$ and $\log_p \colon D_1(r_p^-) \to D(r_p^-)$ so that the proposition actually makes sense. To prove that $\exp_p(x) \in 1 + D(r_p^-) \subset 1 + D(1^-)$ let's note that

$$x \in D(r_p^-) \implies \operatorname{ord}_p \left(\frac{x^n}{n!}\right) = n \cdot \operatorname{ord}_p (x) - \operatorname{ord}_p (n!) > \frac{n}{p-1} - \frac{n - S_n}{p-1} = \frac{S_n}{p-1} \geq \frac{1}{p-1}$$

so we have

$$\operatorname{ord}_p\left(\exp_p(x)-1\right)=\operatorname{ord}_p\left(\sum_{n=1}^{+\infty}\frac{x^n}{n!}\right)\geq\min_{n\geq 1}\left\{\operatorname{ord}_p\left(\frac{x^n}{n!}\right)\right\}>\frac{1}{p-1}$$
$$\implies \exp_p(x)\in 1+D(r_p^-).$$

Instead, to prove that $\log_p(1+x)\in D(r_p^-)$ if $x\in D(r_p^-)$ let's observe that

$$\operatorname{ord}_p\left(\frac{x^n}{n}\right)-\frac{1}{p-1}>\frac{n}{p-1}-\operatorname{ord}_p(n)-\frac{1}{p-1}=\frac{n-1}{p-1}-\operatorname{ord}_p(n)=: f(n).$$

We claim that f has its minima at $n=1$ and $n=p$, where it's zero. To see why this is true let's first observe that we can just consider the case where $n=p^k$ for $k\in\mathbb{N}$ since if $n'=p^k m$ with $p\nmid m$ we have $f(n')\geq f(n)$. It is then an easy calculation to verify that $f(p^{k+1})\geq f(p^k)$ for $k\in\mathbb{N}$. Thus we have

$$\operatorname{ord}_p\left(\log_p(1+x)\right)=\operatorname{ord}_p\left(\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{x^n}{n}\right)\geq\min_{n>0}\left\{\operatorname{ord}_p\left(\frac{x^n}{n}\right)\right\}>\frac{1}{p-1}$$

which means precisely $\log_p(1+x)\in D(r_p^-)$.
We have already proved in some previous propositions that $\exp_p\colon (D(r_p^-),+)\to(D_1(r_p^-),\cdot)$ and $\log_p\colon (D_1(r_p^-),\cdot)\to(D(r_p^-),+)$ are group morphisms so now we have only to prove that they are mutually inverse.
To see that $\log_p\circ\exp_p\colon D(r_p^-)\to D(r_p^-)$ is the identity function we compute

$$\log_p(\exp_p(x))=\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{(\exp_p(x)-1)^n}{n}=\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{\left(\sum_{m=1}^{+\infty}\frac{x^m}{m!}\right)^n}{n}.$$

Since if $x\in\mathbb{R}$ we have $\log(\exp(x))=x$ we infer, by Proposition 4.1, that the following formal identity holds in $\mathbb{Q}[\![X]\!]$:

$$\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{\left(\sum_{m=1}^{+\infty}\frac{X^m}{m!}\right)^n}{n}=X$$

which implies $\log_p(\exp_p(x))=x$ for $x\in D(r_p^-)$. The same exact reasoning can be also used to prove $\exp_p(\log_p(1+x))=1+x$ for $x\in D(r_p^-)$. □

This proposition implies, in particular, that $\log_p$ is injective on $D_1(r_p^-)$. It is easy to see that this is the biggest disc where this is true: in-fact if $\zeta\in\mathbb{C}_p$ is a primitive p-th root of 1 then, by Lemma 4.3, $|\zeta-1|_p=p^{-1/(p-1)}=r_p$ and $\log_p(\zeta)=0=\log_p(1)$.

Definition 4.16. The (partial) functions $\sin_p\colon\mathbb{C}_p\to\mathbb{C}_p$ and $\cos_p\colon\mathbb{C}_p\to\mathbb{C}_p$ defined by

$$\sin_p(x):=\sum_{n=0}^{+\infty}(-1)^n\frac{x^{2n+1}}{(2n+1)!}$$
$$\cos_p(x):=\sum_{n=0}^{+\infty}(-1)^n\frac{x^{2n}}{(2n)!}$$

are the p-adic sine and the p-adic cosine.

It's easy to prove that $\sin_p$ and $\cos_p$ are defined on $D(r_p^-)$.
Another important function in classical analysis is the binomial expansion

$$B_a(x)=\sum_{n=0}^{+\infty}\binom{a}{k}x^n$$

where $x, a \in \mathbb{C}$ and we used the generalized binomial coefficient defined by:

$$\binom{a}{k} := \begin{cases} 1, & \text{if } k = 0 \\ \frac{a(a-1)\dots(a-k+1)}{k!}, & \text{otherwise} \end{cases}.$$

This is exactly the MacLaurin series of $f(x) = (1+x)^a$. Using ratio test it can be proved that for any $a \in \mathbb{C}$ this series converges if $|x| < 1$ and, unless $a \in \mathbb{N}$, diverges if $|x| > 1$. Its behaviour when $|x| = 1$ is a little more complicated and depends on the value of a. We'll now try to define an analogue function in the p-adic environment.

Definition 4.17. Fixed $a \in \mathbb{C}_p$, the (partial) function $B_{a,p}(X)\colon \mathbb{C}_p \to \mathbb{C}_p$ defined by

$$B_{a,p}(X) := \sum_{n=0}^{+\infty} \binom{a}{n} X^n = 1 + \sum_{n=1}^{+\infty} \frac{a(a-1)\dots(a-n+1)}{n!} X^n$$

is the p-adic binomial expansion

We'll now try to study where it converges (it will be more complicated than the previous functions, since this is actually the first series with coefficient in $\mathbb{C}_p$, and not in $\mathbb{Q}$).

Proposition 4.18. *If $|a|_p > 1$ then the region of convergence of $B_{a,p}(X)$ is $D((r_p/|a|_p)^-)$. Instead, if $|a|_p \le 1$ the binomial expansion surely converges on $D(r_p^-)$ (although the region of convergence can be bigger). Finally, if $a \in \mathbb{Z}_p$ then $B_{a,p}(X) \in \mathbb{Z}_p[\![X]\!]$ so it surely converges on $D(1^-)$.*

Proof. Let's suppose $|a|_p > 1$. Then, by the isosceles triangle principle, if $i \in \mathbb{Z}$ then $|a - i|_p = |a|_p$ and we obtain that the n-th term of the series has norm $|ax|_p^n/|n!|_p$. Thus, with a little computation, we obtain that the radius of convergence is $r = p^{-1/(p-1)}/|a|_p = r_p/|a|_p$. Similarly to the exponential case it's easy to prove that the region of convergence if $D((r_p/|a|_p)^-)$.
If $|a|_p \le 1$ it is more difficult to find the exact region of convergence; anyway if $i \in \mathbb{Z}$ we have $|a - i|_p \le \max\{|a|_p, |i|_p\} \le 1$ so $\left|\binom{a}{n}x^n\right|_p \le |x^n/n!|_p$. Then $B_{a,p}(X)$ surely converges on $D(r_p^-)$.
To prove that if $a \in \mathbb{Z}_p$ then $B_{a,p}(X) \in \mathbb{Z}_p[\![X]\!]$ we just need to show that $\binom{a}{n} \in \mathbb{Z}_p$ for every $n \in \mathbb{N}$ (we already know $\binom{a}{n} \in \mathbb{Q}_p$). Let's fix n and choose $a_0 \in \mathbb{Z}$ such that $a_0 > n$ and $\operatorname{ord}_p(a - a_0) > N$, where N will be chosen later (to choose a_0 we can just truncate the p-adic expansion of $a \in \mathbb{Z}_p$ at some index greater than N). Now $\binom{a_0}{n} \in \mathbb{Z} \subset \mathbb{Z}_p$ and it suffices to show that $\left|\binom{a_0}{n} - \binom{a}{n}\right|_p \le 1$ for a suitable N (then we can conclude using the ultrametric inequality). This easily follows from the continuity of the polynomial $X(X-1)\dots(X-n+1)$ (special case of Proposition 4.7). Then $B_{a,p}(X) \in \mathbb{Z}_p[\![X]\!]$ if $a \in \mathbb{Z}_p$ so, by Proposition 4.6, it converges in $D(1^-)$. □

We can now prove the main property of the binomial expansion, and justify the shorthand $B_{a,p}(X) = (1+X)^a$, at least for $a \in \mathbb{Q}$.

Proposition 4.19. *If $a \in \mathbb{Q}^\times$ and $x \in \mathbb{C}_p$ is in the region of convergence of $B_{a,p}(X)$, then $[B_{a,p}(x)]^{1/a} = 1 + x$.*

Proof. Let's first consider $a = 1/m$ with $m \in \mathbb{Z}^\times$. The idea behind the proof is the usual one: if $x \in \mathbb{R}$ and $|x| < 1$ we have $B_{1/m}(x) = (1+x)^{1/m}$ so $B_{1/m}(x)^m = 1 + x$ which, by Proposition 4.1, gives us the formal identity between the two power series in $\mathbb{Q}[\![X]\!]$ (observe that $m < 0$ doesn't create problems since $B_{1/m}(X)$ is an invertible element of $\mathbb{Q}[\![X]\!]$) that we then translate into an equality between p-adic analytic functions (observe the trivial fact $a \in \mathbb{Q} \implies B_{a,p}(X) \in \mathbb{Q}[\![X]\!]$). We must pay attention only to the last step, i.e. we can substitute only x in the region of convergence of $B_{1/m,p}(X)$ so, for example, if $p \mid m$ we can use $x \in D((r_p|m|_p)^-)$ and if $p \nmid m$ we can choose $x \in D(r_p^-)$. We have proved that $B_{1/m,p}(x)^m = 1 + x$ for every x where $B_{1/m,p}(X)$

converges.
Now let $a = n/m$ with $n, m \in \mathbb{Z}^\times$. It is easy to prove, using the same technique as before, that $B_{n/m,p}(X) = B_{1/m,p}(X)^n$. Then we can write

$$B_{n/m,p}(X)^{m/n} = B_{1/m,p}(X)^m = 1 + X,$$

which proves the thesis. □

We can use the p-adic binomial expansion to study an interesting example of how the same convergent series in $(\mathbb{Q}, |\ |)$ and in $(\mathbb{Q}_p, |\ |_p)$ can have different sums.

Example 4.20. Let's consider the following power series:

$$B_{1/2}\left(\frac{7}{9}\right) = \sum_{n=0}^{+\infty} \binom{1/2}{n} \left(\frac{7}{9}\right)^n \qquad \in \mathbb{Q}[\![X]\!],$$
$$B_{1/2,7}\left(\frac{7}{9}\right) = \sum_{n=0}^{+\infty} \binom{1/2}{n} \left(\frac{7}{9}\right)^n \qquad \in \mathbb{Q}_7[\![X]\!].$$

They are exactly the same power series but they converge to different numbers, both of which are of course square roots of $\frac{16}{9}$ (clearly its square roots are the same both in $\mathbb{Q}$ and in $\mathbb{Q}_7$). In the first case, working in $(\mathbb{Q}, |\ |)$, we have

$$B_{1/2}\left(\frac{7}{9}\right) = \left(1 + \frac{7}{9}\right)^{1/2} = \frac{4}{3} > 0.$$

Instead, in the second case, we have

$$B_{1/2,7}\left(\frac{7}{9}\right) = \left(1 + \frac{7}{9}\right)^{1/2} = -\frac{4}{3} < 0.$$

In-fact, $\mathrm{ord}_7\left(\frac{7}{9}\right) = 1$ so for $n \geq 1$ we have

$$\left|\frac{1/2(1/2-1)\dots(1/2-n+1)}{n!} \cdot \left(\frac{7}{9}\right)^n\right|_7 \leq \frac{7^{-n}}{|n!|_7} = 7^{\frac{-5n-S_n}{6}} < 1$$

so it must be $B_{1/2,7}\left(\frac{7}{9}\right) \equiv 1 \mod 7$. Now it's easy to see that $-\frac{4}{3} \equiv 1 \mod 7$ and $\frac{4}{3} \equiv -1 \mod 7$. We conclude that necessarily $B_{1/2,7}\left(\frac{7}{9}\right) = -\frac{4}{3}$.

This example also warns us about the danger of using the notation $B_{a,p}(X) = (1+X)^a$, which comes certainly handy sometimes but we have to remember that it can yield different results than the ones we would expect on $\mathbb{R}$.

4.2 The Iwasawa logarithm and Artin-Hasse exponential

Definition 4.21. Let $X \subseteq \mathbb{C}_p$ be a set with no isolated points. A function $f\colon X \to \mathbb{C}_p$ is *differentiable* at $a \in X$ if

$$\exists \lim_{X \ni x \to a} \frac{f(x) - f(a)}{x - a} =: f'(a) \in \mathbb{C}_p.$$

Equivalently, f is differentiable at $a \in X$ if

$$f(x) = f(a) + (x-a)f'(a) + (x-a)\varphi(x), \qquad \lim_{X \ni x \to a} \varphi(x) = 0.$$

We also introduce a stronger notion of differentiability for p-adic functions, which will give us some analogue theorems to the classical case.

Definition 4.22. Let $X \subseteq \mathbb{C}_p$ be a set with no isolated points. A function $f\colon X \to \mathbb{C}_p$ is *strictly differentiable* at $a \in X$ (and we write $f \in S^1(a)$) if the difference quotients

$$\Phi f(x,y) := \frac{f(x)-f(y)}{x-y}$$

tends to $\mathbb{C}_p \ni \ell = f'(a)$ as $X \times X \setminus \Delta_X \ni (x,y) \to (a,a)$. Here we used the notation $\Delta_X = \{(x,x) : x \in X\} \subset X \times X$. We say $f \in S^1(X)$ if $f \in S^1(a)$ for every $a \in X$.

