FACULTY OF MATHEMATICS
DEPARTAMENT OF ALGEBRA

# The Néron-Ogg-Shafarevich Criterion for elliptic curves

## Jesús Navas Orozco

Memoir presented as part of the requirements for obtaining the Master's degree in Mathematics in the University of Seville.

September 7, 2020

Advisors: Dr. Sara Arias de Reyna Domínguez
Dr. José María Tornero Sánchez

# Contents

# ABSTRACT

This text is the required master thesis that the author needs to present in order to obtain his Master's degree in mathematics. It presents a proof of the Néron-Ogg-Shafarevich Criterion for elliptic curves over complete, discretely valued fields. With that goal, the basics of valuation theory and ramification are also developed, paying special attention to $p$-adic numbers.

# List of Symbols

| | |
|---|---|
| $\mathbb{N}$ | Set of natural numbers, without 0. |
| $\mathbb{Z}$ | Ring of rational integers. |
| $\mathbb{Q}$ | Field of rational numbers. |
| $\mathbb{R}$ | Field of real numbers. |
| $\mathbb{C}$ | Field of complex numbers |
| $\overline{K}$ | Algebraic closure of the field $K$ |
| $\gcd(a, b)$ | Greatest common divisor of $a$ and $b$. |
| $\operatorname{lcm}(a, b)$ | Lowest common multiple of $a$ and $b$. |
| $R^\times$ | Group of units of the ring $R$. |
| $\mathbb{F}_q$ | Finite field of $q$ elements. |
| $\mathbb{Z}/n\mathbb{Z}$ | Ring of integers modulo $n$. |
| $\mathcal{O}$ | Point at infinity of an elliptic curve in Weierstrass form. |
| $K(V)$ | function field of the algebraic variety $V$. |
| $\mathbb{Z}_{(p)}$ | Localization of $\mathbb{Z}$ at the prime ideal $(p)$. |
| $\mathbb{Z}_p$ | Ring of $p$-adic integers. |
| $\mathbb{Q}_p$ | Field of $p$-adic numbers. |
| $[L : K]$ | Degree of the extension $L\|K$. |
| $K^{\mathrm{nr}}$ | Maximal unramified subextension of $\overline{K}\|K$. |
| $\operatorname{Gal}(L/K)$ | Galois group of the Galois extension $L\|K$. |

# Introduction

When I told one of my advisors, Sara Arias, that I wanted to do a master's thesis about a topic related to Algebraic Geometry and Algebraic Number Theory, she recommended the Néron-ogg-Shafarevic Criterion, whose statement is as follows:

**Theorem.** *Let $K$ be a field complete with respect to a discrete valuation $v$ and let $E$ be an elliptic curve over $K$. Let $p$ be the characteristic of the residue class field of $K$, and let $\ell \neq p$ be a prime number.*
*Then $E$ has good reduction if and only if the Tate module $T_\ell(E)$ is unramified.*

We will prove the theorem under a slightly more complete statement (Theorem V.7.2). As it is often the case with results about elliptic curves, this theorem also holds for abelian varieties. The result was first introduced by Andrew Ogg in 1967 for elliptic curves, in his work *Elliptic curves and wild ramification.* Later, it was extented to abelian varieties by Serre and Tate (1968) in *Good reduction of abelian varieties*, using previous result of André Néron. They also named the criterion after Igor Shafarevich commenting that the later seemed to already know the result.

Although this theorem is the main goal of the master's thesis from a structural point of view, it also served as an excuse for me to delve into new topics like valuation theory, $p$-adic numbers and ramification theory. This work also utilizes my previous knowledge about elliptic curves, that I acquired for my bachelor's degree thesis: "*Elliptic curves and the Mordell Theorem*", [11], and further deepens it.

Now I am going to give a detailed exposition of the structure of this text and talk about the references that I used the most.

For the first three chapters, my main reference has been [12, Ch. II]. In order to have other approaches in mind, I have also consulted the texts [9] and [3].

