Bachelor Mathematics

Track: Algebra and geometry

Project pure mathematics

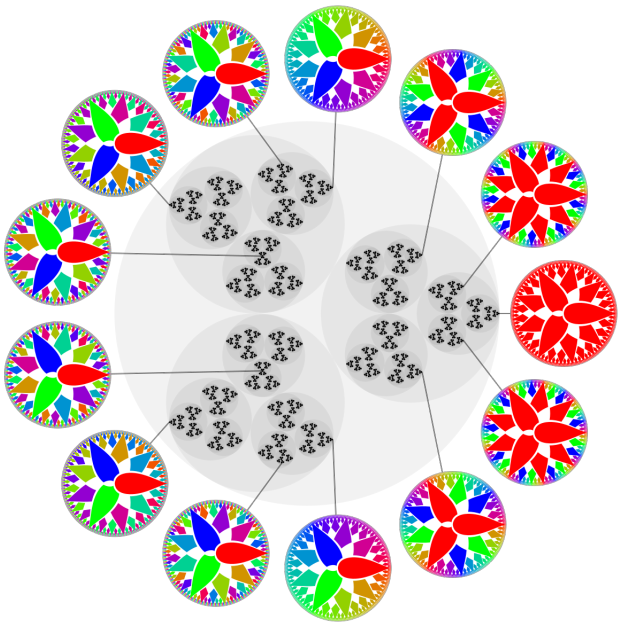
p-adic Numbers

by

Yoav Eshel, Anh Van Giang

June 28, 2021

Supervisor: prof. Rob de Jeu



Department of Mathematics

Faculty of Sciences

VU UNIVERSITY AMSTERDAM

Abstract

The p-adic numbers and p-adic metric are introduced, and various relevant properties are proved. The field $\mathbb{Q}_p$ is then constructed as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value and Hensel's lemma is proved using an iterative method. It is then shown that $\mathbb{Q}_p$ is not algebraically closed and its algebraic closure is $\overline{\mathbb{Q}_p}$ is not complete. The field $\mathbb{C}_p$ is constructed as the completion of the algebraic closure of $\mathbb{Q}_p$ and Newton polygons are discussed as an example of analysis in $\mathbb{C}_p$.

Title: p-Adic Numbers

Authors:
Yoav Eshel, y.eshel@student.vu.nl, 2660535
Anh Van Giang, vangianganh@gmail.com, 2658762
Supervisor: prof. Rob de Jeu

Date: June 28, 2021

Department of Mathematics
Vrije Universiteit Amsterdam
de Boelelaan 1111, 1081 HV Amsterdam
http://www.math.vu.nl/

Contents

Frequently Used Notation

$\mathcal{O}_K$ valuation ring of a field K, page 6

$\overline{K}$ algebraic closure of a field K, page 9

$D(a, r)$ open disk of radius r centered at a, page 4

$K((X))$ field of finite-tailed formal power series with coefficients in K, page 2

$N_{L/K}(\alpha)$ field norm of $\alpha \in L$ over K, page 10

1 Introduction

The p-adic numbers were first discovered[1] by Kurt Hensel in 1897 [1], as a way to introduce the tools and techniques of power series into number theory. Hensel started with the analogy between $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$ and $\mathbb{C}[X]$ together with its field of fractions, $\mathbb{C}(X)$. Both $\mathbb{Z}$ and $\mathbb{C}[X]$ are *unique factorization domains*: any integers factors as ± 1 times the product of primes and any polynomial uniquely factors as a product of prime elements $X - \alpha \in \mathbb{C}[X]$. Furthermore, any polynomial in $\mathbb{C}[X]$ can be expanded in "base" $X - \alpha$ using its Taylor series around α and for any integer $m \in \mathbb{Z}^+$ and prime p we can write

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n, \quad a_i \in \{0, 1, \ldots, p-1\}.$$

There is also a natural expansion for -1, at least in a formal sense, as

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$$

since if we add 1 we get

$$\begin{aligned} 0 &= 1 - 1 \\ &= 1 + (p-1) + (p-1)p + (p-1)p^2 + \cdots \\ &= p^2 + (p-1)p^2 + (p-1)p^3 + \cdots \\ &= 0. \end{aligned}$$

Note that the powers of p are disappearing "to the right". The analogy gets interesting when we start considering rational numbers. We know that every rational function in $\mathbb{C}(X)$ has an finite tailed Laurent series around $\alpha \in \mathbb{C}$ as $P(X)/Q(X) = \sum_{i \geq k} a_i (X - \alpha)^i$. Working formally, we can obtain a similar series for rational numbers. For example, consider $p = 3, a = 22$ and $b = 7$. Then $a = 1 + p + 2p^2, b = 1 + 2p$ and so

$$\frac{a}{b} = \frac{1 + p + 2p^2}{1 + 2p} = 1 - p + 4p^2 - 8p^3 + 16p^4 - 32p^5 + \cdots . \tag{1.1}$$

It is easy to check that the above expansion is correct by multiplying both side by $b = 1 + 2p$.

To make such expansions rigorous, we must define a new metric on $\mathbb{Q}$, such that larger powers of p become increasingly small so that the series such as the one in (1.1) actually converges. This gives us the p-adic metric $|\cdot|_p$ defined in section 2.1. Furthermore, we

[1] or invented, depending on your philosophical preferences

know that every rational function has a Laurent expansion around α, but not every Laurent expansion corresponds to a rational function (for example the Laurent series for e^z). This gives us the inclusion $\mathbb{C}(X) \hookrightarrow \mathbb{C}((X-\alpha))$. The field of all formal power series in p is denoted $\mathbb{Q}_p$ and is defined as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ in section 2.2. After discussing an application of p-adic numbers to solving congruence relations modulo a prime p in section 2.3 we move to the problem of construction a complete and algebraically closed field of p-adic numbers, analogous to the field $\mathbb{C}$ of complex numbers.

Using the standard norm on $\mathbb{Q}$, we can complete it to get the field $\mathbb{R}$ and then take the algebraic closure to end up with $\mathbb{C}$, a complete and algebraically closed field. In the p-adic world, things get a bit more complicated. In chapter 3 we show that $\mathbb{Q}_p$ is not algebraically closed and takes its algebraic closure $\overline{\mathbb{Q}_p}$. However, $\overline{\mathbb{Q}_p}$ is not complete anymore, and so we take its completion again to get $\mathbb{C}_p$. We then prove that the completion of an algebraic closure of a complete field is always algebraically closed. Finally, in chapter 4 Newton polygons are introduced as a way to analyze roots of polynomials and radius of convergence of power series.

2 p-adic Numbers

The expansion of a p-adic integer resembles the decimal expansion of a real number. However, the decimal expansion converges while the p-adic expansion might not. As the field of real numbers is the set of all decimal expansions, we can construct the field $\mathbb{Q}_p$ of all p-adic expansions by replacing the ordinary absolute value with a p-adic one.

2.1 p-adic absolute value

Let $x = a/b \in \mathbb{Q}$ and p prime. Then we can write $x = p^m \frac{a'}{b'}$ with $m \in \mathbb{Z}$ (or $m = \infty$ if $x = 0$) and $\gcd(a'b', p) = 1$. The p-adic absolute value of x is given by $|x|_p = p^{-m}$ and is easily checked to verify the usual properties:

- $|a|_p \geq 0$ and $|a|_p = 0 \iff a = 0$
- $|ab|_p = |a|_p |b|_p$
- $|a + b|_p \leq |a|_p + |b|_p$

for all $a, b \in \mathbb{Q}$.