In the classical case this definition is not very useful: in-fact if $I \subset \mathbb{R}$ is an open interval and $f \in \mathcal{C}^1(I, \mathbb{R})$ then f is strictly differentiable at every point of I. In the next example we'll see this is not the case in p-adic analysis.

Example 4.23. Let's consider the sequence of disjoint open balls $(B_n)_{n\geq 1}$ defined by

$$B_n := \{x \in \mathbb{Z}_p : |x - p^n|_p < \left|p^{2n}\right|_p\} \subseteq \{x \in \mathbb{Z}_p : |x|_p = |p^n|_p\}$$

and let $f\colon \mathbb{Z}_p \to \mathbb{C}_p$ defined by

$$f(x) := \begin{cases} p^{2n}, & \text{if } x \in B_n; \\ 0, & \text{otherwise}; \end{cases}.$$

The function f is constant on each open ball B_n, hence f is locally constant outside the origin. Then f is differentiable at every $\mathbb{Z}_p \ni x \neq 0$ and $f'(x) = 0$. At the origin

$$\lim_{\mathbb{Z}_p \ni x \to 0} \frac{f(x) - f(0)}{x} = \lim_{\mathbb{Z}_p \ni x \to 0} \frac{f(x)}{x} = 0$$

so $f'(0) = 0$ (to see why it is true, let $x = up^n, u \in \mathbb{Z}_p^\times$; then $f(x) = p^{2n}$ and so $\frac{f(x)}{x} = u^{-1}p^n$). Then $f'\colon \mathbb{Z}_p \to \mathbb{C}_p$ is identically 0 so it is obviously continuous (i.e. $f \in \mathcal{C}^1$) but f is not strictly differentiable at 0. In-fact, let's consider $\Phi f(x,y)$ where $x = x_n = p^n$ and $y = y_n = p^n - p^{2n}$:

$$\Phi f(x_n, y_n) = \frac{f(x_n) - f(y_n)}{x_n - y_n} = \frac{p^{2n} - 0}{p^{2n}} = 1$$

so, if we consider this particular path $(x_n, y_n) \to (0,0)$ as $n \to +\infty$ we obtain

$$0 = f'(0) \neq \lim_{n \to +\infty} \Phi f(x_n, y_n) = 1,$$

which implies f is not strictly differentiable at 0 (we have used that $|y_n|_p = |p^n|_p$ and $y_n \notin B_n$).

We'll now prove a proposition which we're very familiar with in classical analysis.

Proposition 4.24. *If $f\colon X \to \mathbb{C}_p$ is strictly differentiable at $a \in X$ and $f'(a) \neq 0$, then there is a neighbourhood V of $a \in X$ in which f is injective.*

Proof. Since $f \in S^1(a)$ and $|f'(a)|_p > 0$ we can find a neighbourhood V of a such that

$$\left|\Phi f(x,y) - f'(a)\right|_p < \left|f'(a)\right|_p \qquad \text{for } (x,y) \in V \times V \setminus \Delta_V.$$

Then, by the isosceles triangle principle, we must have $|\Phi f(x,y)|_p = |f'(a)|_p$ which means exactly

$$|f(x) - f(y)|_p = \left|f'(a)\right|_p |x-y|_p \qquad \text{for } (x,y) \in V \times V. \qquad \square$$

Let's now focus on analytic functions; they are, like in the classical case, everywhere strictly differentiable any number of times (i.e. they're in $\bigcap_{k>0} S^k$). We'll only prove it for $k = 1$.

Theorem 4.25. *Let $f(X) = \sum_{n\geq 0} a_n X^n$ be an analytic function which converges on $D = D(r^-)$. Then $f \in S^1(D)$ and f' is given by*

$$f'(X) = \sum_{n=1}^{+\infty} n a_n X^{n-1}.$$

Proof. It's immediate to note that the radius of convergence of f' is greater or equal to r, the radius of convergence of f, since $|n|_p \leq 1$ for every $n \in \mathbb{N}$. First of all let's fix $x \in D$ and prove that

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

We can re-write this limit as

$$\lim_{h\to 0} \left| \sum_{n=2}^{+\infty} a_n \cdot \left(\frac{(x+h)^n - x^n}{h} - n x^{n-1} \right) \right|_p = 0;$$

and using the binomial theorem on $(x+h)^n$ we can then write

$$\lim_{h\to 0} \left| \sum_{n=2}^{+\infty} a_n \cdot \left(\sum_{i=0}^{n-2} \binom{n}{i} x^i h^{n-1-i} \right) \right|_p = 0.$$

Let's now distinguish two cases: $x = 0$ and $x \neq 0$.
If $x = 0$ then we must prove $\lim_{h\to 0} \left|\sum_{n=2}^{+\infty} a_n \cdot h^{n-1}\right|_p = 0$, which easily follows from

$$\lim_{h\to 0} \left| \sum_{n=2}^{+\infty} a_n \cdot h^{n-1} \right|_p \leq \lim_{h\to 0} \left(|h|_p \cdot \max_{n\geq 2} \left\{ \left|a_n h^{n-2}\right|_p \right\} \right) = 0,$$

where we considered $0 < |h|_p < r$ and exploited the fact that $\lim_{n\to+\infty} \left|a_n h^{n-2}\right|_p = 0$ so the maximum in the limit above is bounded.
Now, assuming $x \neq 0$ and $0 < |h|_p < |x|_p$, it's easy to see that

$$\left| \sum_{i=0}^{n-2} \binom{n}{i} x^i h^{n-1-i} \right|_p \leq |h|_p^{n-1} \cdot \max_{0\leq i\leq n-2} \left\{ \left|x^i h^{-i}\right|_p \right\} \leq |h|_p^{n-1} \cdot \left(\frac{|x|_p}{|h|_p} \right)^{n-2} = |h|_p \cdot |x|_p^{n-2}.$$

Then we have

$$\left| \sum_{n=2}^{+\infty} a_n \cdot \left(\sum_{i=0}^{n-2} \binom{n}{i} x^i h^{n-1-i} \right) \right|_p \leq |h|_p \cdot \max_{n\geq 2} \left\{ \left|a_n x^{n-2}\right|_p \right\},$$

and since $\lim_{n\to+\infty} \left|a_n x^{n-2}\right|_p = 0$ the maximum above is bounded so

$$\lim_{h\to 0} \left| \sum_{n=2}^{+\infty} a_n \cdot \left(\sum_{i=0}^{n-2} \binom{n}{i} x^i h^{n-1-i} \right) \right|_p \leq \lim_{h\to 0} \left(|h|_p \cdot \max_{n\geq 2} \left\{ \left|a_n x^{n-2}\right|_p \right\} \right) = 0.$$

We have proved that f is differentiable everywhere and f' is its derivative.
We won't prove here that f is actually strictly differentiable: a proof of this statement for a particular case (where $r \geq 1$, i.e. $\lim_{n\to+\infty} |a_n|_p = 0$) can be found at [6, p. 239]. □

Example 4.26. We can now prove one well known result of classical analysis: the derivative of e^x is e^x. More precisely, if $x \in D(r_p^-)$ then $\frac{\mathrm{d}}{\mathrm{d}x} \exp_p(x) = \exp_p(x)$. It easily follows applying Theorem 4.25:

$$\frac{\mathrm{d}}{\mathrm{d}x} \exp_p(x) = \frac{\mathrm{d}}{\mathrm{d}x} \left(\sum_{n=0}^{+\infty} \frac{x^n}{n!} \right) = \sum_{n=1}^{+\infty} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$

Definition 4.27. Let $f\colon \mathbb{C}_p \to \mathbb{C}_p$ be a (partial) function. If for every x in its domain there exists a neighbourhood where f is a power series, we say that f is *locally analytic.*

We present now two p-adic locally analytic functions: the *Iwasawa logarithm* and the *Artin-Hasse* exponential.

Proposition 4.28. *There exists a unique function* $\operatorname{Log}_p\colon \mathbb{C}_p^\times \to \mathbb{C}_p$ *such that:*

(1) Log_p *agrees with* $\log_p$ *in* $D_1(1^-)$*, i.e.,*

$$\operatorname{Log}_p(x) = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(x-1)^n}{n} \qquad \text{for } |x-1|_p < 1;$$

(2) $\operatorname{Log}_p(xy) = \operatorname{Log}_p(x) + \operatorname{Log}_p(y)$ *for all* $x, y \in \mathbb{C}_p^\times$*;*

(3) $\operatorname{Log}_p(p) = 0$.

Proof. We recall from Proposition 3.40 that any non-zero $x \in \mathbb{C}_p$ can be written as $x = p^r \omega(x_1)\langle x_1\rangle$, where p^r is a root of the equation $X^b - p^a = 0$ where $r = \frac{a}{b} = \operatorname{ord}_p(x)$, $\omega(x_1)$ is a root of 1 and $|\langle x_1\rangle - 1|_p < 1$. If such an extension of the logarithm exists, then, by *(2)* and *(3)*, it must be

$$\operatorname{Log}_p(x) = \operatorname{Log}_p(p^r) + \operatorname{Log}_p(\omega(x_1)) + \operatorname{Log}_p(\langle x_1\rangle) = 0 + 0 + \operatorname{Log}_p(\langle x_1\rangle) = \log_p(\langle x_1\rangle),$$

since $\langle x_1\rangle \in D_1(1^-)$. Then there is at most one extension of the logarithm and it is the one defined by

$$\operatorname{Log}_p(x) := \log_p(\langle x_1\rangle).$$

First of all we have to show that this is well defined: in-fact we could have chosen another root of $X^b - p^a = 0$ and we would have obtained a different factorization of the same element. Let's suppose that

$$x = p^r \cdot \omega(x_1) \cdot \langle x_1\rangle = \frac{p^r}{\zeta} \cdot \omega\left(x_1\overline{\zeta}\right) \cdot \left\langle x_1\overline{\zeta}\right\rangle,$$

where $\zeta \in \mathbb{C}_p$ is a b-th root of unity and $\overline{\zeta} = \zeta + M \in A/M$ (we recall that $A = D(1), M = D(1^-)$ in $\mathbb{C}_p$). We have to prove then that $\log_p(\langle x_1\rangle) = \log_p(\langle x_1\overline{\zeta}\rangle)$. Let's first recall how the Teichmüller representatives are defined: if $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$ then $\omega\colon \overline{\mathbb{F}_p} \to \mathbb{Z}_p^{\text{unram}}$ is a section of the projection $\pi\colon \mathbb{Z}_p^{\text{unram}} \twoheadrightarrow \mathbb{Z}_p^{\text{unram}}/p\mathbb{Z}_p^{\text{unram}} = \overline{\mathbb{F}_p}$ such that $\omega(x)^{p^f-1} = 1$ if $x \in \mathbb{F}_{p^f}^\times$ and $\omega(0) = 0$ (it is immediate that since ω can be defined on every finite field of characteristic p, see the proof of Proposition 3.28, it can be extended to $\overline{\mathbb{F}_p}$). It's easy to see that $\omega\colon \overline{\mathbb{F}_p}^\times \to \left(\mathbb{Z}_p^{\text{unram}}\right)^\times$ is a group morphism, i.e. $\omega(xy) = \omega(x)\cdot\omega(y)$: in-fact if $x, y \in \mathbb{F}_{p^f}$ then $\omega(xy)$ is defined as the only element of $\mathbb{Z}_p^{\text{unram}}$ such that $\omega(xy)^{p^f} = \omega(xy)$ and $\pi(\omega(xy)) = xy$ and it's clear that $\omega(x)\cdot\omega(y)$ satisfies both these conditions. We also recall from Proposition 3.40 that we can find a big enough $f \in \mathbb{N}$ such that

$$\mathbb{F}_{p^f} \ni x_1 = \frac{x}{p^r} + M,$$
$$\mathbb{F}_{p^f} \ni x_1\overline{\zeta} = \frac{x\zeta}{p^r} + M = \left(\frac{x}{p^r} + M\right)\cdot(\zeta + M).$$

Explained all the notations, we can finally write

$$\omega\left(x_1\overline{\zeta}\right) = \omega(x_1)\cdot\omega\left(\overline{\zeta}\right) \implies \left\langle x_1\overline{\zeta}\right\rangle = \frac{x\zeta}{p^r\cdot\omega\left(x_1\overline{\zeta}\right)} = \langle x_1\rangle\cdot\frac{\zeta}{\omega\left(\overline{\zeta}\right)}.$$

Now, since $\zeta^b = 1$, we have $\overline{\zeta}^b = 1$ so $\omega\left(\overline{\zeta}\right)^b = 1$, since ω is a group morphism and $\omega(1) = 1$. Finally,

$$\left(\frac{\zeta}{\omega\left(\overline{\zeta}\right)}\right)^b = \frac{\zeta^b}{\omega\left(\overline{\zeta}\right)^b} = 1$$

so $\xi := \frac{\zeta}{\omega(\overline{\zeta})}$ is a root of 1. Let's prove that $|\xi - 1|_p < 1$; let's suppose by contradiction that $\xi = 1 + \Delta$ with $|\Delta|_p \geq 1$ and let's write $\langle x_1 \rangle = 1 + \delta$ with $|\delta|_p < 1$. We know by hypothesis that $\langle x_1 \overline{\zeta} \rangle \in D_1(1^-)$ so we must have

$$|(1+\delta)\cdot(1+\Delta) - 1|_p = |\delta + \Delta \cdot (1+\delta)|_p < 1$$

but since $|\delta|_p < 1$ and $|1+\delta|_p = 1$, we have $|\Delta \cdot (1+\delta)|_p = |\Delta|_p \geq 1$ so

$$|\delta + \Delta \cdot (1+\delta)|_p = \max\left\{|\delta|_p, |\Delta \cdot (1+\delta)|_p\right\} = |\Delta|_p \geq 1,$$

which is absurd (here we have used several times the isosceles triangle principle). We have proved that ξ is a root of 1 with $|\xi - 1|_p < 1$ so we can compute $\log_p(\xi) = 0$. Then

$$\log_p\left(\langle x_1 \overline{\zeta} \rangle\right) = \log_p(\langle x_1 \rangle) + \log_p(\xi) = \log_p(\langle x_1 \rangle)$$

and the function Log_p is well defined.
Properties *(1)* and *(3)* are now obvious from the definition: if $x \in D_1(1^-)$ then we can choose $x = \langle x \rangle$ so $\operatorname{Log}_p(x) = \log_p(x)$ and $p = p^1 \cdot 1 \cdot 1$ so $\operatorname{Log}_p(p) = \log_p(1) = 0$. To prove *(2)* let $x = p^r \omega(x_1)\langle x_1 \rangle$, $y = p^s \omega(y_1)\langle y_1 \rangle$ and $z = xy = p^{r+s}\omega(z_1)\langle z_1 \rangle$. Now p^{r+s} isn't necessarily the same fractional power as $p^r p^s$ (it can differ by a root of unit), but we can choose to use exactly $p^r p^s$, since the value of Log_p doesn't depend on the choice of the fractional power. In this case we'll have $z_1 = \frac{z}{p^r p^s} + M = x_1 y_1$ so $\omega(z_1) = \omega(x_1) \cdot \omega(y_1)$ and $\langle z_1 \rangle = \langle x_1 \rangle \cdot \langle y_1 \rangle$. Then $\operatorname{Log}_p(xy) = \operatorname{Log}_p(x) + \operatorname{Log}_p(y)$. □

Proposition 4.29. *Log_p is locally analytic on $\mathbb{C}_p^\times$ with derivative $\mathbb{C}_p^\times \ni x \mapsto \frac{1}{x}$.*

Proof. Let's fix a point $x_0 \in \mathbb{C}_p^\times$ and let $r := |x_0|_p$. For every $x \in D_{x_0}(r^-)$ (the largest disc about x_0 which doesn't contain 0) we have $\left|\frac{x}{x_0} - 1\right|_p < 1$ and so

$$\operatorname{Log}_p(x) = \operatorname{Log}_p\left(x_0 \cdot \left(1 + \frac{x}{x_0} - 1\right)\right) = \operatorname{Log}_p(x_0) + \sum_{n=1}^{+\infty} (-1)^{n+1} \cdot \frac{(x-x_0)^n}{n \cdot x_0^n}.$$

We have just proved that, in a neighbourhood of x_0, Log_p can be represented by a convergent power series in $x - x_0$. Since this reasoning can be done for any $x_0 \in \mathbb{C}_p^\times$ we can conclude that Log_p is locally analytic.
Let's consider $x \in D_{x_0}(r^-)$ as above: using the locally analyticity of Log_p and Theorem 4.25 we obtain:

$$\frac{\mathrm{d}}{\mathrm{d}x}\operatorname{Log}_p(x) = \sum_{n=1}^{+\infty}(-1)^{n+1} \cdot \frac{(x-x_0)^{n-1}}{x_0^n} = x_0^{-1} \cdot \sum_{n=0}^{+\infty}\left(1 - \frac{x}{x_0}\right)^n = \frac{x_0^{-1}}{(x/x_0)} = \frac{1}{x}. \qquad \square$$

We have found a locally analytic function defined on $\mathbb{C}_p^\times$ which extends $\log_p$ and has the same basic properties.

It is now natural to try to build a homomorphism $f\colon \mathbb{C}_p \to \mathbb{C}_p^\times$ extending the exponential, which is only defined in $D(r_p^-)$. If there exists such an extension then, fixed $x \in \mathbb{C}_p^\times$ and $n \in \mathbb{N}$ such that $p^n x \in D(r_p^-)$, then

$$f(x)^{p^n} = f(p^n x) = \exp_p(p^n x)$$

so $f(x)$ must be a p^n-th root of $\exp_p(p^n x)$. As stated in the next proposition, this extension can actually be done in a coherent way.

Proposition 4.30. *There exists a continuous homomorphism* $\mathrm{Exp}\colon \mathbb{C}_p \to D_1(1^-)$ *extending* $\exp_p$.

Proof. The idea behind the proof exploits the fact that, since $(D_1(1^-), \cdot)$ is a divisible group, there is an extension property for homomorphisms defined over subgroups. For the whole proof see [6, p. 259]. □

Unlike the Iwasawa logarithm, the extensions Exp of the exponential are not defined in a canonic way so they're not very useful. Anyway it is easy to prove that, chosen such an extension Exp, $\log_p \circ \mathrm{Exp} = \mathrm{id}_{\mathbb{C}_p}$. In-fact:

$$p^n \cdot \left(\log_p \circ \mathrm{Exp}(x)\right) = \log_p \left(\mathrm{Exp}(x)^{p^n}\right) = \log_p \left(\mathrm{Exp}\left(p^n x\right)\right) = \log_p \left(\exp_p \left(p^n x\right)\right) = p^n x.$$

We'll now describe a slightly different exponential function which converges in $D(1^-)$: the Artin-Hasse exponential. Before defining it we'll need to study some basic properties of the well known Möbius function.

Definition 4.31. Let $\mu\colon \mathbb{N}^\times \to \mathbb{N}$ be defined by

$$\mu(n) := \begin{cases} 0, & \text{if } n \text{ is divisible by a perfect square greater than 1;} \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct prime factors;} \end{cases}.$$

This is the *Möbius function.*

Proposition 4.32. *Let* $n \in \mathbb{N}^\times$, *then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{otherwise;} \end{cases}.$$

In particular, if p is a prime,

$$\sum_{d|n,\, p\nmid d} \mu(d) = \begin{cases} 1, & \text{if } n \text{ is a power of p;} \\ 0, & \text{otherwise;} \end{cases}.$$

Proof. The case $n = 1$ is trivial ($\mu(1) = 1$). Let $n = p_1^{a_1} \dots p_s^{a_s}$ with $s \geq 1$ and p_i prime for every $i = 1, \dots, s$. Then, by an easy combinatoric argument, we have

$$\sum_{d|n} \mu(d) = \sum_{\varepsilon_i = 0 \vee 1} \mu(p_1^{\varepsilon_1} \dots p_s^{\varepsilon_s}) = \sum_{\varepsilon_i = 0 \vee 1} (-1)^{\sum \varepsilon_i} = (1-1)^s = 0.$$

The second statement is just a particular case of the first one applied to $n \cdot p^{-\mathrm{ord}_p(n)}$ in place of n. □

Proposition 4.33. *In* $\mathbb{Q}[\![X]\!]$ *the following holds:*

$$\exp(X) = \prod_{n=1}^{+\infty} B_{-\mu(n)/n}(-X^n).$$

Proof. First of all let's observe that the infinite product of series actually makes sense: in-fact $B_{-\mu(n)/n,p}(-X^n) = 1 + \frac{\mu(n)}{n} X^n + o(X^n)$ so the n-th factor has no power of X less than the n-th, so only a finite number of series is involved to determine the coefficient of any power of X. To prove that the identity holds we'll use Proposition 4.1; let $x \in \mathbb{R}$ with $|x| < 1$, then we know that

$$B_{-\mu(n)/n}(-x^n) = (1 - x^n)^{-\frac{\mu(n)}{n}}.$$

Taking the (classical) log of the right side we obtain

$$\log\left(\prod_{n=1}^{+\infty}(1-x^n)^{-\frac{\mu(n)}{n}}\right) = -\sum_{n=1}^{+\infty}\frac{\mu(n)}{n}\cdot\log(1-x^n) = \sum_{n=1}^{+\infty}\frac{\mu(n)}{n}\cdot\sum_{m=1}^{+\infty}\frac{x^{nm}}{m} = \sum_{j=1}^{+\infty}\left(\frac{x^j}{j}\cdot\sum_{n|j}\mu(n)\right)$$

where in the last step we set $j = nm$ and we rearranged the terms of the series since it is absolutely convergent. To see why this is true, let's consider

$$\sum_{n=1}^{+\infty}\left|\frac{\mu(n)}{n}\right|\cdot|\log(1-x^n)| \leq \sum_{n=1}^{+\infty}\frac{|\log(1-x^n)|}{n}.$$

Since $|\log(1-x^n)| \sim -|x|^n$ as $n \to +\infty$, we can just study the convergence of the series

$$\sum_{n=1}^{+\infty}\frac{|x|^n}{n},$$

which converges since it is dominated by the convergent geometric series $\sum_{n=1}^{+\infty}|x|^n$ (we're using $|x| < 1$). Now that we have justified why we can rearrange terms, using Proposition 4.32, we obtain

$$\log\left(\prod_{n=1}^{+\infty}(1-x^n)^{-\frac{\mu(n)}{n}}\right) = \sum_{j=1}^{+\infty}\left(\frac{x^j}{j}\cdot\sum_{n|j}\mu(n)\right) = x = \log(\exp(x))$$
$$\implies \exp(x) = \prod_{n=1}^{+\infty}(1-x^n)^{-\frac{\mu(n)}{n}}$$

which, translated back to formal power series, concludes the proof. □

We have just proved that

$$\exp_p(X) = \prod_{n=1}^{+\infty}B_{-\mu(n)/n,\,p}(-X^n)$$

(recall that $B_{-\mu(n)/n,\,p}(X) = B_{-\mu(n)/n}(X)$ and $\exp_p(X) = \exp(X)$, as elements of $\mathbb{Q}[\![X]\!]$). With this new expression of $\exp_p(X)$ we can understand where convergence "problems" arise. In-fact if $p \mid n$ and n is square-free (so $\mu(n) \neq 0$) then $|\mu(n)/n|_p = |n|_p^{-1} \geq p$ so $B_{-\mu(n)/n,\,p}(-X^n)$ converges only if $|x|_p^n \in D((r_p|n|_p)^-)$ (see Proposition 4.18). If $n = p$ we have convergence precisely when

$$|x|_p < \left(p^{-1/(p-1)}\cdot p^{-1}\right)^{\frac{1}{p}} = p^{-1/(p-1)} = r_p.$$

Instead, if $p \nmid n$, we have no problems, since $-\frac{\mu(n)}{n} \in \mathbb{Z}_p$ and, by Proposition 4.18, we have $B_{-\mu(n)/n,\,p}(-X^n) \in \mathbb{Z}_p[\![X]\!]$ so $x \in D(1^-)$ guarantees convergence. This motivates the following definition.

Definition 4.34. The (partial) function $\mathrm{E}_p(X)\colon \mathbb{C}_p \to \mathbb{C}_p$ defined by

$$\mathrm{E}_p(X) := \prod_{\substack{n=1\\ p\nmid n}}^{+\infty}B_{-\mu(n)/n,\,p}(-X^n) = \prod_{\substack{n=1\\ p\nmid n}}^{+\infty}(1-X^n)^{-\frac{\mu(n)}{n}}$$

is called the *Artin-Hasse exponential.*

We observe again that $B_{-\mu(n)/n,\,p}(-X^n) \in 1 + X^n\mathbb{Q}[\![X]\!]$ so the infinite product makes sense.

Proposition 4.35. *In $\mathbb{Q}[\![X]\!]$ the following holds:*

$$\mathrm{E}_p(X) = \exp_p\left(\sum_{i=0}^{+\infty} \frac{X^{p^i}}{p^i}\right).$$

Proof. As usual let's consider $x \in \mathbb{R}$ with $|x| < 1$: then

$$\mathrm{E}_p(x) := \prod_{\substack{n=1 \\ p\nmid n}}^{+\infty} (1 - x^n)^{-\frac{\mu(n)}{n}}$$

and taking logarithm we obtain

$$\log\left(\mathrm{E}_p(x)\right) = -\sum_{\substack{n=1 \\ p\nmid n}} \frac{\mu(n)}{n}\left(\sum_{m=1}^{+\infty} \frac{x^{mn}}{m}\right) = \sum_{j=1}^{+\infty}\left(\frac{x^j}{j} \cdot \sum_{n|j,\, p\nmid n} \mu(n)\right),$$

where in the last step we set $j = nm$ and we rearranged the terms of the series (we can do it, the proof is analogue to the one given in Proposition 4.33). Using Proposition 4.32 we obtain the following relation (in $\mathbb{R}$):

$$\log\left(\mathrm{E}_p(x)\right) = \sum_{m=0}^{+\infty} \frac{x^{p^m}}{p^m} \implies \mathrm{E}_p(x) = \exp\left(\sum_{m=0}^{+\infty} \frac{x^{p^m}}{p^m}\right).$$

We can conclude immediately applying Proposition 4.1 (recall that $\exp_p$ and exp are exactly the same formal series in $\mathbb{Q}[\![X]\!]$). □

At this point it is very easy to prove that $\mathrm{E}_p(X)$ converges on $D(1^-)$ (much better than the smaller disc of convergence of $\exp_p(X)$).

Proposition 4.36. *The Artin-Hasse exponential* $\mathrm{E}_p(X)$ *converges on* $D(1^-)$.