The number m associated with x is called the p-adic valuation of x and is denoted $v_p(a)$ This gives the map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. We then have

Proposition 2.1. *The map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ satisfies*

1. $v_p(x) = \infty \iff x = 0$
2. $v_p(xy) = v_p(x) + v_p(y)$
3. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

Proof. The first two properties are readily verified. For the third, if $x + y = 0$ then $v_p(x + y) = \infty$ and the proof is trivial. So take $x, y \in \mathbb{Q}$ with $x + y \neq 0$ and without loss of generality, assume that $v_p(x) \leq v_p(y)$. Let $x = a/b$ and $y = c/d$. It is clear from the definition that $v_p(x) = v_p(a) - v_p(b)$ and so we have

$$v_p(x) \leq v_p(y) \implies v_p(ad) \leq v_p(bc).$$

Let $v_p(ad) = m$ and $v_p(bc) = n$. Then $ad + bc = p^m k_1 + p^n k_2$ with $k_1, k_2 \in \mathbb{Z}$ and since $m \leq n$ it follows that $p^m \mid ad + bc$. Thus $v_p(ad + bc) \geq v_p(ad)$ and so

$$v_p(x + y) = v_p\left(\frac{ad + bc}{bd}\right) = v_p(ad + bc) - v_p(bd) \geq v_p(a) - v_p(b) = v_p(x).$$

□

From proposition 2.1 it follows that for $x, y \in \mathbb{Q}$ nonzero with $v_p(x) \leq v_p(y)$ and $x + y \neq 0$ we have

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

and so $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. By defining $p^{-\infty} = 0$, the result extends to all of $\mathbb{Q}$. Notice that this property is stronger than the usual triangle inequality, and so the p-adic absolute value is *non-Archimedean* as opposed to the ordinary absolute value on $\mathbb{Q}$. As one may expect, this property is quite unintuitive. For example, every point a_2 in an open disk $D(a_1, r) = \{x \in \mathbb{Q} \mid |x - a_1|_p < r\}$ is its center. That is becuase for any $x \in D(a_1, r)$ we have

$$|x - a_2|_p = |(x - a_1) + (a_1 - a_2)|_p \leq \max\{|x - a_1|_p, |a_1 - a_2|_p\} \leq r$$

so $x \in D(a_2, r)$. We can similarly show that $x \in D(a_2, r)$ implies that $x \in D(a_1, r)$ and so $D(a_1, r) = D(a_2, r)$.

2.2 The field $\mathbb{Q}_p$

From real analysis, we know that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with repspect to a standard absolute value, i.e. $\mathbb{R}$ is a complete field, the absolute value in $\mathbb{R}$ is induced by the absolute value on $\mathbb{Q}$ and $\mathbb{Q}$ is dense in $\mathbb{R}$. In this section we construct the field $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with repspect to $|\cdot|_p$ in a similar manner. First recall that

Definition 2.2. A field K with an absolute value $|\cdot|$ is complete if every Cauchy sequence in K has a limit in K.

Due to Ostrowski, we know that there countably many non-equivalent[1] absolute values on $\mathbb{Q}$. Namely, the trivial absolute value which maps all non-zero elements to one, the ordinary absolute value and the p-adic absolute value(s) [1, p. 46]. As it turns out, $\mathbb{Q}$ is not complete with respect to any of its non-trivial absolute values. It is easy to show that $\mathbb{Q}$ is not compelte with repspect to the ordinary absolute value: consider the sequence given by $x_1 = 2$ and $x_n = \frac{1}{2}x_n + \frac{1}{x_n}$ which converges to $\sqrt{2} \notin \mathbb{Q}$. To show that $\mathbb{Q}$ is not complete with respect to the p-adic absolute value requires some more work. The following theorem is one of the many nice properties of non-Archimedean absolute values which will be used in showing that $\mathbb{Q}$ is not complete.

Theorem 2.3. *Let F be a field with a non-Archimedean norm $|\cdot|$ and $\langle x_n \rangle$ a sequence in F. Then $\langle x_n \rangle$ is a Cauchy sequence if and only if* $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.

Proof. The first implication is immidiate. Suppose that $\langle x_n \rangle$ is a sequence such that $|x_{n+1} - x_n| \to 0$. Let $k > 0$ and $m = n + k$ then we have

$$\begin{aligned} |x_m - x_n| &= |x_{n+k} - x_{n+k-1} + x_{n+k-1} + ... - x_n| \\ &\leq \max(|x_{n+k} - x_{n+k-1}|, |x_{n+k-1} - x_{n+k-2}|, ..., |x_{n+1} - x_n|) \\ &\leq |x_{n+h} - x_{n+h-1}|, \quad \text{for some } h \in \{1, 2, ..., k\}. \end{aligned}$$

[1] A more rigorous discussion what it means for two absolute values to be equivalent is found in Chapter 3. For now, an intuitive understanding of "equivalent" will suffice.

As the last expression goes to 0 by assumption, $\langle x_n \rangle$ is Cauchy. $\square$

We can now prove that the field $\mathbb{Q}$ is not complete with respect to the p-adic absolute value.

Theorem 2.4. *The field $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$.*

Proof. If $p \in \{2, 3\}$, the proof is more complicated and requires Hensel's lemma. A sketch of the proof is given in the end of section 2.3.

Suppose $p > 3$. Let $1 < a < p - 1$ and define the sequence $x_n = a^{p^n}$. Then

$$|x_{n+1} - x_n|_p = \left|a^{p^n}\left(a^{(p-1)p^n} - 1\right)\right|_p \leq p^{-n}$$

where the last inequality follows from Euler's theorem as $a^{(p-1)p^n} = a^{\phi(p^n)} \equiv 1 \mod p^n$. Thus $\langle x_n \rangle$ is a Cauchy sequence. Suppose that $x_n \to x \in \mathbb{Q}$. Since the roots of $X^p - X$ are the $\frac{p-1}{2}$th primitive roots of unity, ± 1 and 0, it follows that $x = 0, \pm 1$. As $p \nmid a^{p^n}$ for all n, $|x_n|_p = 1$ for all n, and so $|x|_p = \lim_{n\to\infty} |x_n|_p = 1$. Thus $x \neq 0$. If $x = \pm 1$, then $0 < x - a < p$ and so $|x - a|_p = 1$. Thus there exists $n \in \mathbb{N}$ such that $\left|a^{p^n} - x\right|_p < |x - a|_p$. It is easy to check that $|x - a|_p \leq \max\{\left|x - a^{p^n}\right|_p, \left|a^{p^n} - a\right|_p\}$ implies that $|x - a|_p = \left|a^{p^n} - a\right|_p$. But $\left|a^{p^n} - a\right|_p = \left|a^{p^{n-1}} - 1\right|_p$ and by Fermat's little theorem we have $a^{p^{n-1}} - 1 \equiv 0 \mod p$ so $|x - a|_p < 1$, contradicting our previous assertion. Thus $x \notin \mathbb{Q}$ and it follows that $\mathbb{Q}_p$ is not complete with respect to the p-adic norm for all primes p. $\square$

We now know that $\mathbb{Q}$ is not complete, but it is unclear how to obtain a complete extension of $\mathbb{Q}$, and in particular, how does the p-adic absolute value extends. It turns out that one can mimic the Cauchy construction of $\mathbb{R}$ by letting $\mathbb{Q}_p$ be the set of equivalence classes of Cauchy sequences in $\mathbb{Q}$ with respect to the p-adic norm. The proof is adapted from [2, p. 468].