Proof. We recall the definition of E_p:

$$\mathrm{E}_p(X) := \prod_{\substack{n=1 \\ p\nmid n}}^{+\infty} B_{-\mu(n)/n,\, p}(-X^n).$$

Now if $p \nmid n$ we have already proved that $B_{-\mu(n)/n,\, p}(-X^n) \in 1 + X^n(\mathbb{Z}_p \cap \mathbb{Q})[\![X]\!]$ so the whole series $\mathrm{E}_p(X)$ has coefficients in $\mathbb{Z}_p \cap \mathbb{Q}$. Then we conclude using Proposition 4.6. □

We could have proved directly that $\exp_p\left(\sum_{n=0}^{+\infty} \frac{x^{p^n}}{p^n}\right) \in \mathbb{Z}_p[\![X]\!]$ using the Dwork's lemma. In-fact we already know that $\mathrm{E}_p(X) \in 1 + X\mathbb{Q}_p[\![X]\!]$ and we can compute

$$\mathrm{E}_p(X^p) = \exp_p\left(\sum_{n=0}^{+\infty} \frac{X^{p^{n+1}}}{p^n}\right),$$

$$\mathrm{E}_p(X)^p = \exp_p\left(\sum_{n=0}^{+\infty} \frac{X^{p^n}}{p^{n-1}}\right) = \exp_p\left(pX + \sum_{n=0}^{+\infty} \frac{X^{p^{n+1}}}{p^n}\right),$$

where we used $\exp_p(Y)^p = \exp_p(pY)$ (this formal identity can be easily verified using Proposition 4.1). Since $\frac{\exp_p(X)}{\exp_p(Y)} = \exp_p(X - Y)$ (also easy to prove) we have

$$\frac{\mathrm{E}_p(X^p)}{\mathrm{E}_p(X)^p} = \frac{\exp_p\left(\sum_{n=0}^{+\infty} \frac{X^{p^{n+1}}}{p^n}\right)}{\exp_p\left(pX + \sum_{n=0}^{+\infty} \frac{X^{p^{n+1}}}{p^n}\right)} = \exp_p(-pX) \in 1 + pX\mathbb{Z}_p[\![X]\!]$$

and we can conclude that $\mathrm{E}_p(X) \in 1 + X\mathbb{Z}_p[\![X]\!]$ thanks to Lemma 4.2.

5 Newton polygons

We'll now introduce a very useful tool to study radius of convergence and zeroes of an analytic function: the Newton polygon. We'll first introduce it for polynomials and then try to generalize our results to power series.

5.1 Newton polygons for polynomials

Definition 5.1. Let $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ be a polynomial and consider the following set of points in $\mathbb{R}^2$:

$$\Gamma := \{(0,0)\} \cup \{(i, \operatorname{ord}_p a_i) \mid a_i \neq 0, i \in \{1, \dots, n\}\}.$$

The *Newton polygon* of $f(X)$ is the inferior convex hull of these points, i.e. the highest convex polygonal line joining $(0,0)$ with $(n, \operatorname{ord}_p a_n)$ which passes on or below all the points in Γ.

A nice way to think at the Newton polygon is the following: we begin with a vertical line through $(0,0)$ and we rotate it about $(0,0)$ counter-clockwise until we hit some point of Γ; then we consider the segment joining $(0,0)$ with the last point we hit (P) as the first segment of the Newton polygon and we continue to rotate the line counter-clockwise about P and repeat the procedure.

Example 5.2. In Fig. 5.1 it is shown the Newton polygon for $f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4 + 54X^5$ in $\mathbb{Q}_3[X]$.

Let's introduce some basic terms we'll adopt from now on.

Definition 5.3. The *vertices* of the Newton polygon are the points $\left(i_j, \operatorname{ord}_p a_{i_j}\right)$ where the slope changes, the *segments* of the Newton polygon are the segments joining one vertex to the next one; if a segment joins (i, m) to (i', m') its slope is $\frac{m'-m}{i'-i}$ and its length is $i' - i$, i.e. the length of its projection onto the horizontal axis.

We have defined the Newton polygon only for a polynomial with constant term 1, but this doesn't cause loss of generality because the main use of the Newton polygon is to characterize

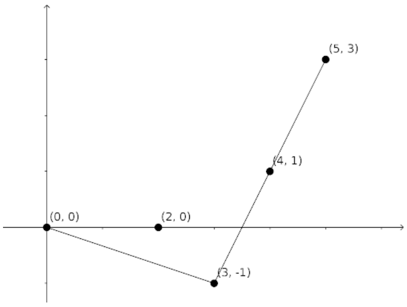


Figure 5.1: Newton polygon of $f(X) \in \mathbb{Q}_3[X]$

zeroes (and radius of convergence) of $f(X)$. Given a generic $g(X) \in \mathbb{C}_p[X]$ we can write:

$$g(X) = b_k X^k + \cdots + b_n X^n = b_k \cdot X^k \cdot \left(1 + \frac{b_{k+1}}{b_k} X + \cdots + \frac{b_n}{b_k} X^{n-k}\right) =: b_k \cdot X^k \cdot f(X)$$

and we can study $f(X)$, which satisfies our initial hypothesis. Before proving our main result about the Newton polygon for polynomials, let's recall what symmetric polynomials are.

Definition 5.4. Let K be a commutative ring with unit, $\underline{X} := (X_1, \ldots, X_n)$ and let $P(\underline{X}) \in K[\underline{X}]$ be a polynomial in n variables. We say that $P(\underline{X})$ is symmetric if for every $\sigma \in S_n$ we have $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$, where S_n is the symmetric group of n elements.
The symmetric polynomials $\{e_i(\underline{X}) : i \in \{0, 1, \ldots, n\}\}$ defined by

$$e_0(\underline{X}) = 1,$$
$$e_k(\underline{X}) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \ldots X_{i_k}$$

are the *elementary symmetric polynomials.*

It is well known that the symmetric polynomials in n variables form a subring $K[\underline{X}]^{S_n}$ and if $P(\underline{X})$ is symmetric then there exists $Q(\underline{Y}) \in K[\underline{Y}]$ such that $P(\underline{X}) = Q(e_1(\underline{X}), \ldots, e_n(\underline{X}))$, i.e. the elementary symmetric polynomials "generate" all symmetric polynomials. It is easy to prove that if $f(X) \in K[X]$ is a monic polynomial of degree n (here we add the hypothesis that K is an integral domain, i.e. there are no divisors of zero) and all its roots are $\alpha_1, \ldots, \alpha_n$ then

$$f(X) = \prod_{j=1}^{n} (X - \alpha_j) = \sum_{j=0}^{n} (-1)^{n-j} \cdot e_{n-j}(\alpha_1, \ldots, \alpha_n) \cdot X^j,$$

which is a precise relation between the coefficients of f and its roots. Finally we recall that if $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in K[X]$ has degree n (here K is a field) and $\alpha_1, \ldots, \alpha_n$ are all of its roots, we can write

$$f(X) = \prod_{j=1}^{n} \left(1 - \frac{X}{\alpha_j}\right) = \sum_{j=0}^{n} (-1)^j \cdot e_j\left(\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_n}\right) \cdot X^j;$$

in-fact $f(0) = 1$ and we can divide by $1 = (-1)^n a_n \alpha_1 \ldots \alpha_n$ both sides of $f(X) = a_n(X - \alpha_1) \ldots (X - \alpha_n)$.
We are ready to state and prove the following.

Theorem 5.5. *Let $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ be a polynomial of degree n, let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}_p$ be all of its roots and $\lambda_i := \mathrm{ord}_p(1/\alpha_i)$. If λ is a slope of the Newton polygon of f with length l, it follows that precisely l of the λ_i are equal to λ. Vice-versa, if γ is a p-adic order of a reciprocal root then there is a segment of the Newton polygon with slope γ.*

Proof. The last statement is trivial if we prove the first one: in-fact the total length of the Newton polygon is n so we have already considered all the roots (counting multiplicity).
Let's suppose the α_i arranged so that $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Let's suppose that $\lambda_1 = \lambda_2 = \cdots = \lambda_r < \lambda_{r+1}$. We then claim that the first segment of the Newton polygon is the one joining $(0, 0)$ to $(r, r\lambda_1)$. We know that $a_i = (-1)^i \cdot e_i(1/\alpha_1, \ldots, 1/\alpha_n)$ and, recalling how the i-th elementary symmetric polynomial is defined (sum of all possible products of i different variables) and that $\mathrm{ord}_p(x + y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$, we obtain

$$\mathrm{ord}_p(a_i) \geq i\lambda_1,$$

which means that the point $(i, \mathrm{ord}_p(a_i))$ is on or above the line joining $(0, 0)$ to $(r, r\lambda_1)$. Let's now consider a_r: only one of the products of r of the $1/\alpha_i$ has p-adic order $r\lambda_1$ and it is exactly

$1/(\alpha_1 \dots \alpha_r)$, while all the other products have bigger p-adic order since they must include at least one $1/\alpha_i$ with $i > r$. Then, by the isosceles triangle principle, $\mathrm{ord}_p(a_r) = r\lambda_1$. Finally, let's consider a_i with $i > r$: for the same reasoning as before we have $\mathrm{ord}_p(a_i) > i\lambda_1$.
All these considerations means exactly that the first segment of the Newton polygon is the one joining $(0,0)$ and $(r, r\lambda_1) = (r, \lambda_1 + \dots + \lambda_r)$. Now, if we have $\lambda_s < \lambda_{s+1} = \dots = \lambda_{s+t} < \lambda_{s+t+1}$ the line joining $(s, \lambda_1 + \dots + \lambda_s)$ to $(s+t, \lambda_1 + \dots + \lambda_s + t\lambda_{s+1})$ is a segment of the Newton polygon. The proof is very similar: if $s \leq i$ then $\mathrm{ord}_p(a_i) \geq \lambda_1 + \dots + \lambda_s + (i-s)\lambda_{s+1}$, since this is the minimum p-adic order in $e_i(1/\alpha_1, \dots, 1/\alpha_n)$, reached for example by $1/(\alpha_1 \dots \alpha_i)$, $\mathrm{ord}_p(a_{s+t}) = \lambda_1 + \dots + \lambda_s + t\lambda_{s+1}$ by the isosceles triangle principle and if $i > s+t$ then $\mathrm{ord}_p(a_i) > \lambda_1 + \dots + \lambda_s + (i-s)\lambda_{s+1}$ since we have to choose at least one $1/\alpha_j$ with $j > s+t$. □

This theorem, in other words, says that the slopes of the Newton polygon of $f(X)$ are counting with multiplicity the p-adic orders of the reciprocal roots of $f(X)$. The aim of the rest of this chapter will be to extend this result to formal power series, but we'll need to do a little more work before.

5.2 Newton polygons for power series

The definition of the Newton polygon for $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ is the same of Definition 5.1: it is the inferior convex hull of all the points in Γ (which, this time, will be infinite). Sometimes we'll denote the Newton polygon of $f(X)$ by $\mathfrak{N}(f)$. From now on we'll only consider proper power series, i.e. we'll exclude the case in which $f(X)$ is a polynomial. We can distinguish three different kinds on Newton polygon.

(1) We get infinitely many segments of finite length, for example the Newton polygon $f(X) = 1 + \sum_{i=1}^{+\infty} p^{i^2} X^i$ shown in Fig. 5.2a.

(2) At some point the line we're rotating simultaneously hits infinite points. In this case the Newton polygon has only a finite number of segments, the last one being infinitely long. An example is $f(X) = 1 + \sum_{i=1}^{+\infty} X^i$, whose Newton polygon is simply the horizontal axis.

(3) At some point the line we're rotating has not hit any point yet but it cannot rotate any farther without passing above some points. If this happens, we let the last segment of the Newton polygon have slope equal to the least upper bound of all possible slopes for which the line passes below all the points. A simple example is given by $f(X) = 1 + \sum_{i=1}^{+\infty} pX^i$, whose Newton polygon is the horizontal axis as shown in Fig. 5.2b.

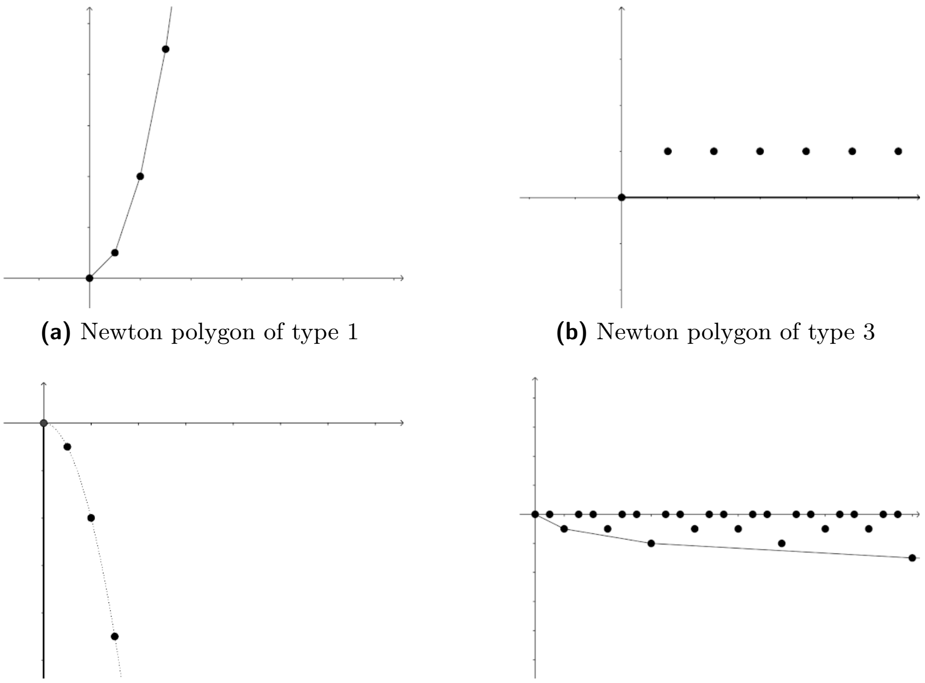
There is a degenerate case of type (3): the vertical line through $(0,0)$ cannot be rotated at all without crossing above some points $(i, \mathrm{ord}_p a_i)$. An example of this possibility is given by $f(X) = \sum_{i=0}^{+\infty} \frac{X^i}{p^{i^2}}$, whose Newton polygon is shown in Fig. 5.2c. We'll exclude this case from our study since, as we'll prove in the next proposition, all such series have zero radius of convergence.

Proposition 5.6. *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ be a power series whose Newton polygon is a degenerate case of type (3), i.e.*

$$\forall m \in \mathbb{R} \quad \exists i_m \in \mathbb{N} : \mathrm{ord}_p\, a_{i_m} < m \cdot i_m.$$

Then the radius of convergence of f is 0.