Theorem 2.5. *Let K be a field with an absolute value $|\cdot|$. Then there exists a field K' with an absolute value $|\cdot|'$ and an embedding $i : K \to K'$ such that $|i(x)|' = |x|$ for $x \in K$ and the image of K is dense in K'. The field K' is unique up to isomorphism. Moreover, if $|\cdot|$ is non-Archimedean, then $|\cdot|'$ is non-Archimedean.*

Proof. The set R of Cauchy sequences in K forms a ring, with addition and multiplication defined componentwise. We call a sequence $\langle x_n \rangle$ a *null sequence*, if $x_n \to 0$. As any Cauchy sequence that is not null, will stay away from 0 for sufficiently large n, we can then take the inverse of almost all the terms. For finitely many of them, we again obtain a Cauchy sequence. Thus the set of all null-sequences M forms a maximal ideal in R.

We then define K' as R/M and the embedding i is the map sending $x \in K$ to the class of constant Cauchy sequences $(x, x, \dots)$. The absolute value $|\cdot|'$ is defined by continuity, i.e. for an element $\alpha \in K'$ representing a sequence $\langle x_n \rangle$ we have $|\alpha|' = \lim_{n\to\infty} |x_n|$. This limit exists since $||x_n| - |x_m|| \leq |x_n - x_m|$ implies that $|x_n|$ is a Cauchy sequence

in $\mathbb{R}$. It is immediate that $|\cdot|'$ has the usual properties independently of the choice of x_n and that $|i(x)|' = |x|$ for all $x \in K$. If $|\cdot|$ is non-Archimedean, then for $\alpha, \beta \in K'$ representing the sequences $\langle x_n \rangle, \langle y_n \rangle$ (respectively) in K, we have

$$|\alpha + \beta|'_p = \lim |x_n + y_n| \leq \lim \max\{|x_n|, |y_n|\} = \max\{|\alpha|', |\beta|'\}.$$

To show that K' is complete, let α_n be a Cauchy sequence in K'. Then there exist $x_n \in K$ such that $|\alpha_n - i(x_n)|' < \frac{1}{n}$. The sequence x_n forms a Cauchy sequence in K with a limit $\alpha \in K'$. As

$$|\alpha_n - \alpha|' \leq |\alpha_n - i(x_n)|' + |i(x_n) - \alpha|'$$

it follows that $\alpha_n \to \alpha$ and so K' is complete.

For any $\alpha \in K'$ represented by a sequence $\langle x_n \rangle$ in K, there exists an x_N for $N \in \mathbb{N}$ so that $i(x_N)$ is arbitrarily close to α and so $i(K)$ is dense in K'. Finally, uniqueness is immediate, since for any complete field $\hat{K}$ that contains K as a dense subfield, we can map limits in $\hat{K}$ of Cauchy sequences in K to their representatives in K'. □

Thus the extension $\mathbb{Q}_p/\mathbb{Q}$ exists and is unique, and there is a well defined absolute value on $\mathbb{Q}_p$ which is induced by the p-adic absolute value on $\mathbb{Q}$. As a result, we will denote the absolute value on $\mathbb{Q}_p$ as $|\cdot|_p$ as well.

Let K be a complete field w.r.t. a non-Archimedean absolute value $|\cdot|$. Let $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$. It is immediate from the properties of non-Archimedean absolute values that $\mathcal{O}_K$ is a ring. We calle this the valuation ring of K. Similarly, it can be found that $M = \{x \in K \mid |x| < 1\}$ is an ideal of $\mathcal{O}_K$. To show that M is the unique maximal ideal of $\mathcal{O}_K$, take $\alpha \in \mathcal{O}_K \setminus M$. Then $|\alpha| = 1$ so $|\alpha^{-1}| = 1$ and it follows that any ideal containing α must be the whole ring. If K is complete and $\langle x_n \rangle$ is a Cauchy sequence in $\mathcal{O}_K$ with limit $x \in K$, then $|x_n|$ is a Cauchy sequence in $[0, 1]$ and so $x \in \mathcal{O}_K$. We summarize our results in the following proposition.

Proposition 2.6. *Let K be field with a non-Archimedean absolute value $|\cdot|$. The subset $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ is a ring with a unique maximal ideal $M = \{x \in K \mid |x| < 1\}$. If K is complete, then $\mathcal{O}_K$ is complete.*

The valuation ring of $\mathbb{Q}_p$ is called the p-adic integers and denoted by $\mathbb{Z}_p$.

2.3 Hensel's Lemma

At this point, the only understanding we have of p-adic numbers is that their are limits of Cauchy sequences in $\mathbb{Q}$. Recall that we can write any rational number as a p-adic expansion, but not every p-adic expansion corresponds to a rational number. This is analogous to the inclusion $\mathbb{C}(X) \hookrightarrow C((X - \alpha))$ of the field of rational functions to the field of finite-tailed Laurent series in $(X - \alpha)$. Let K denote the field of all elements of the form $\sum_{i \geq k} a_i p^i, a_i \in \{0, 1, \ldots, p-1\}$ where $k \in \mathbb{Z}$ and $a_k \neq 0$. It is clear that for any $\alpha \in K$, $\alpha \in \mathbb{Q}_p$ since the partial sums form a Cauchy sequence in $\mathbb{Q}$ and that for

$\alpha \in K$, $|\alpha|_p = p^{-k}$. If $\alpha_n = \sum_{i \geq k_n} a_i^{(n)} p^i$ forms a Cauchy sequence in K, then the partial sums $x_n = \sum_{i=k_n}^{n-1} a_i^{(n)} p^i$ form a Cauchy sequence in $\mathbb{Q}$ with a limit $\alpha \in \mathbb{Q}_p$. Then

$$|\alpha_n - \alpha|_p \leq \max\{|\alpha_n - x_n|_p, |x_n - \alpha|_p\} = \max\{p^{-n}, |x_n - \alpha|\}.$$

Thus K is complete and so

Proposition 2.7. *For every $\alpha \in \mathbb{Q}_p$ there exists $k \in \mathbb{Z}$ such that*

$$\alpha = \sum_{i \geq k} a_i p^i, \quad a_i \in \{0, 1, \ldots, p-1\}, a_k \neq 0$$

and $v_p(\alpha) = k$. Conversely, for every $k \in \mathbb{Z}$ there exists $\alpha \in \mathbb{Q}_p$ with $v_p(\alpha) = k$.

We are now ready to prove Hensel's lemma, which is one of the most important theorems of p-adic numbers. Using Hensel's lemma, we can, in many cases, quite easily determine whether a polynomial has a roots in $\mathbb{Z}_p$. There are in fact many forms of Hensel's lemma, and we give here the proof of only one, together with a more general statement which we will not prove here. The idea is that in $\mathbb{R}$, we can sometime decide on the existence of roots by looking at the sign of a polynomial. For example, since $x^2 + 1 > 1$ for all $x \in \mathbb{R}$, $\mathbb{R}$ is not algebraically closed. In the p-adic world, this translates to reduction $\mod p$. The following proof is adapted from [1, p. 89].

Theorem 2.8. *Let $P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdot + a_0$ be a polynomial with coefficients in $\mathbb{Z}_p$. Suppose that there exists $\alpha_1 \in \mathbb{Z}_p$ such that $P(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p$ and $P'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p$ where P' is the formal derivative of P. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p$ and $P(\alpha) = 0$.*

Proof. We construct a unique Cauchy sequence $\langle \alpha_n \rangle$ in $\mathbb{Z}_p$ such that for all $n \geq 1$: (a) $P(\alpha_n) \equiv 0 \mod p^n$ and (b) $\alpha_n \equiv \alpha_{n-1} \mod p^n$.