Proof. We just need to prove that $\limsup |a_n|_p^{1/n} = +\infty$. Let's define a subsequence of the coefficients $(a_{n_k})_{k\geq 1}$ by induction. We set $n_1 = i_{-1}$ so that $(n_1, \mathrm{ord}_p\, a_{n_1})$ lies below the line $y = -x$. Let's now consider the lines ℓ_1, joining $(0,0)$ to $(n_1, \mathrm{ord}_p\, a_{n_1})$, and ℓ_2, with equation $y = -2x$: by hypothesis there must be an infinite number of points $(i, \mathrm{ord}_p\, a_i)$ lying below both of these two lines. Then there is at least one such point $(j, \mathrm{ord}_p\, a_j)$ with $j > n_1$ and we



(a) Newton polygon of type 1

(b) Newton polygon of type 3

(c) Degenerate Newton polygon

(d) Newton polygon of $f(X)$

Figure 5.2: Various Newton polygons

set $n_2 := j > n_1$. We can iterate this procedure (every time we choose $n_k > n_{k-1}$ such that $(n_k, \operatorname{ord}_p a_{n_k})$ lies below both $y = -kx$ and the line joining $(0,0)$ to $(n_{k-1}, \operatorname{ord}_p a_{n_{k-1}})$). We have obtained an increasing sequence $(n_k)_{k\geq 1} \subseteq \mathbb{N}$ such that

$$\operatorname{ord}_p a_{n_k} < -k \cdot n_k \implies |a_{n_k}|_p^{1/n_k} > p^k.$$

Using this subsequence we can conclude. □

From now on we'll always consider analytic functions with a non-trivial disc of convergence. Before proving general properties of the Newton polygon of analytic functions, let's consider a concrete example.

Example 5.7. Let's consider the function f defined by

$$f(X) = \sum_{n=0}^{+\infty} \frac{X^n}{n+1} = \frac{1}{X} \cdot \sum_{n=0}^{+\infty} \frac{X^{n+1}}{n+1} = -\frac{1}{X} \cdot \log_p(1-X).$$

Looking at the right member it's immediate to see that f converges in $D(1^-)$. If we denote ℓ_i the segment joining $\left(p^i - 1, -i\right)$ to $\left(p^{i+1} - 1, -i-1\right)$ then it's easy to see that the Newton polygon of f is the polygonal line $\bigcup_{i\in\mathbb{N}} \ell_i$ shown in Fig. 5.2d for $p = 3$. Assuming that the power series analogue of Theorem 5.5 holds, then, by looking at the Newton polygon of f, we would expect to find exactly $p^{i+1} - p^i$ roots having p-adic order $1/\left(p^{i+1} - p^i\right)$ for every $i \in \mathbb{N}$ and no other roots.

Let's prove this claim: let's fix $j \in \mathbb{N}$ and consider $x = 1 - \zeta$, where $\zeta \in \mathbb{C}_p$ is a primitive p^{j+1}-th root of 1. Then we know by Lemma 4.3 that $\operatorname{ord}_p x = 1/\left(p^{j+1} - p^j\right)$ and that $\log_p(1-x) = 0$ by Corollary 4.10.1 so $f(x) = 0$. Since there are exactly $p^{i+1} - p^i$ primitive roots of 1, we have found all the predicted roots. Let's now prove that there are no other roots of f, i.e. any root is of the form $1 - \xi$ where ξ is a primitive p^k-th root of 1. Let $x \in D(1^-)$ be a root of f and let

$$x_j := 1 - (1-x)^{p^j}$$

for any $j \in \mathbb{N}$. Using Newton's binomial expansion we get

$$|x_j|_p = \left|1-(1-x)^{p^j}\right|_p = \left|\sum_{i=1}^{p^j}\binom{p^j}{i}(-x)^i\right|_p \leq |x|_p < 1,$$

which implies $x_j \in D(1^-)$ for every j. We claim that for any $M > 0$ we can find $j_m \in \mathbb{N}$ such that $|x_{j_m}|_p < M$. Fixed $M > 0$ we just need to find a j such that

$$\max_{1\leq i\leq p^j}\left|\binom{p^j}{i}x^i\right|_p < M.$$

Since $|x|_p < 1$ we can find $N \in \mathbb{N}$ such that if $n > N$ then $\left|\binom{p^j}{n}x^n\right|_p < M$. Now we just need to find a j such that

$$\max_{1\leq i\leq N}\left|\binom{p^j}{i}x^i\right|_p < M.$$

Writing $m := \max_{1\leq i\leq N}(1/|i!|_p) > 0$ we have that

$$\left|\binom{p^j}{i}\right|_p \leq \left|\frac{p^j}{i!}\right|_p \leq |p^j|_p \cdot m$$

and we can conclude, since $\left|p^j\right|_p \to 0$ as $j \to +\infty$. Now let's consider $j \in \mathbb{N}$ such that $x_j \in D(r_p^-)$; thanks to Proposition 4.15 we have

$$1-x_j = \exp_p(\log_p(1-x_j)) = \exp_p\left(p^j \cdot \log_p(1-x)\right) = \exp_p(0) = 1$$

hence $(1-x)^{p^j} = 1$ so that $x = 1-\zeta$ where ζ is a p^j-th root of 1 and it's one of the roots we already considered.
We have proved that, for this particular $f(X)$, the power series analogue of Theorem 5.5 holds.

Let's now prove a simple but interesting result which explains how we can find the radius of convergence of a series just by looking at its Newton polygon.

Proposition 5.8. *Let $f(X) = 1+\sum_{i=1}^{+\infty} a_iX^i \in 1+X\mathbb{C}_p[\![X]\!]$ and let b be the least upper bound of all slopes of the Newton polygon of f. Then the radius of convergence of $f(X)$ is p^b (if $b = +\infty$ then f converges everywhere).*

Proof. Let's fix $x \in \mathbb{C}_p$ with $|x|_p < p^b$, i.e. $-b' := \operatorname{ord}_p x > -b$. Then $\operatorname{ord}_p(a_ix^i) = \operatorname{ord}_p a_i - ib'$ but, since $b' < b$, it's clear that sufficiently far out all the points $(i, \operatorname{ord}_p a_i)$ will lie arbitrarily far above $(i, b'i)$, see Fig. 5.3. This means exactly $\lim_{i\to+\infty}\operatorname{ord}_p(a_ix^i) = +\infty$, i.e. $f(X)$ converges at x. Let's now consider the case $|x|_p > p^b$, i.e. $-b' := \operatorname{ord}_p x < -b$. Since $b' > b$ we find an infinite number of $i \in \mathbb{N}$ such that $\operatorname{ord}_p(a_ix^i) = \operatorname{ord}_p a_i - ib' < 0$ which implies that $f(X)$ does not converge at x. We can then conclude that the radius of convergence of f is exactly p^b. □

Obviously this proposition doesn't tell us anything about the convergence of $f(X)$ at the radius of convergence, i.e. if $|x|_p = p^b$.

Proposition 5.9. *Let $f(X) = 1+\sum_{i=1}^{+\infty} a_iX^i \in 1+X\mathbb{C}_p[\![X]\!]$ be an analytic power series with radius of convergence $r = p^b$, where b is the least upper bound of the slopes of the Newton polygon. Then $f(X)$ converges on $D(r)$ if and only if $\mathfrak{N}(f)$ is of type (3) (see the beginning of Section 5.2) and $\lim_{i\to+\infty} d_i = +\infty$, where d_i is the distance between $(i, \operatorname{ord}_p a_i)$ and the last line of $\mathfrak{N}(f)$.*

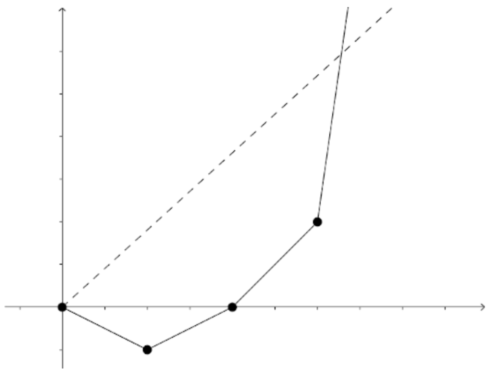
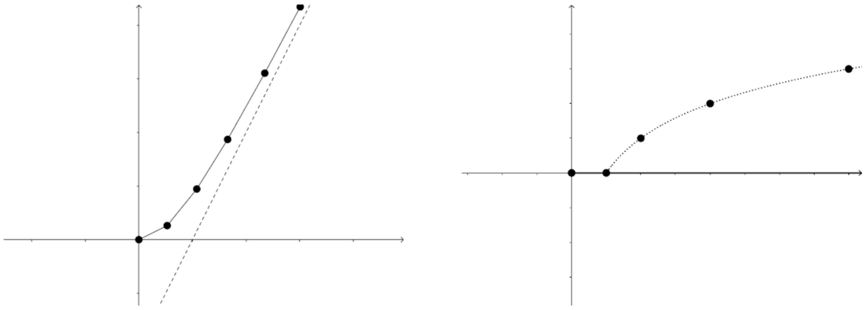


Figure 5.3: Case $|x|_p < p^b$



(a) Newton polygon with an asymptote

(b) Newton polygon with convergence at border

Figure 5.4: Two other types of Newton polygons

Proof. If $b \notin \mathbb{Q}$ there's nothing to prove since no element of $\mathbb{C}_p$ can have order b; from now on we'll assume $b \in \mathbb{Q}$. First of all we prove that if the Newton polygon of f is of type (1) or (2) then $f(X)$ does not converge if $|x|_p = p^b$.

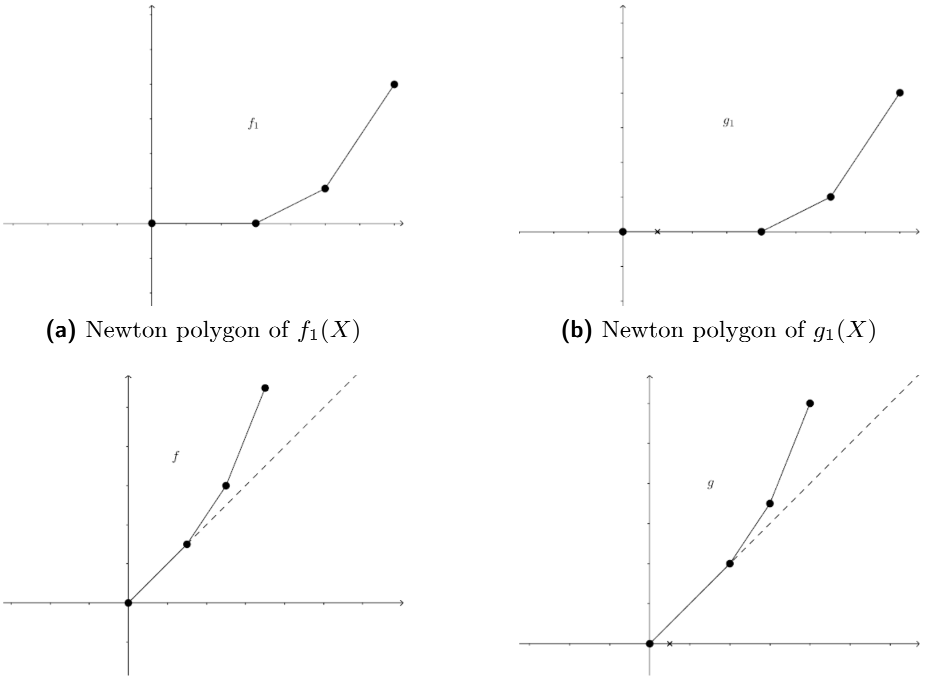
Let's first consider a Newton polygon of type (1) and let Λ be the set of all its slopes. Then $b = \sup \Lambda$ and if $b = +\infty$ there's nothing to prove. If $b < +\infty$ then there exists $y_0 \in \mathbb{R}$ such that $\ell \colon y = y_0 + bx$ is an "asymptote" of the Newton polygon, see Fig. 5.4a (the slopes are increasing and their sup/lim is b). Then we can consider the vertices of the Newton polygon, indexed by $(i_j)_{j \in \mathbb{N}}$. It is clear that the distance d_j between $\left(i_j, \operatorname{ord}_p a_{i_j}\right)$ and ℓ tends to 0 and so does $\left(\operatorname{ord}_p a_{i_j} - i_j b\right)$, which is equal to $d_j / \cos(\arctan b)$ (if $b = 0$ then it is equal to d_j). If $|x|_p = p^b$ then $\operatorname{ord}_p x = -b$ so $\operatorname{ord}_p (a_i x^i) = \operatorname{ord}_p a_i - ib$. We then conclude that $\operatorname{ord}_p (a_i x^i) \not\to +\infty$ when $i \to +\infty$, i.e. f does not converge at x. Instead if f has a Newton polygon of type (2) then b is its final slope and, by definition, there are infinite points on this final segment. This means that if we call the final line $\ell \colon y_0 + bx$ then we can find an increasing subsequence $(i_j)_{j \in \mathbb{N}} \subseteq \mathbb{N}$ such that $\operatorname{ord}_p a_{i_j} = y_0 + i_j b$ so $\operatorname{ord}_p \left(a_{i_j} x^{i_j}\right) = y_0 \not\to +\infty$ and we can conclude that there's no convergence in x.

Let's now suppose that $\mathfrak{N}(f)$ is of type (3) and $x \in \mathbb{C}_p$ with $|x|_p = p^b$. Then $f(X)$ converges in x if and only if $\lim_{i \to +\infty} \operatorname{ord}_p \left(a_i x^i\right) = +\infty$; as before, with a little trigonometry, we have

$$\operatorname{ord}_p \left(a_i x^i\right) = \operatorname{ord}_p a_i - ib = \begin{cases} d_i, & \text{if } b = 0; \\ \frac{d_i}{\cos(\arctan b)}, & \text{otherwise;} \end{cases}$$

and we can conclude (by hypothesis $\lim_{i \to +\infty} d_i = +\infty$). An example is $f(X) = 1 + \sum_{i=1}^{+\infty} 2^i X^{2^i} \in 1 + X\mathbb{C}_2[\![X]\!]$, whose Newton polygon is shown in Fig. 5.4b. □

Let's introduce a useful trick we'll often use in the next proofs.