We assume that α_1 exists. To find α_2, note that by condition (b) it must be of the form $\alpha_2 = \alpha_1 + b_1 p$, for $b_1 \in \mathbb{Z}_p$. Using the Taylor expansion of $P(X)$ around α_1 we obtain

$$\begin{aligned} P(\alpha_2) &= P(\alpha_1 + b_1 p) \\ &= P(\alpha_1) + P'(\alpha_1) b_1 p + \text{terms divisible by } p^2 \\ &\equiv P(\alpha_1) + P'(\alpha_1) b_1 p \mod p^2. \end{aligned}$$

Thus we need b_1 such that $P(\alpha_1) + P'(\alpha_1) b_1 p \equiv 0 \mod p^2$. From $P(\alpha_1) \equiv 0 \mod p$ it follows that $P(\alpha_1) = px$ for some $x \in \mathbb{Z}_p$ and so $x + P'(\alpha_1) b \equiv 0 \mod p$. As $P'(\alpha_1)$ is not divisible by p, it is invertible in $\mathbb{Z}_p$ and so $b_1 \equiv -x \left(P'(\alpha_1)\right)^{-1} \mod p$. Such b_1 exists in $\{0, 1, \ldots, p-1\}$, and for such b_1 we can set $\alpha_2 = \alpha_1 + b_1 p$ satisfying both conditions.

Exactly the same procedure can be taken to obtain α_{n+1} from α_n (and choosing b_n in $\{0, 1, \ldots, p^n - 1\}$) and so our sequence exists. As $\alpha_{n+1} - \alpha_n \equiv 0 \mod p^n$ it follows that $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$ and so $\langle \alpha_n \rangle$ is Cauchy and it has a limit $\alpha \in \mathbb{Z}_p$. Moreover, we have $P(\alpha) = 0$ by continuity and so the proof is complete. $\square$

We will need a more general version of Hensel's Lemma to prove that $|\cdot|_p$ extends uniquely to algebraic extensions of $\mathbb{Q}_p$, and so we note it here. The proof can be found in [3, p. 129]

Lemma 2.9. *Let K be a field with equipped with a non-Archimedean absolute value $|\cdot|$, a valuation ring $\mathcal{O}_K$ and it maximal ideal M. If a primitive polynomial $f \in \mathcal{O}_K[X]$ admits modulo M factorization $f = \bar{g}\bar{h} \mod M$ into relatively prime polynomials $\bar{g}, \bar{h} \in \mathcal{O}/M[X]$, then f admits a factorization $f = gh$ into polynomials $g, h \in \mathcal{O}_K[X]$ such that $\deg g = \deg \bar{g}$, $g \equiv \bar{g} \mod M$ and $h \equiv \bar{h} \mod M$*

One may see that the proof technique used is quite similar to Newton's method for find real root of a polynomial. We find α_{n+1} by solving $b_n = -x\left(P'(\alpha_n)\right)^{-1}$ so putting it all together we get

$$\alpha_{n+1} = \alpha_n - p\frac{P(\alpha_n)}{p}\left(P'(\alpha_n)\right)^{-1} = \alpha_n - \frac{P(\alpha_n)}{P'(\alpha_n)}.$$

Example 2.10. We show that the "square root" of 2^2 is in $\mathbb{Z}_7$. Let $f(X) = X^2 - 2$. Then modulo 7, 3 and 4 are roots so let $\alpha_1 = 3$. Then $f(\alpha_1) = 7$ and $f'(\alpha_1) = 6$. As $6^{-1} \equiv 41 \mod 7^2$, we have

$$\alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_2)} = \frac{11}{6} \equiv 10 \mod 7^2.$$

So $\alpha_2 = 10 = 3{+}1{\cdot}7$ Continuing in the same manner we find that $\alpha_3 = 108 = 3{+}1{\cdot}7{+}2{\cdot}7^2$ and so on. Thus the square root of 2 in $\mathbb{Z}_7$ has an initial expansion $3{+}1{\cdot}7{+}2{\cdot}7^2{+}6{\cdot}7^3{+}\cdots$.

Another application of Hensel's lemma is proving that $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$ when $p = 2, 3$. The polynomial $X^3 + 3$ is irreducible over $\mathbb{Q}[X]$ but it has a root modulo 2. Thus by Hensel's lemma it has a root in $\mathbb{Z}_p$ and it follows that $\mathbb{Q}$ is a proper subset of $\mathbb{Q}_2$ so $\mathbb{Q}$ cannot be complete. A similar argument using the polynomial $X^2 + 2$ when $p = 3$ does the trick.

[2]Meaning, a root of $X^2 - 2 \in \mathbb{Z}_p[X]$

3 Complete and Algebraically Closed Extension of $\mathbb{Q}_p$

The aim of the following chapter is to construct the field $\mathbb{C}_p$, a complete and algebraically closed extension of $\mathbb{Q}_p$. This field takes the role of the complex numbers $\mathbb{C}$ in the p-adic world. We start by proving that $\mathbb{Q}_p$ is not algebraically closed by showing that $\sqrt{p} \notin \mathbb{Q}_p$.

Proposition 3.1. *The field $\mathbb{Q}_p$ is not algebraically closed.*

Proof. Suppose there exists $x \in \mathbb{Q}_p$ such that $x^2 = p$. Then $2v_p(x) = v_p(x^2) = v_p(p) = 1$. As the p-adic valuation on $\mathbb{Q}_p^\times$ is always an integer, we have a contradiction. Thus $x \notin \mathbb{Q}_p$ and so $\mathbb{Q}_p$ is not algebraically closed. □

Before we can move on to the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$, we need to show that the p-adic value can, in fact, be extended to $\overline{\mathbb{Q}_p}$,

3.1 Extensions of absolute values

Let K be a complete field equipped with an absolute value $|\cdot|$. Before proving that $|\cdot|$ can be uniquely extended to algebraic extensions of K, we define what it means for two absolute values to be equivalent.

Definition 3.2. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K are called equivalent if they define the same topology on K.

An alternative and more useful definition is given by the following proposition, the proof of which is due to [3, p. 117].

Proposition 3.3. *Two non-trivial absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K are equivalent if and only if*

$$|\alpha|_1 < 1 \implies |\alpha|_2 < 1$$

for $\alpha \in K$.

Proof. Suppose the two absolute values are equivalent. For $x \in K$ we have $|x|_1 < 1$ if and only if $x^n \to 0$ as $n \to \infty$. As $|\cdot|_1$ and $|\cdot|_2$ define the same topology on K, it follows that $|x|_2 < 1$ as well.