(a) Newton polygon of $f_1(X)$ **(b)** Newton polygon of $g_1(X)$

(c) Newton polygon of $f(X)$ **(d)** Newton polygon of $g(X)$

Figure 5.5: Example of Lemma 5.11

Lemma 5.10. *Let $c \in \mathbb{C}_p^\times$ with $\operatorname{ord}_p c = \lambda$, $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ and $g(X) := f\left(X/c\right)$. Then the Newton polygon of g is obtained subtracting the line $y = \lambda x$ to the Newton polygon of f.*

Proof. If we write $g(X) = 1 + \sum_{i=1}^{+\infty} b_i X^i$ then it's immediate that $b_i = a_i / \left(c^i\right)$ so $\operatorname{ord}_p b_i = \operatorname{ord}_p a_i - i\lambda$ and we can conclude. □

We'll now prove four technical lemmas we'll then use to prove our final result.

Lemma 5.11. *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ and suppose that λ_1 is the first slope of its Newton polygon. Let $c \in \mathbb{C}_p$ with $\operatorname{ord}_p c = \lambda \leq \lambda_1$ and assume that $f(X)$ converges on the closed disc $D(p^\lambda)$ (this automatically happens if $\lambda < \lambda_1$ or if the Newton polygon has more than one segment). Let*

$$g(X) = (1 - cX)f(X) \in 1 + X\mathbb{C}_p[\![X]\!].$$

Then $\mathfrak{N}(g)$ is obtained by joining $(0,0)$ to $(1,\lambda)$ and then translating $\mathfrak{N}(f)$ by $\vec{v} = (1,\lambda)$ (1 to the right and λ upwards). If $\mathfrak{N}(f)$ has last slope λ_f and $f(X)$ converges on $D(p^{\lambda_f})$ then $g(X)$ also converges on $D(p^{\lambda_f})$. Conversely, if $g(X)$ converges on $D(p^{\lambda_f})$ then so does $f(X)$.

Proof. A graphic interpretation of the lemma can be found at Fig. 5.5. We can consider only the special case $c = 1, \lambda = 0$. In-fact, let's suppose the lemma holds for this case and let $f(X)$ and $g(X)$ as in the statement. Then $f_1(X) := f\left(\frac{X}{c}\right)$ and $g_1(X) := (1 - X)f_1(X)$ satisfy our hypothesis (with the parameters $\underline{c} = 1, \underline{\lambda} = 0, \underline{\lambda_1} = \lambda_1 - \lambda$, by Lemma 5.10). Thus, since we're assuming the lemma to be true if $c = 1$, we know the shape of the Newton polygon of $g_1(X)$ (and the convergence of $g_1(X)$ on $D(p^{\lambda_f - \lambda})$ when f converges on $D(p^\lambda)$). Now, $g(X) = g_1(cX)$ so, using again Lemma 5.10, we obtain the desired information about the Newton polygon of $g(X)$ (and the desired convergence, which is immediate). So we can just prove the lemma when $c = 1$. If $g(X) = 1 + \sum_{i=1}^{+\infty} b_i X^i$ then, since by definition $g(X) = (1 - X)f(X)$, we have $b_{i+1} = a_{i+1} - a_i$ for $i \geq 0$ (clearly $a_0 = 1$). Then

$$\operatorname{ord}_p b_{i+1} \geq \min\left\{\operatorname{ord}_p a_{i+1}, \operatorname{ord}_p a_i\right\} \tag{$\star$}$$

and the equality holds when $\operatorname{ord}_p a_{i+1} \neq \operatorname{ord}_p a_i$. It is easy to see that both $(i, \operatorname{ord}_p a_i)$ and $(i, \operatorname{ord}_p a_{i+1})$ lie on or above the Newton polygon of $f(X)$ and so does $(i, \operatorname{ord}_p b_{i+1})$, by $(\star)$. If $(i, \operatorname{ord}_p a_i)$ is a vertex then necessarily $\operatorname{ord}_p a_{i+1} > \operatorname{ord}_p a_i$ so $\operatorname{ord}_p b_{i+1} = \operatorname{ord}_p a_i$. This means exactly that the Newton polygon of $g(X)$ has the shape described in the lemma, as far as the last vertex of $f(X)$. If $\mathfrak{N}(f)$ is of type (1) we can conclude here: there is no last vertex and no last slope. It remains only to show that when $\mathfrak{N}(f)$ has last slope λ_f then also $\mathfrak{N}(g)$ does and if $f(X)$ converges on $D(p^{\lambda_f})$ then so does $g(X)$. We already know $\operatorname{ord}_p b_{i+1} \geq \min\{\operatorname{ord}_p a_{i+1}, \operatorname{ord}_p a_i\}$ so $g(X)$ converges wherever $f(X)$ does; then if λ_g is the least upper bound of the slopes of $\mathfrak{N}(g)$ we have $\lambda_g \geq \lambda_f$ (by Proposition 5.8). We must only rule out the case $\lambda_g > \lambda_f$. If it were the case, then, for some large i, the point $(i+1, \operatorname{ord}_p a_i)$ would lie below $\mathfrak{N}(g)$ so we'd have $\operatorname{ord}_p b_j > \operatorname{ord}_p a_i$ for every $j \geq i+1$ (this holds in this particular case where $\lambda = 0$ since $0 \leq \lambda_1 \leq \lambda_f < \lambda_g$). Using $j = i+1$ we obtain $\operatorname{ord}_p a_{i+1} = \operatorname{ord}_p a_i$ because $a_{i+1} = b_{i+1} + a_i$. Then, using $j = i+2$, we obtain $\operatorname{ord}_p a_{i+2} = \operatorname{ord}_p a_{i+1} = \operatorname{ord}_p a_i$ and so on for every j. This means $\operatorname{ord}_p a_j = \operatorname{ord}_p a_i$ for every $j \geq i$ and contradicts the assumed convergence of $f(X)$ on $D(1) \subseteq D(p^{\lambda_f})$. Then we must have $\lambda_g = \lambda_f$ and $\mathfrak{N}(g)$ is exactly of the predicted shape. This implies in particular that if $f(X)$ converges on $D(p^{\lambda_f})$ then so does $g(X)$ (see Proposition 5.9). The converse assertion, i.e. convergence of $g(X)$ implies convergence of $f(X)$, can be proved in an analogue way. □

Lemma 5.12. *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ have Newton polygon with first slope λ_1. Let's assume that $f(X)$ converges on $D\left(p^{\lambda_1}\right)$ and that the line ℓ: $y = \lambda_1 x$ actually passes through a point $(i, \operatorname{ord}_p a_i)$ with $i \geq 1$ (both of these conditions are automatically satisfied if $\mathfrak{N}(f)$ has more than one slope). Then there exists an $x \in \mathbb{C}_p$ for which $\operatorname{ord}_p x = -\lambda_1$ and $f(x) = 0$.*

Proof. Let's first consider the case $\lambda_1 = 0$ and then reduce the general case to this one. If $\lambda_1 = 0$ we have $\operatorname{ord}_p a_i \geq 0$ for every $i \in \mathbb{N}$ and $\lim_{i\to+\infty} \operatorname{ord}_p a_i = +\infty$ since $f(X)$ converges on $D(1)$. Let $N := \max\{i \in \mathbb{N}^\times : \operatorname{ord}_p a_i = 0\}$ and let $f_n(X) := 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$. By Theorem 5.5, if $n \geq N$ then the polynomial $f_n(X)$ has precisely N roots with p-adic order 0, let them be $x_{n,1}, \dots, x_{n,N}$ (it's immediate that $\mathfrak{N}(f_n)$ has a first segment with slope 0 and length N). Let's define a sequence: $x_N := x_{N,1}$ and, for $n \geq N$, $x_{n+1} := x_{n+1,i}$ where i is such that $|x_{n+1,i} - x_n|_p$ is minimal. We claim that $(x_n)_{n\geq N} \subseteq \mathbb{C}_p$ is Cauchy and its limit x is the desired root of f. If S_n denotes the set containing the roots of $f_n(X)$, counted with multiplicity, for $n \geq N$ we have

$$|f_{n+1}(x_n) - f_n(x_n)|_p = |f_{n+1}(x_n)|_p = \prod_{\alpha\in S_{n+1}} \left|1 - \frac{x_n}{\alpha}\right|_p$$

where we used $f_n(x_n) = 0$ and $f_{n+1}(X) = \prod_{\alpha\in S_{n+1}} \left(1 - \frac{X}{\alpha}\right)$. It's clear that if $\alpha \in S_{n+1}$ then $\operatorname{ord}_p \alpha \leq 0$: in-fact we cannot have $\operatorname{ord}_p \alpha > 0$ and $f_{n+1}(\alpha) = 0$ by the isosceles triangle principle (recall that $\operatorname{ord}_p a_i \geq 0$). Now if $\alpha \in S_{n+1}$ has $\operatorname{ord}_p \alpha < 0$ then $\left|1 - \frac{x_n}{\alpha}\right|_p = 1$, since $|x_n|_p = 1$. Then we can write

$$|f_{n+1}(x_n) - f_n(x_n)|_p = \prod_{i=1}^{N} \left|1 - \frac{x_n}{x_{n+1,i}}\right|_p = \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \geq |x_{n+1} - x_n|_p^N,$$

by the choice of x_{n+1}. We have obtained

$$|x_{n+1} - x_n|_p^N \leq |f_{n+1}(x_n) - f_n(x_n)|_p = \left|a_{n+1} x_n^{n+1}\right|_p = |a_{n+1}|_p$$

so $\lim_{n\to+\infty} |x_{n+1} - x_n|_p^N = 0$ (by hypothesis $\lim_{n\to+\infty} |a_{n+1}|_p = 0$) and we have proved that $(x_n)_{n\geq N}$ is Cauchy (see Lemma 3.5). Since $\mathbb{C}_p$ is complete there exists $x := \lim_{n\to+\infty} x_n$ and, by continuity of $|\ |_p$, we have $|x|_p = 1$. It's clear that for any $y \in D(1)$ we have $\lim_{n\to+\infty} f_n(y) = f(y)$ (the p-adic absolute value of the difference tends to zero) so we have $f(x) = \lim_{n\to+\infty} f_n(x)$. Now,

$$|f_n(x)|_p = |f_n(x) - f_n(x_n)|_p = |x - x_n|_p \cdot \left|\sum_{i=1}^{n} a_i \frac{x^i - x_n^i}{x - x_n}\right|_p \leq |x - x_n|_p$$

because $|a_i|_p \leq 1$ and $\left|\frac{x^i - x_n^i}{x - x_n}\right|_p = \left|x^{i-1} + x^{i-2}x_n + \cdots + x_n^{i-1}\right|_p \leq 1$. Hence we can conclude that $f(x) = \lim_{n\to+\infty} f_n(x) = 0$ and we have proved the lemma if $\lambda_1 = 0$.
The general case follows easily. Let $\pi \in \mathbb{C}_p$ be any number with $\operatorname{ord}_p \pi = \lambda_1$. Clearly such a π exists: for example, if $(i, \operatorname{ord}_p a_i)$ lies on $y = \lambda_1 x$ and $i \geq 1$ (such a point exists by assumption) then π can be any i-th root of a_i (recall that $\mathbb{C}_p$ is algebraically closed). Now let $g(X) := f(X/\pi)$; it's clear by Lemma 5.10 that $g(X)$ satisfies the conditions of the lemma with $\lambda_1 = 0$. Then we already know that there exists x_0 with $\operatorname{ord}_p x_0 = 0$ such that $g(x_0) = 0$. Then if $x = x_0/\pi$ we have $\operatorname{ord}_p x = -\lambda_1$ and $f(x) = f(x_0/\pi) = g(x_0) = 0$. □

Lemma 5.13. *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ and let $\alpha \in \mathbb{C}_p$ such that $f(\alpha) = 0$. Let $g(X)$ be obtained by dividing $f(X)$ by $1 - \frac{X}{\alpha}$. Then $g(X)$ converges on $D(|\alpha|_p)$.*

Proof. First of all, let's observe that $\alpha \neq 0$ and that dividing $f(X)$ by $1 - \frac{X}{\alpha}$ is the same thing of multiplying $f(X)$ by the geometric series $\sum_{i=0}^{+\infty} \left(\frac{X}{\alpha}\right)^i$. Let's write $g(X) = 1 + \sum_{i=1}^{+\infty} b_i X^i$ and let $f_n(X) := 1 + \sum_{i=1}^{n} a_i X^i$ be the n-th partial sum of $f(X)$. By an easy computation we infer that

$$b_i = \sum_{j=0}^{i} \frac{a_j}{\alpha^j}$$

where we set $a_0 = 1$. Then it's easy to see that

$$b_i \alpha^i = f_i(\alpha)$$

hence $\left|b_i \alpha^i\right|_p = |f_i(\alpha)|_p \to 0$ as $i \to +\infty$, since $f(\alpha) = 0$ and $f(x) = \lim_{n\to+\infty} f_n(x)$ wherever f converges. This means exactly that $g(X)$ converges on $D(|\alpha|_p)$. □

Lemma 5.14. *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ such that λ is the first slope of $\mathfrak{N}(f)$ and f converges on some disc D. If $\alpha \in D$ is a root of f, i.e. $f(\alpha) = 0$, then $\operatorname{ord}_p \alpha \leq -\lambda$. If λ is the only slope of $\mathfrak{N}(f)$ and no point of $\mathfrak{N}(f)$ lies on $y = \lambda x$, then $\operatorname{ord}_p \alpha < -\lambda$.*

Proof. Let's suppose that $\alpha \in D$ is such that $\operatorname{ord}_p \alpha = -\lambda' > -\lambda$. We have

$$\operatorname{ord}_p (a_i \alpha^i) = \operatorname{ord}_p a_i - i\lambda' > \operatorname{ord}_p a_i - i\lambda \geq 0,$$

where we used that all the points $(i, \operatorname{ord}_p a_i)$ lie on or above the line $y = \lambda x$ (by definition of Newton polygon). Then we have $\operatorname{ord}_p 1 = 0$ and $\operatorname{ord}_p (a_i \alpha^i) > 0$ for $i \geq 1$ and so α cannot be a root of f. The last statement can be proved with an analogue reasoning. □

Finally we are ready to prove the main theorem of this section which will imply, as a corollary, the power series analogue of Theorem 5.5.