Conversely, suppose that $|x|_1 < 1 \implies |x|_2 < 1$. As both absolute values are non trivial, there exists $x_0 \in K$ such that $|x_0|_1 > 1$. Then $|x_0|_2 > 1$ since $\left|x_0^{-1}\right|_1 < 1$. Let $a = |x_0|_1$, $b = |x_0|_2$ and $\lambda = \log a / \log b$. Take $x \in K$ with $x \neq 0$. Then there

exists $\alpha \in \mathbb{R}$ such that $|x|_1 = |x_0|^\alpha$. Let $m, n \in \mathbb{Z}$, $n > 0$ such that $\alpha < \frac{m}{n}$. Then $|x|_1 = |x_0|^\alpha < |x_0|_1^{m/n}$ and so $|x^n/x_0^m|_1 < 1$. Thus $|x^n/x_0^m|_2 < 1$ and it follows that $|x|_2 < |x_0|_2^{m/n}$. As $\frac{m}{n}$ can get arbitrarily close to α, it follows that $|x|_2 \leq |x_0|_2^\alpha$. By taking $\frac{m}{n} < \alpha$ we obtain that $|x_0|_2^\alpha \leq |x|_2$ and so $|x|_2 = |x_0|_2^\alpha$. Hence

$$|x|_2^\lambda = |x_0|_2^{\alpha\lambda} = \left(b^\lambda\right)^\alpha = a^\alpha = |x_0|_1^\alpha = |x|_1$$

and it follows that the two absolute values are equivalent. □

Corollary 3.3.1. *If*

$$|x|_1 \leq 1 \implies |x|_2 \leq 1, \quad \forall x \in K$$

then $|\cdot|_1$ *and* $|\cdot|_2$ *are equivalent.*

Proof. Assume for contradiction that the two absolute values are not equivalent. Then there exists $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_2 \geq 1$. Similarly, there exists $\beta \in K$ such that $|\beta|_1 \geq 1$ and $|\beta|_2 < 1$. Set $y = \frac{\alpha}{\beta}$, so $|y|_1 < 1$ and $|y|_2 \geq 1$. Then the sequence $x_n = \frac{y^n}{1+y^n}$ converges to 0 with respect to $|\cdot|_1$ and to 1 with respect to $|\cdot|_2$. Then for $0 < \varepsilon < 1$ there exists an $n \in \mathbb{N}$ such that $|x_n + \varepsilon|_1 \leq 1$ and $|x_n + \varepsilon|_2 > 1$. □

From the properties of non-Archimedean absolute value, it immediately follow that the set of all element $x \in K$ such that $|x| \leq 1$ forms a subring of K. It is called the valuation ring of K and denoted by $\mathcal{O}_K$.

The last definition we will need is that of an integral closure of a ring.

Definition 3.4. Let A be a subring of of B. The integral closure of A is in B is the set of all $b \in B$ such that b is a root of a monic polynomial in $A[X]$.

The integral closure of A forms a subring of B, which we will not prove here. For a proof, the reader is referred to [2, p. 336].

We are now ready to prove that absolute values extend uniquely to extensions of K. The following proof is given by [3, p. 131].

Theorem 3.5. *Let K be a complete field with respect to the non-Archimedean absolute value $|\cdot|$ and let L/K be algebraic. Then the absolute value on K extends uniquely to L. If $[L : K] = n < \infty$, then the extension is given by*

$$|\alpha| = \sqrt[n]{\left|N_{L/K}(\alpha)\right|}, \quad \alpha \in L.$$

The notation $N_{L/K}(\alpha)$ denotes the *field norm* of $\alpha \in L$ over K. The reader is referred to [2, p. 284] for the definition and properties.

Proof. We start by considering a finite extension $[L : K] = n$.

Existence: let $\alpha \in L$. It is immediate that $|\alpha| \geq 0, \forall \alpha \in L$. As the field norm is a field homomorphism, it follows that $|\alpha| = 0 \iff \alpha = 0$. As the norm is multiplicative, for $\alpha, \beta \in L$ we have $|\alpha\beta| = |\alpha||\beta|$.

Lastly, we want to show that for $\alpha, \beta \in L$ we have

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

By dividing by $\max\{|\alpha|, |\beta|\}$ and renaming if necessary, we find the it is equivalent to $|\alpha| \leq 1 \implies |\alpha + 1| \leq 1$. To prove that the latter holds, we show that the set of all $\alpha \in L$ such that $|\alpha| \leq 1$ forms a ring. Let

$$\begin{aligned}\mathcal{O} &= \{\alpha \in L \mid |\alpha| \leq 1\} \\ &= \{\alpha \in L \mid \left|N_{L/K}(\alpha)\right| \leq 1\} \\ &= \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}_K\}.\end{aligned}$$

We claim that $\mathcal{O}$ is the integral closure of $\mathcal{O}_K$. Suppose $\alpha \in L$ is integral over $\mathcal{O}_K$. Then conjugates $\sigma(\alpha)$ of α are also integral over $\mathcal{O}_K$ by Galois theory, and so the coefficients of f_K^α are in $\mathcal{O}_k$. Thus

$$N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}(\alpha)\right)^{[L:K(\alpha)]} = (\pm a_0)^{[L:K(\alpha)]} \in \mathcal{O}_K,$$

so $\alpha \in \mathcal{O}$. Conversely, suppose that $\alpha \in L^\times$ and $N_{L/K}(\alpha) \in \mathcal{O}_K$. Let $f = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of α. Then $(\pm a_0)^{[L:K(\alpha)]} = N_{L/K}(\alpha) \in \mathcal{O}_K$ so $|a_0| \leq 1 \implies a_0 \in \mathcal{O}_K$. Let a_r be the first coefficient amongst $a_0, a_1, \ldots, a_n = 1$ such that $|a_r| = \max\{|a_0|, \ldots, |a_{d-1}|, |1|\}$. Then

$$a_r^{-1} f \equiv x^r \left(\frac{1}{a_r} x^{d-r} + \frac{a_{d-1}}{a_r} x^{d-1-r} \cdots + 1\right) \mod M,$$

where M is the maximal ideal of $\mathcal{O}_K$. If $\max\{|a_0/a_r|, |1/a_r|\} < 1$, then $|a_r| > 1 \implies 0 < r < d$ which contradicts Lemma 2.9. Thus $|a_i| \leq 1$ for all $i = 0, \ldots, d$ and so $f \in \mathcal{O}_K[X]$. Hence $\mathcal{O}$ is the integral closure of $\mathcal{O}_K$ and from

$$|\alpha| \leq 1 \iff |\alpha|^{\frac{1}{n}} \leq 1, \forall n \in \mathbb{N}$$

it follows that $\mathcal{O}$ is the valuation ring of L. Hence $\alpha \in \mathcal{O} \implies \alpha + 1 \in \mathcal{O}$.

Uniqueness: suppose $|\cdot|'$ is another absolute value on L such that $|x|' = |x|$ for all $x \in K$. Let $\mathcal{O}$ and $\mathcal{O}'$ be the valuation rings of $|\cdot|$ and $|\cdot|'$ respectively. Let M and M' be the maximal ideals of $\mathcal{O}$ and $\mathcal{O}'$ respectively. Take $\alpha \in \mathcal{O} \setminus \mathcal{O}'$ (assuming it's nonempty) and let

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathcal{O}_K[X]$$

be its minimal polynomial (we can take $f \in \mathcal{O}_K[X]$ since $\mathcal{O}$ is the integral closure of $\mathcal{O}_K$). Since $\alpha \notin \mathcal{O}'$, it follows that $\alpha^{-1} \in \mathcal{O}'$. But if $|\alpha^{-1}|' = 1$ then $|\alpha|' = 1$ and $\alpha \in \mathcal{O}'$. Therefore $\alpha^{-1} \in M'$. Hence

$$1 = -a_{d-1}\alpha^{-1} - \cdots - a_0\alpha^{-d} \in M'$$

which is impossible. Therefore $\mathcal{O} \subset \mathcal{O}'$, i.e. $|\alpha| \leq 1 \implies |\alpha|' \leq 1$ and by Corollary 3.3.1 the two absolute values are equivalent. Since they agree on $K \subset L$, they are equal.