Theorem 5.15 (p-adic Weierstrass Preparation Theorem)**.** *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ converge on $D(p^\lambda)$. Let N be the total horizontal length of all segments in $\mathfrak{N}(f)$ having slope less or equal to λ if this length is finite (i.e. if $\mathfrak{N}(f)$ hasn't an infinitely long last segment of slope λ). On the other hand, if the Newton polygon of f has last slope λ, then let N be the greatest index i such that $(i, ord_p a_i)$ lies on that final segment (there must be such a final index since f converges on $D(p^\lambda)$). Then there exists a polynomial $h(X) \in 1 + X\mathbb{C}_p[X]$ of degree N and a power series $g(X) = 1 + \sum_{i=1}^{+\infty} b_i X^i$, which converges and is non-zero on $D(p^\lambda)$, such that*

$$h(X) = f(X) \cdot g(X).$$

The polynomial $h(X)$ is uniquely determined by these properties and $\mathfrak{N}(h)$ coincides with $\mathfrak{N}(f)$ up to $x = N$.

Proof. We use induction on N. Let's first consider the basic case $N = 0$, where the first slope of $\mathfrak{N}(f)$ is greater or equal to λ. In this case it's evident that we can assume $\lambda \in \mathbb{Q}$ without loss of generality. We have to show that $g(X) = 1/f(X)$ converges and is non-zero on $D(p^\lambda)$ (recall that any power series with a non-zero constant term is invertible). We can only consider the special case $\lambda = 0$. In-fact, let $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ converge on $D(p^\lambda)$: we can choose $c \in \mathbb{C}_p$ with $\operatorname{ord}_p c = \lambda$ using Proposition 3.39 (we assumed $\lambda \in \mathbb{Q}$) and then define $\widetilde{f}(X) := f\left(\frac{X}{c}\right)$. Now, $\widetilde{f}$ converges on $D(1)$ and if $\lambda = 0$ then $N = 0$, i.e. the first slope of its Newton polygon is greater or equal to 0 by Lemma 5.10. So, assuming the theorem holds when $N = \lambda = 0$ we infer that there exists $\widetilde{g}(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ which converges and is non-zero on $D(1)$ such that $1 = \widetilde{f}(X) \cdot \widetilde{g}(X)$. Using cX in place of X we obtain $1 = f(X) \cdot \widetilde{g}(cX)$ and it's immediate that $g(X) := \widetilde{g}(cX)$ has all the desired properties. So we can only consider the special case $\lambda = 0$. Thus, we can suppose $\operatorname{ord}_p a_i > 0$ for every $i \in \mathbb{N}$ and $\lim_{i\to+\infty} \operatorname{ord}_p a_i = +\infty$ (we have convergence on $D(1)$). It's easy to obtain the following equality for the coefficients of $g(X) = 1/f(X)$:

$$b_i = -\left(\sum_{j=1}^{i} b_{i-j}a_j\right),$$

where we set $b_0 = 1$. From an easy induction on i it follows that $\operatorname{ord}_p b_i > 0$ for $i \geq 1$. This implies that the first slope of $\mathfrak{N}(g)$ is greater than 0 (or it's equal to 0 but with no points on it) and, by Lemma 5.14, we know that g doesn't have roots on $D(1)$. Now it remains only to show that $g(X)$ actually converges on $D(1)$, i.e. that $\lim_{i\to+\infty} \operatorname{ord}_p b_i = +\infty$. Let's fix $M > 0$: we can find $m \in \mathbb{N}$ such that $i > m$ implies $\operatorname{ord}_p a_i > M$. Now if

$$\varepsilon := \min_{1\leq j\leq m} \operatorname{ord}_p a_j > 0$$

we claim that $i > nm$ implies $\operatorname{ord}_p b_i > \min\{M, n\varepsilon\}$, from which it easily follows $\operatorname{ord}_p b_i \to +\infty$ as $i \to +\infty$. We'll prove this claim by induction on n. We have already proved the case $n = 0$. Now, let's suppose $n \geq 1$ and that the claim holds for $n - 1$; if $i > nm$ we have

$$b_i = -\left(b_{i-1}a_i + \cdots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \cdots + a_1\right).$$

The terms $b_{i-j}a_j$ with $j > m$ have p-adic order greater than M, while if $j \geq m$ we have $\operatorname{ord}_p(b_{i-j}a_j) \geq \operatorname{ord}_p b_{i-j} + \varepsilon$ and, since $i - j > (n-1)m$, by inductive hypothesis we obtain

$$\operatorname{ord}_p(b_{i-j}a_j) \geq \operatorname{ord}_p b_{i-j} + \varepsilon > \min\{M, (n-1)\varepsilon\} + \varepsilon.$$

This proves our claim, hence the theorem when $N = 0$ (the statement about the Newton polygon here is trivial since $h(X) = 1$).

Now let's consider the general case with $N \geq 1$ and suppose that the theorem holds for $N - 1$. Let $\lambda_1 \leq \lambda$ be the first slope of $\mathfrak{N}(f)$; if it is the only slope then, since $N \geq 1$, there's at least one point on $y = \lambda_1 x$. We can then use Lemma 5.12 to find α such that $f(\alpha) = 0$ and $\operatorname{ord}_p \alpha = -\lambda_1$. Let's define

$$f_1(X) := \frac{f(X)}{1 - \frac{X}{\alpha}} = f(X) \cdot \sum_{j=0}^{+\infty} \left(\frac{X}{\alpha}\right)^j \in 1 + X\mathbb{C}_p[\![X]\!].$$

By Lemma 5.13, f_1 converges on $D(p^{\lambda_1})$. Setting $c := \frac{1}{\alpha}$ we have $f(X) = (1 - cX) \cdot f_1(X)$. Let λ_1' be the first slope of $\mathfrak{N}(f_1)$; it must necessarily be $\lambda_1' \geq \lambda_1$. In-fact $\lambda_1' < \lambda_1$ implies that $\mathfrak{N}(f_1)$ has more than one slope and that, by Lemma 5.12, f_1 has a root with p-adic order $-\lambda_1'$ and so does f, but this is impossible by Lemma 5.14 since $-\lambda_1' > -\lambda_1$. We can now apply Lemma 5.11, with parameters $\underline{f} = f_1, \underline{g} = f, \underline{\lambda} = \lambda_1, \underline{\lambda_1} = \lambda_1'$ and we get that $\mathfrak{N}(f_1)$ is obtained translating $\mathfrak{N}(f) \setminus \ell((0,0),(1,\lambda_1))$ by $\vec{v} = (-1, -\lambda_1)$, where $\ell(P,Q)$ is the segment joining P to Q. We claim that f_1 converges on $D(p^\lambda)$: if λ isn't the final slope of $\mathfrak{N}(f)$ then it's trivially true, otherwise

Lemma 5.11 tells us that when $\mathfrak{N}(f)$ has last slope λ and f converges on $D(p^\lambda)$ then so does f_1. Thus, f_1 satisfies all the conditions of the theorem with $N-1$ instead of N (recall that, to obtain $\mathfrak{N}(f_1)$, we removed a segment with slope $\lambda_1 \leq \lambda$ and with length 1 from $\mathfrak{N}(f)$). By inductive hypothesis we can find $h_1(X) \in 1 + X\mathbb{C}_p[X]$ of degree $N-1$ and a series $g(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, convergent and non-zero on $D(p^\lambda)$, such that

$$h_1(X) = f_1(X) \cdot g(X).$$

Multiplying both sides by $(1-cX)$ and setting $h(X) := (1-cX)h_1(X)$ we obtain

$$h(X) = f(X) \cdot g(X),$$

where h and g have the desired properties. Let's also observe that $\mathfrak{N}(h_1)$ coincides with $\mathfrak{N}(f_1)$ up to $x = N-1$ and that, since $h(X) = (1-cX)h_1(X)$, $\mathfrak{N}(h)$ is obtained joining $(0,0)$ to $(1, \lambda_1)$ and then translating $\mathfrak{N}(h_1)$. Then it's clear that $\mathfrak{N}(h)$ will coincide with $\mathfrak{N}(f)$ up to $x = N$. Now we have only to prove the uniqueness of $h(X)$ (we have only proved its existence). Let's suppose that $\widetilde{h}(X) \in 1 + X\mathbb{C}_p[X]$ is another polynomial of degree N such that

$$\widetilde{h}(X) = f(X) \cdot g_1(X),$$

where $g_1(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ converges and is non-zero on $D(p^\lambda)$. We have

$$\widetilde{h}(X) \cdot g(X) = f(X) \cdot g(X) \cdot g_1(X) = h(X) \cdot g_1(X). \tag{$*$}$$

To prove uniqueness it suffices to show that $(*)$ implies that h and h_1 have the same roots with the same multiplicities (they both have constant term 1). The case $N = 1$ is trivial. Let's now consider $N > 1$. The polynomial $h(X)$ is the one we built before so we already know that $\mathfrak{N}(h)$ coincides with $\mathfrak{N}(f)$ up to $x = N$. Using Theorem 5.5, this means that every root of $h(X)$ is in $D(p^\lambda)$ (by assumption all the slopes of $\mathfrak{N}(h)$ are less or equal to λ). Let $\alpha \in \mathbb{C}_p$ be a root of $h(X)$. Since $\alpha \in D(p^\lambda)$ we can compute $g(\alpha)$ and $g_1(\alpha)$ and, by hypothesis, they're not zero. So α must also be a root of $\widetilde{h}(X)$. Let's define

$$\widetilde{k}(X) := \frac{\widetilde{h}(X)}{1 - \frac{X}{\alpha}}, \qquad k(X) := \frac{h(X)}{1 - \frac{X}{\alpha}};$$

they're two polynomials in $1 + X\mathbb{C}_p[X]$ of degree $N-1$ satisfying $\widetilde{k}(X) \cdot g(X) = k(X) \cdot g_1(X)$. We can repeat this process with every other root of $h(X)$ and, at the end, both polynomials will be 1 so we have proved uniqueness. □

This is a very powerful theorem, with a lot of interesting corollaries.

Corollary 5.15.1. *If a segment of the Newton polygon of $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ has finite length N and slope λ, then there are exactly N values of x (counting multiplicity) for which $f(x) = 0$ and* $\operatorname{ord}_p x = -\lambda$.

Proof. It is an immediate application of Theorem 5.15 and Theorem 5.5. □

Example 5.16. We can use the Newton polygon to study the exact region of convergence of $\mathrm{E}_p(X)$, the Artin-Hasse exponential (see Definition 4.34). We already know, by Proposition 4.35 and Proposition 4.35, that

$$\mathrm{E}_p(X) = \exp_p\left(\sum_{i=0}^{+\infty} \frac{X^{p^i}}{p^i}\right)$$

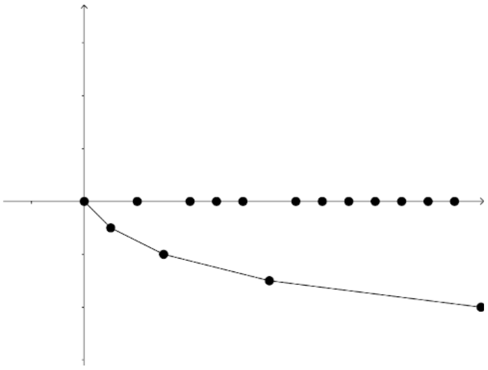


Figure 5.6: Newton polygon of $f(X)$ for $p = 2$

and that $\mathrm{E}_p(X)$ converges on $D(1^-)$. We'll show that this is the exact region of convergence, i.e. that $\mathrm{E}_p(X)$ doesn't converge if $|x|_p = 1$. Let's define

$$f(X) = \sum_{i=0}^{+\infty} \frac{X^{p^i-1}}{p^i} \in 1 + X\mathbb{C}_p[\![X]\!],$$

so that $\mathrm{E}_p(X) = \exp_p(X \cdot f(X))$. Now, $\mathrm{E}_p(X)$ converges at $x \in \mathbb{C}_p$ if and only if $x \cdot f(x) \in D(r_p^-)$. We'll show that $f(X)$ doesn't even converge if $|x|_p = 1$. Writing $f(X) = 1 + \sum_{n=1}^{+\infty} a_i X^i$, it's immediate that

$$(i, \operatorname{ord}_p a_i) = \begin{cases} \left(p^k - 1, -k\right), & \text{if } \exists k \in \mathbb{N} \text{ such that } i = p^k - 1; \\ (i, 0), & \text{otherwise;} \end{cases}.$$

If ℓ_i is the segment joining $\left(p^i - 1, -i\right)$ to $\left(p^{i+1} - 1, -i - 1\right)$ then we have $\mathfrak{N}(f) = \bigcup_{i\in\mathbb{N}} \ell_i$ (see Fig. 5.6 for $p = 2$). It is clearly a type (1) polygon (infinite number of finite segments). The segment ℓ_i has slope $\lambda_i = -\frac{1}{p^i(p-1)} < 0$ and we have $\lim_{i\to+\infty} \lambda_i = 0$. This proves that 0 is the least upper bound of all slopes of $\mathfrak{N}(f)$ so, using Proposition 5.8, we can conclude: the radius of convergence of f is $1 = p^0$ and we cannot have convergence "at the border", since we would need a type (3) polygon.

Finally, we'll show a nice application of Theorem 5.15, which will imply the non-existence of a non-constant power series which converges on $\mathbb{C}_p$ and is never zero. This means exactly that we cannot have an exponential with the same properties of the classical one: in-fact in the classical case, if $h(X)$ is a convergent power series, then $e^{h(X)}$ is everywhere convergent and non-zero. We'll first need a technical lemma.

Lemma 5.17. *Let $f(X)$ be a power series which converges on $D(p^\lambda)$. If $f(X)$ has an infinite number of zeroes on $D(p^\lambda)$ then $f(X)$ is identically zero.*

Proof. If $f(X) = 0$ there's nothing to prove, otherwise we can assume, by contradiction, $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ (we can write $f(X) = a_d X^d \cdot g(X)$, where d is such that a_d is the first non-zero coefficient and study $g(X) \in 1 + X\mathbb{C}_p[\![X]\!]$). We can then apply Theorem 5.15, using λ, to obtain $N \in \mathbb{N}$, $h(X) \in 1 + X\mathbb{C}_p[X]$, a polynomial of degree N, and $g(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, a power series convergent and non-zero on $D(p^\lambda)$, such that

$$h(X) = f(X) \cdot g(X).$$

By hypothesis, $f(X)$ has infinite zeroes in $D(p^\lambda)$ and, since $g(X)$ is never zero on $D(p^\lambda)$, $h(X)$ must have infinite zeroes on $D(p^\lambda)$. But $h(X)$ is a non-zero polynomial of degree N so it cannot have infinite zeroes, and this is a contradiction. Thus the only possible case is $f(X) = 0$. □

Proposition 5.18. *Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ be an everywhere convergent power series. For every λ, let $h_\lambda(X)$ be the polynomial obtained applying Theorem 5.15. Then $h_\lambda \to f$ as $\lambda \to +\infty$ (i.e., each coefficient of h_λ converges to the corresponding coefficient of f). In particular, if f is not a polynomial, then its zeroes are $(r_n)_{n\geq 1}$ (i.e. they're countable infinite) and*

$$f(X) = \prod_{i=1}^{+\infty} \left(1 - \frac{X}{r_i}\right).$$

Proof. If $f(X)$ is a polynomial, then the statement is trivial. From now on we'll consider $f(X)$ to be a proper power series. It's clear that such an f must have a type (1) Newton polygon. Let $(\lambda_n)_{n\geq 1}$ be the slopes of $\mathfrak{N}(f)$ (clearly we consider them in order, i.e. such that $\lambda_1 < \lambda_2 < \cdots < \lambda_n < \ldots$). Since $f(X)$ converges everywhere, by Proposition 5.8 we must have $\lim_{n\to+\infty} \lambda_n = +\infty$. It is also clear that f has a countable infinite set of zeroes (there's clearly no contradiction here, because the zeroes are in $\mathbb{C}_p$): in-fact, applying Corollary 5.15.1, we obtain that for any segment of $\mathfrak{N}(f)$ we have a finite number of zeroes (and clearly the segments of the Newton polygon are countable infinite). Let it be $(r_n)_{n\geq 1}$, where they're listed in such a way that the first "cluster" corresponds to slope λ_1, the second to slope λ_2 and so on. Applying Theorem 5.15 with $\lambda = \lambda_n$ we obtain a polynomial $1 + X\mathbb{C}_p[X] \ni h_n(X) := h_{\lambda_n}(X)$ and a power series $g_n(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, convergent and non-zero on $D(p^{\lambda_n})$, such that

$$h_n(X) = f(X) \cdot g_n(X).$$

Let's introduce some terminology:

$$h_n(X) = 1 + \sum_{i=1}^{d_n} a_{n,i} X^i, \qquad g_n(X) = 1 + \sum_{i=1}^{+\infty} b_{n,i} X^i,$$

where we set $d_n := \deg h_n(X)$. By Theorem 5.15 we know that d_n is the total horizontal length of segments of $\mathfrak{N}(f)$ with slope less or equal to λ_n and this also means that

$$h_n(X) = \prod_{j=1}^{d_n} \left(1 - \frac{X}{r_j}\right). \tag{$*$}$$

First of all, let's prove that the sequences $(a_{n,m})_{n\geq 1}$ are all Cauchy *uniformly* in m, i.e. we'll find an upper bound which doesn't depend on m. Let $k \in \mathbb{N}$ be such that $\lambda_1 < \cdots < \lambda_k < 0 \leq \lambda_{k+1}$, i.e. the first k slopes of $\mathfrak{N}(f)$ are negative. Let's consider $r_1, \ldots, r_{d_k}$, all the roots of f (they're not necessarily distinct) corresponding to the negative slopes of $\mathfrak{N}(f)$. Then $|1/r_i|_p = p^{\operatorname{ord}_p r_i} > 1$, for every $1 \leq 1 \leq d_k$. Instead, for any other root r_m with $m > d_k$ we have $|1/r_m|_p \leq 1$, since it corresponds to a non-negative slope. Let's set $M := |1/r_1|_p \cdots |1/r_{d_k}|_p$ (if all slopes are non-negative we simply set $M = 1$). Recalling the relations between coefficients and reciprocal of roots (using elementary symmetric polynomials), for $n \geq k$, by $(*)$, we have

$$a_{n,m} = (-1)^m \cdot e_m \left(\frac{1}{r_1}, \ldots, \frac{1}{r_{d_k}}, \frac{1}{r_{d_k+1}}, \ldots, \frac{1}{r_{d_n}}\right).$$

Since for any $j > d_k$ we have $|1/r_j|_p \leq 1$, it's easy to see that

$$|a_{n,m}|_p \leq |1/(r_1 \cdots r_{d_k})|_p = M,$$

for any $m \in \mathbb{N}$ and $n \geq k$. We have found a common upper bound for all the coefficients of all the polynomials $h_n(X)$ with $n \geq k$. Now we have

$$h_{n+1}(X) = h_n(X) \cdot \prod_{j=d_n+1}^{d_{n+1}} \left(1 - \frac{X}{r_j}\right)$$

so we obtain

$$a_{n+1,m} = a_{n,m} + \sum_{j=1}^{m} (-1)^j \cdot a_{n,m-j} \cdot e_j\left(\frac{1}{r_{d_n+1}}, \ldots, \frac{1}{r_{d_{n+1}}}\right),$$

where we set $a_{n,0} = 1$. Since $\lim_{n\to+\infty} d_n = +\infty$ (by construction) we can choose a large enough n such that $\lambda_{n+1} > 0$. Then, $|1/r_j|_p = p^{\operatorname{ord}_p r_j} = p^{-\lambda_{n+1}} < 1$ for any $d_n + 1 \leq j \leq d_{n+1}$. Now it's easy to see that

$$\begin{aligned} \forall\, j \in \mathbb{N}, \quad & \left|e_j\left(\frac{1}{r_{d_n+1}}, \ldots, \frac{1}{r_{d_{n+1}}}\right)\right|_p \leq \left|\frac{1}{r_{d_n+1}}\right|_p = p^{-\lambda_{n+1}} \\ \implies |a_{n+1,m} - a_{n,m}|_p = \max_{1\leq j\leq m} & \left|a_{n,m-j} \cdot e_j\left(\frac{1}{r_{d_n+1}}, \ldots, \frac{1}{r_{d_{n+1}}}\right)\right|_p \leq M \cdot p^{-\lambda_{n+1}}. \end{aligned}$$

Since $\lim_{n\to+\infty} p^{-\lambda_{n+1}} = 0$, $(a_{n,m})_{n\geq 1}$ is Cauchy (see Lemma 3.5). Let's observe that our bounds don't depend on m, i.e. $|a_{n+1,m} - a_{n,m}|_p \leq M \cdot p^{-\lambda_{n+1}}$ for any $m \in \mathbb{N}$ and $n \geq k$. Since $(\lambda_n)_{n\geq 1}$ is non-decreasing, for $m > n \geq k$ we obtain

$$|a_{m,i} - a_{n,i}|_p \leq \max_{n\leq j<m} |a_{j+1,i} - a_{j,i}|_p \leq \max_{n\leq j<m} Mp^{-\lambda_{j+1}} = Mp^{-\lambda_{n+1}}.$$

Now, we know that $g_n(X)$ converges and is non-zero on $D(p^{\lambda_n})$; this means exactly that, if γ_n is the first slope of $\mathfrak{N}(g_n)$, then $\gamma_n > \lambda_n$. In-fact, $\gamma_n \leq \lambda_n$ would imply, by Corollary 5.15.1, the existence of $\alpha \in \mathbb{C}_p$ such that $|\alpha|_p = p^{\gamma_n} \leq p^{\lambda_n}$ such that $g(\alpha) = 0$ and this cannot be the case. From a geometrical point of view, this means that every point $(i, \operatorname{ord}_p b_{n,i})$ lies on or above the line $y = \gamma_n \cdot x$, i.e.

$$\operatorname{ord}_p b_{n,i} \geq i \cdot \gamma_n.$$

We have already proved that $\lim_{n\to+\infty} \lambda_n = +\infty$ so $\lim_{n\to+\infty} \gamma_n = +\infty$ and this implies $\lim_{n\to+\infty} \operatorname{ord}_p b_{n,i} = +\infty$, i.e. $\lim_{n\to+\infty} b_{n,i} = 0$ for every $i \geq 1$. Let's now come back to the relation $h_n(X) = f(X) \cdot g_n(X)$ and let's consider the single coefficients; we obtain

$$\begin{aligned} a_{n,1} &= b_{n,1} + a_1; \\ a_{n,2} &= b_{n,2} + a_1 b_{n,1} + a_2; \\ &\vdots \\ a_{n,m} &= b_{n,m} + \sum_{j=1}^{m-1} a_j b_{n,m-j} + a_m. \end{aligned}$$

Then, for any $m \geq 1$, we have $\lim_{n\to+\infty} a_{n,m} = a_m$. Let's fix $x \in D(1)$ and $\varepsilon > 0$ and consider

$$|f(x) - h_n(x)|_p = \left|\sum_{i=1}^{+\infty} (a_i - a_{n,i}) x^i\right|_p \leq \max\left\{\max_{1\leq i\leq d_n} |a_i - a_{n,i}|_p, \max_{i>d_n} |a_i|_p\right\}$$

where we set $a_{n,i} = 0$ if $i > d_n$. We already know $\lim_{n\to+\infty} d_n = +\infty$ and we know that $\lim_{i\to+\infty} |a_i|_p = 0$ since f converges everywhere (see Proposition 3.7). Let's choose $n \in \mathbb{N}$ such that $i > d_n$ implies $|a_i|_p < \varepsilon$. Now we have only to give an upper bound on the first term, but this is easy thanks to the bounds we proved before:

$$\begin{aligned} |a_i - a_{n,i}|_p = \lim_{m\to+\infty} |a_{m,i} - a_{n,i}|_p &\leq \lim_{m\to+\infty} Mp^{-\lambda_{n+1}} = Mp^{-\lambda_{n+1}} \\ \implies \max_{1\leq i\leq d_n} |a_i - a_{n,i}|_p &\leq M \cdot p^{-\lambda_{n+1}} \end{aligned}$$

and we can assume that $n \in \mathbb{N}$ is big enough such that $M \cdot p^{-\lambda_{n+1}} < \varepsilon$ and $i > d_n$ implies $|a_i|_p < \varepsilon$. Since ε is chosen arbitrarily, we conclude that if $x \in D(1)$ then

$$f(x) = \lim_{n \to +\infty} h_n(x) = \lim_{n \to +\infty} \prod_{j=1}^{d_n} \left(1 - \frac{x}{r_j}\right) = \prod_{j=1}^{+\infty} \left(1 - \frac{x}{r_j}\right).$$

Let's define $\ell(X) := \prod_{j=1}^{+\infty} \left(1 - \frac{X}{r_j}\right)$. It can be proved that $\ell(X) \in 1 + X\mathbb{C}_p[\![X]\!]$ exploiting the fact that $\lim_{n \to +\infty} |1/r_n|_p = 0$ and that its coefficient of X^m is simply the sum of the series of all possible products of m of the $-1/r_i$'s (which converges). Now, $\ell(X)$ converges on $D(1)$ because $\ell(x) = f(x)$ for any $x \in D(1)$. We can conclude that, in $\mathbb{C}_p[\![X]\!]$, we have

$$f(X) = \ell(X) = \prod_{j=1}^{+\infty} \left(1 - \frac{X}{r_j}\right)$$

since $g(X) := f(X) - \ell(X)$ is a power series convergent on $D(1)$ with infinite zeroes and, by Lemma 5.17, it must be $g(X) = 0$. □

This proposition resembles a lot the Weierstrass factorization theorem of complex analysis, although the p-adic result is much more clean: there are no exponential factor in the product. One immediate implication is that any power series which converges everywhere and is never zero must be a constant: here is why we cannot have an exponential similar to the classic one, which converges everywhere, is never zero but isn't constant. Finally we can think as power series which converges everywhere simply as "polynomials with infinite zeroes", which can be factorized in the same exact way we factorize polynomials.

Bibliography

Books

[1] N. Bourbaki. *Topologie Générale*. Paris: Hermann, 1974.

[4] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer, 1977.

[6] Alain M. Robert. *A Course in p-adic Analysis*. New York: Springer, 2000.

Sites

[2] Yuchen Chen. *P-adics, Hensel's lemma and Strassman's theorem*. 2018. URL: https://math.uchicago.edu/~may/REU2018/REUPapers/Chen,Yuchen.pdf.

[3] Brian Conrad. COMPLETION OF ALGEBRAIC CLOSURE. URL: http://math.stanford.edu/~conrad/248APage/handouts/algclosurecomp.pdf.

[5] Gérard P. Michon. *p-adic Arithmetic*. URL: http://numericana.com/answer/p-adic.htm#decimal.

[7] Jack A. Thorne. *p-adic analysis, p-adic arithmetic*. URL: https://www.dpmms.cam.ac.uk/~jat58/all.pdf.