Finally, since every algebraic extension is union of finite extensions, it follows that the absolute value extends uniquely to arbitrary algebraic extensions. □

Corollary 3.5.1. *The p-adic absolute value extends uniquely to $\overline{\mathbb{Q}_p}$, the algebraic closure of $\mathbb{Q}_p$.*

Proof. This is immediate from the last statement of the preceding theorem. □

3.2 $\overline{\mathbb{Q}_p}$ is closed but not complete

A standard approach to show that $\overline{\mathbb{Q}_p}$ is not complete is to construct a Cauchy sequence that does not converge in $\overline{\mathbb{Q}_p}$. This approach can be found, for example, in [1, p. 219]. However, it requires some algebraic tools that have not been developed here and so we take a different and more general approach and show that a algebraic closure of countable degree over a complete field is never complete. This is done by introducing the notion of a Baire space, and proving that such a space cannot be a Baire space.

Definition 3.6. A Baire space is a topological space in which the union of countably many closed sets with empty interior has an empty interior as well.

The following lemma, which is a weaker version of *Baire category theorem*, is adapted from [4, p. 296].

Lemma 3.7. *Every complete metric space is a Baire space.*

Proof. Let X be a complete metric space and $\{A_n\}_{n\in\mathbb{N}}$ a set of closed sets in X with empty interiors. Let U_0 be a non-empty, open subset of X. Since A_1 has an empty interior, there is a point $x_1 \in U_0$ such that $x_1 \notin A_1$. As A_1 is closed and X is Hausdorff, there is a neighborhood U_1 of x_1 with diameter less than 1 such that its closure does not intersect A_1 and $\bar{U}_1 \subset U_0$. For each n, given an open set U_{n-1}, choose a point $x_n \in U_{n-1}$ that is not in A_n, and let U_n be a neighborhood of x_n such that: (a) $\bar{U}_n \cap A_n = \varnothing$, (b) $\bar{U}_n \cap U_{n-1}$ and (c) diam $U_n < \frac{1}{n}$. We claim that $\bigcap \bar{U}_n$ is nonempty. Indeed, the sequence $\langle x_n \rangle$ is a Cauchy sequence in X and so $x = \lim_{n\to\infty} x_n \in \bigcap \bar{U}_n$. Then $x \in U_0$ as $\bar{U}_1 \subset U_0$ and since $U_n \cap A_n = \varnothing$, $x \notin A_n$ for all n. Thus any open set $U_0 \subset X$, intersects the set $V = \bigcap A_n^c$ and so V is dense in X. Therefore $\operatorname{Int} \bigcup A_n = \operatorname{Int}(X \setminus \bigcap A_n^c) = \varnothing$. □

As any algebraic extension L/K of countable degree is a countable union of finite extension, if we can show that this finite extensions are closed in $\overline{K}$ and have an empty interior, it would follow that $\overline{K}$ is not complete. By viewing a field extension as a vector space over the base field, we can easily prove both statements. We first define the notion of a normed vector space. F

Let K be a field with a non-trivial absolute value $|\cdot|$ and E a K-vector space. A norm on E is a function which satisfies the same properties as an absolute value and induces the absolute value on K. If E is a finite K-vector space it turns out that any norm on E that induce the absolute value on K is equivalent to the maximum norm [2, p. 470]. Thus, we say that E is a normed vector space over K.

Lemma 3.8. *Let V be a normed vector space over a complete field K, and S a finite-dimensional subspace of V. Then S is closed.*

Proof. Let x be in the closure of S and $\langle s_i \rangle$ a sequence in S that converges to x. Let $\{e_1, \ldots, e_n\}$ be a basis of S and let the norm on S be the maximum norm. Then $s_i = \sum_{k=1}^{n} a_k^{(i)} e_k$ for $a_k^{(i)} \in K$ and since

$$\|s_i - s_j\| = \left\| \sum_{k=1}^{n} \left(a_k^{(i)} - a_k^{(j)} \right) e_k \right\| = \max_{1 \leq k \leq n} \left\{ \left| a_k^{(i)} - a_k^{(j)} \right| \right\}$$

goes to 0, it follows that $\left\langle a_k^{(i)} \right\rangle_{i \in \mathbb{N}}$ is a Cauchy sequence in K, and it has a limit $a_k \in K$. Let $s = \sum_{k=1}^{n} a_k e_k$. As

$$\|s - s_i\| = \left\| \sum_{k=1}^{n} \left(a_k - a_k^{(i)} \right) e_k \right\|$$

goes to 0, it follows that $x = s \in S$ and so S is closed. □

Lemma 3.9. *Let V be a normed vector space and S a proper subspace. Then S has an empty interior.*

Proof. Suppose S contains some ball $B(x, r) = \{y \in V \mid \|x - y\| < r\}$ and take $z \in V$. Then $y = x + \frac{r}{2\|z\|} z \in B(x, r) \subset S$ and since S is a subspace, $z = \frac{2\|z\|}{r}(y - x) \in S$, so $S = V$. □

Theorem 3.10. *Let K be a complete field with respect to a absolute value $|\cdot|$ and L/K a countably infinite extension. Then L is not complete with respect to the extension of $|\cdot|$.*

Proof. Let $\{e_n\}_{n \in \mathbb{N}}$ be a basis for L/K and $X_n = \text{span}\,\{e_1, \ldots, e_n\}$. Then X_n is closed by Lemma 3.8 and has an empty interior by Lemma 3.9. Since $L = \bigcup_{n \in \mathbb{N}} X_n$, L is not complete by Lemma 3.7. □

It can be shown that for a given $n \in \mathbb{N}$, there are only finitely many $K \subset \overline{\mathbb{Q}_p}$ such that $[K : \mathbb{Q}_p] \leq n$. The proof of which can be found in [5, p. 54]. It follows that the degree of $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ is countable, and so

Corollary 3.10.1. *$\overline{\mathbb{Q}_p}$ is not complete.*

3.3 $\mathbb{C}_p$ is complete and algebraically closed

By Theorem 2.5, there exists a unique (up to isomorphism) field extension $\mathbb{C}_p$ of $\overline{\mathbb{Q}_p}$ that is complete with respect to the extension of $|\cdot|_p$.

Definition 3.11. The field $\mathbb{C}_p$ is the unique completion of $\overline{\mathbb{Q}_p}$ with respect the p-adic absolute value.

To prove that $\mathbb{C}_p$ is also algebraically closed, we need to prove that every polynomial in $\mathbb{C}_p$, splits in $\mathbb{C}_p$. It follows from the following theorem that completions of algebraic closures of complete fields are always algebraically closed.

Theorem 3.12. *Let K be a complete field with a non-archimdean and non-trivial absolute value $|\cdot|$. Then the completion L of $\overline{K}$ is algebraically closed.*

Proof. The field L exist and is unique up to isomorphism by Theorem 2.5. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L[X]$, $n > 0$. Since any $x \in L$ is a limit of a Cauchy sequence in $\overline{K}$, it follows that $\overline{K}$ is dense in L. Thus there exist $f_j = X^n + a_{n-1}^{(j)}X^{n-1} + \cdots + a_0^{(j)} \in \overline{K}[X]$ such that $\lim_{j\to\infty} a_i^{(j)} = a_i$. If $a_i \neq 0$ we can choose the sequence $a_i^{(j)}$ such that $|a_i^{(j)} - a_i| < \min\{|a_i|, 1/j\}$ for all j. If $a_i = 0$ then we may take $a_i^{(j)} = 0$. Thus we have $|a_i^{(j)}| = |a_i|$ and $|a_i^{(j)} - a_i| < \frac{1}{j}$ for all j. As $\overline{K}$ is algebraically closed, for each j there is a root r_j of f_j in $\overline{K}$. We want to find a convergent subsequence of $\langle r_j \rangle_j$ so it has a limit $r \in L$ with $f(r) = 0$.

As $f_j(r_j) = 0$ $\forall j$, we have

$$|r_j{}^{\backprime n}| = \left| -\sum_{i=0}^{n-1} a_i^{(j)} r_j^i \right| \leq \max_{0\leq i\leq n-1} \left| a_i^{(j)} \right| |r_j|^i = \max_{0\leq i\leq n-1} |a_i||r_j|^i$$

since $\left|a_i^{(j)}\right| = |a_i|$. Thus, there exists $0 \leq k \leq n-1$ such that $|r_j|^n \leq |a_k||r_j|^k$ for all j. Let $a = \max\{|a_0|^{\frac{1}{n}}, |a_1|^{\frac{1}{n-1}}, \ldots, |a_n|, 1\}$, then $|r_j| \leq a$ for all j. Next we have

$$\begin{aligned} |f(r_j)| &= |f(r_j) - f_j(r_j)| \\ &= \left| -\sum_{i=0}^{n} \left(a_i - a_i^{(j)} \right) r_j^i \right| \\ &\leq \max_{0\leq i\leq n-1} \left| a_i - a_i^{(j)} \right| |r_j|^i \\ &\leq \left| a_i - a_i^{(j)} \right| a^{n-1}. \end{aligned}$$

Since $\left|a_i^{(j)} - a_i\right| \leq \frac{1}{j}$, it follows that $|f(r_j)| \leq \frac{a^{n-1}}{j}$ so $f(r_j) \to 0$ as $j \to \infty$.

Let $F = \Omega_L^f$. As F/L is algebraic of finite degree, the absolute value on L extends uniquely to F by Theorem 3.5. Then $f(X) = \prod_{i=1}^n X - \alpha_i \in F[X]$ and $\prod_{i=1}^n |r_j - \alpha_i| \to 0$ in $\mathbb{R}$. Therefore there exists some k_0 such that $\langle |r_j - \alpha_{k_0}| \rangle_j$ has a subsequence converging to 0. Thus r_j has a subsequence r_{j_k} converging to α_{k_0} in F. Therefor r_{j_k} is a Cauchy sequence in L and so $\alpha_{k_0} \in L$ since L is complete. It follows that L is algebraically closed. □

As $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$, it follows that

Corollary 3.12.1. *$\mathbb{C}_p$ is a algebraically closed.*

It is unclear at this point what is the algebraic structure of $\mathbb{C}_p$. As it is a complete and algebraically closed field, it is tempting to associate it with the field of complex numbers, $\mathbb{C}$. It is in fact true that $\mathbb{C}_p$ and $\mathbb{C}$ are isomorphic, but unfortunately we cannot explicitly construct this isomorphism. For the details of the proof, see [6, p. 144].

4 p-adic Analysis

The field of p-adic analysis is vast, and many things from real analysis translate to the p-adic world, with unique and surprising property. We discuss here only one interesting application of p-adic number, called Newton polygons. This method assigns a polygon to every polynomial and power series with coefficients in $\mathbb{C}_p$, which tells us a lot about the roots of that polynomial and the radius of converges of the power series.

4.1 Newton polygons for polynomials

In this section we shall denote $f(X)$ as a polynomial of the form $f(X) = 1 + \sum_{i=1}^{n} a_i X^i$ with $a_i \in \mathbb{C}_p$. Since $\mathbb{C}_p$ is algebraically closed, every polynomial $f(X)$ in $\mathbb{C}_p[X]$ has a root and we will discover the behavior of said roots using Newton polygon.

Using the coefficients of $f(X)$, plot the following points

$$(0,0), (1, v_p(a_1)), (1, v_p(a_2)), \ldots, (1, v_p(a_n))$$

on a plane and if any $a_i = 0$, we simply ignore it. Then the Newton polygon can be constructed as follow: from the point $(0,0)$ construct a vertical line through $(0,0)$ and rotate it counter clockwise until it hits a second point then said line is a segment joining $(0,0)$ and $(i, v_p a_i)$. Repeat the same process for every other points to finish the construction. This generates the lower boundary of the convex hull of the above set of points. For each segments in a Newton polygon, we need to pay attention these items:

1. The slope of the segment.
2. The length of the projection of the segment onto the x-axis.
3. The values of i at each vertices or breaks of the polygon.

The reason why said items are special will become apparent soon.

Example 4.1. Let $f(X) = 1 + X^2 + 1/3X^3 + 3X^4$ with $p = 3$. Then the points are $(0,0)$, $(2,0)$, $(3,-1)$, $(4,1)$.

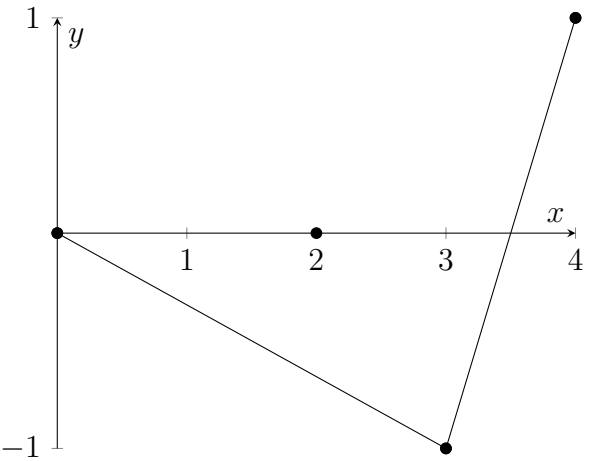


Figure 4.1: The Newton polygon of $f(X) = 1 + X^2 + 1/3X^3 + 3X^4 \in \mathbb{C}_3[X]$

As it turns out, the slopes of the Newton polygon count the number of roots of a given absolute value. The following theorem is adapted from [7, p. 97]

Theorem 4.2. *Let $f(X) = (1 - X/\alpha_1)(1 - X/\alpha_2)...(1 - X/\alpha_n)$ be the factorization of $f(X)$ in terms of its roots in $\mathbb{C}_p$. Let $\lambda_i = v_p(1/\alpha_i)$. Then if λ is a slope of the Newton polygon having length l, it follows that there are l of λ_i equal to λ (counting multiplicities).*

Proof. Suppose that the roots α_i are arranged in such a way that $\lambda_1 \leq \lambda_2 \leq ...\lambda_n$. Assume that $\lambda_1 = \lambda_2 = ... = \lambda_r < \lambda_{r+1}$ for $r \in \{2, 3, ..., n\}$. We first claim that the first segment of the polygon is the segment joining $(0, 0)$ and $(r, r\lambda_1)$. Recall that each a_i is expressed in terms of $1/\alpha_1$, $1/\alpha_2$, ..., $1/\alpha_n$ as the sum of all possible products of i of the $1/\alpha$'s. Since p-adic valuation of such product is at least $i\lambda_i$, the same is true for a_i, so the point $(i, v_p(a_i))$ is on or above the point $(i, i\lambda_1)$.

Now consider a_r. Of the various products of r of the $1/\alpha$'s, exactly one has the valuation $r\lambda_1$, namely, the product $1/(\alpha_1\alpha_2...\alpha_r)$. All of the other products have valuation $> r\lambda_1$ since we must include at least one of the $\lambda_{r+1}, \lambda_{r+2}, ..., \lambda_n$. Thus, a_r is a sum of something with valuation $r\lambda_1$ and something with valuation $> r\lambda_1$, so by a property of the non-Archimedean norm, $v_p(a_r) = r\lambda_1$.

Suppose that $i > r$. In the same way as before, we see that all of the products of i of the $1/\alpha$'s have valuation $> i\lambda_i$. Hence, $v_p a_i > i\lambda_i$. If we now think of how Newton polygon is constructed, we see that we have shown that its first segment is the line joining $(0, 0)$ with $(r, r\lambda_i)$.

If for $s \in \{1, 2, ..., n\}$, we have $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = ... = \lambda_r < \lambda_{r+1} < ... < \lambda_n$ with $r \in \{s, s + 1, ..., n\}$, then the line joining $(s, \sum_{i=1}^{s} \lambda_i)$ to $(r, \sum_{i=1}^{s} \lambda_i + (r - s)\lambda_{s+1})$ is a segment of the Newton polygon can be proved analogously. □

In other words, the slopes of the Newton polygon of $f(X)$ are the valuations of the reciprocal roots of $f(X)$ (counting multiplicities).

Example 4.3. Let $f(X) = 1 + 1/25X^2 + 5X^3 + 25X^4 + 7X^5$ with $p = 5$. Then we have a set of points $(0, 0)$, $(2, -2)$, $(3, 1)$, $(4, 2)$, $(5, 0)$ with its Newton polygon

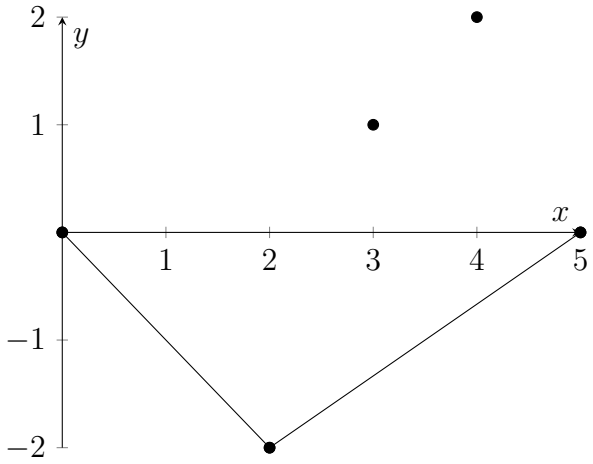


Figure 4.2: Newton polygon of $f(X) = 1 + 1/25X^2 + 5X^3 + 25X^4 + 7X^5 \in \mathbb{C}_5[X]$

Observably, there are two segments of slopes -1, $2/3$ and lengths 2, 3 respectively. Thus, there are two and three roots with absolute value 5 and $5^{-2/3}$ respectively.

4.2 Newton polygons for power series

Having studied the Newton polygon for a polynomial, one of the natural next steps is to consider the Newton polygon of a power series $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i$ with $a_i \in \mathbb{C}_p$. The rules for the construction of the Newton polygon shall be revised as: start with the vertical half-line which is in negative part of the y-axis and rotate that line counter-clockwise until one of the following occurs:

1. The line simultaneously hits infinitely many of the points plotted. In this case, stop and the construction is complete.

2. The line reaches a position where it contains only one of our points but can be rotated no further without leaving behind some points. In this case, stop and the construction is complete.

3. The line hits a finite number of the points. In this case, break the line at the last point that was hit and begin the whole construction again.

Example 4.4. Let $f(X) = 1 + \sum_{i=1} p^i X^i$, Then the points are $(0, 0)$, $(1, 1)$, $(2, 2)$, ...

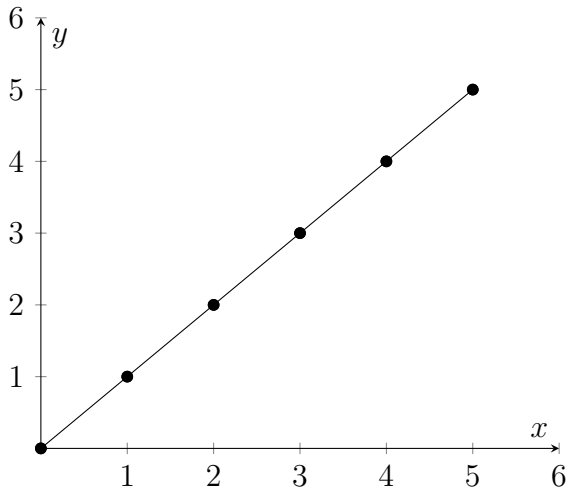


Figure 4.3: Newton polygon of $1 + \sum_{i=1} p^i X^i$

Similar to that of a polynomial, the Newton polygon also gives us useful information about its zeros but for the purpose of this paper, we shall only look at its radius of convergence. We start by proving the following lemma, which is one of the many nice properties of non-Archimedean absolute values.

Lemma 4.5. *Let $\langle a_k \rangle$ be a sequence in $\mathbb{C}_p$. Then $\sum_{k=0}^{\infty} a_k$ converges in $\mathbb{C}_p$ if and only if $\lim_{k\to\infty} a_k = 0$.*

Proof. Since the first implication is a known result, we shall only show the converse. Suppose that $a_k \to 0$ as $k \to \infty$. Let $A_n := \sum_{k=0}^{n} a_k$ be the partial sum of the series then for any integers m, n with $0 < m < n$ we have

$$|A_n - A_m|_p = \left| \sum_{k=m+1}^{n} a_k \right|_p \leq \max(|a_{m+1}|_p, ..., |a_n|_p) \to 0 \text{ as } m, n \to \infty.$$

So the partial sums A_n forms a Cauchy sequence, hence must converge to a limit in $\mathbb{C}_p$. □

Theorem 4.6. *Let b be the least upper bound of all slopes of the Newton polygon of $f(X)$. Then the radius of convergence is p^b (if b is infinite then $f(X)$ converges on all of $\mathbb{C}_p$).*

Proof. First let $x \in \mathbb{C}_p$ and $|x|_p < p^b$, i.e., $v_p(x) > -b$. Let $v_p(x) = -b'$, where $b' < b$. Then $v_p(a_i x_i) = v_p(a_i) - ib'$. But it is clear that, sufficiently far out, the point $(i, v_p(a_i))$ lies arbitrarily far above $(i, b'i)$, in other words, $v_p(a_i x^i) \to \infty$, and $f(X)$ converges at $X = x$.

Now let $|x|_p > p^b$, i.e., $v_p(x) = -b' < -b$. Then we find in the same way that $v_p(a_i x^i) = v_p(a_i) - b'i$ is negative for infinitely many values of i. Thus $f(x)$ does not converge. □

References

[1] Fernando Q. Gouvea. *p-adic Numbers: An Introduction*. Springer, Jun 2013.

[2] Serge Lang. *Algebra: Revised third edition*. Springer-Verlag, 2002.

[3] Neukirch Jurgen. *Algebraic number theory*. Springer, 1999.

[4] James Raymond Munkres. *Topology*. Pearson, 2nd edition, 2014.

[5] Serge Lang. *Algebraic Number Theory*. Springer, 2nd edition, 1986.

[6] Alain M. Robert. *A Course in p-adic Analysis*. Springer, Apr 2013.

[7] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer, Oct 2012.