The first chapter is basic valuation theory. I start defining absolute values on fields and then showing that the nonarchimedean ones can also be seen as (exponential) valuations. We focus our attention to discrete valuations. In any case, we end up with a metric in our field $K$. Then we show how to obtain a complete field $\widehat{K}$ out of $K$, through the process of *completion.* This generalizes to any field how the real numbers $\mathbb{R}$ are constructed as the completion of $\mathbb{Q}$ with the usual absolute value, and also how the $p$-adic numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ for the $p$-adic metric. Usually it is made the other way around: first one explain $p$-adic numbers and see the completion of a metric field as a generalization. In order to not being redundant and also for the sake of brevity, I opted to explain the general theory first. In chapter II, this sped up the construction of $\mathbb{Q}_p$ as a completion and the connection between the four different definitions of $p$-adic numbers that I am going to introduce. Of course, all those definitions lead to the same mathematical object, as we will show.

The third chapter is an introduction to ramification theory of valuations, followed by some basic results on the inertia subgroup. I have tried to present only the results that I was going to need, together with some basic ones to make the exposition clear and self-contained.

Chapter IV is about formal groups. The first two sections are general theory, and I mainly followed [16, Ch. V], with some help of the notes [10].

At this point, any reader that may not know or recall much about elliptic curves, should head to the Appendix A. In contains everything necessary to understand Chapter IV, §3 and the rest of this text. All of it was covered in bachelor's degree thesis [11].

Once we have presented the formal group of and elliptic curve in Chapter IV, §3, we pass on to the last Chapter. Here, we define and prove everything we still need to prove the Criterion, for example, the good or bad reduction of an Elliptic curve. Also, we present some practical applications of our results in the computation of the subgroup of points of finite order in §V.5. We end this text with the proof of the Criterion of Néron-Ogg-Shafarevich.

For Chapter IV, §3 and Chapter V, I followed the standard reference on elliptic curves: [16].

# Chapter I

# Valuation Theory

## I.1 Elementary valuation theory

**Definition I.1.1.** *A multiplicative valuation or* ***absolute value*** *of a field $K$ is a function $| \ | : K \to \mathbb{R}$ satisfying the properties:*

*I)* $|x| \geq 0$, *and* $|x| = 0 \iff x = 0$.

*II)* $|xy| = |x|\,|y|$.

*III)* $|x + y| \leq |x| + |y|$. *(triangle inequality)*

*for every $x, y \in K$.*

These properties immediately imply that $|1| = 1 = |-1|$, $|-x| = |x|$ and $\left|x^{-1}\right| = |x|^{-1}$. This last one shows that if $K$ is the field of fractions of a ring $R$, then it suffices to define $| \ |$ in $R$ to completely determine $| \ |$ in all of $K$.

We will always exclude tacitly the trivial absolute value of $K$: $|x| = 1$ for every $x \in K$. Just like we would do with a norm, we can use an absolute value $| \ |$ to define a distance function for every $x, y \in K$, namely $d(x, y) = |x - y|$, turning $K$ into a metric topological space. As per usual, two absolute values of $K$ are called **equivalent** if they define the same topology in $K$.

**Proposition I.1.2.** *Two absolute values $| \ |_1$ and $| \ |_2$ on $K$ are equivalent if and only if there exists a real number $s > 0$ such that:*

$$|x|_1 = |x|_2^s \qquad \forall x \in K.$$

*Proof.* If $| \ |_1 = | \ |_2^s$, then they are obviously equivalent since sequences have the same convergence and limits for both absolute values.

Conversely, assume both topologies are equivalent. Notice that $|x| < 1$ if and only if $\{x^n\}_{n \in \mathbb{N}}$ converges to 0 in the topology given by $| \ |$. Therefore we have

$$|x|_1 < 1 \implies |x|_2 < 1.$$

Let $x$ be any nonzero element of $K$ and let us fix an element $y \in K$ such that $|y|_1 > 1$. Then there exists $\alpha \in \mathbb{R}$ such that $|x|_1 = |y|_1^\alpha$. Let $\{m_i/n_i\}_{i\in\mathbb{N}}$ be a sequence of rational numbers with $n_i > 0$ that converges to $\alpha$ from above. Then $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$, or equivalently $\left|\dfrac{x_i^n}{y^{m_i}}\right|_1 < 1$, which implies $\left|\dfrac{x_i^n}{y^{m_i}}\right|_2 < 1$. We then have $|x|_2 < |y|_2^{m_i/n_i}$, and taking the limit this implies $|x|_2 \leq |y|_2^\alpha$.

Now, if we use the same argument but with a sequence $\{m_i/n_i\}_{i\in\mathbb{N}}$ of rational numbers that converges to $\alpha$ from below, we get $|x|_2 \geq |y|_2^\alpha$. So we have $|x|_2 = |y|_2^\alpha$. Therefore:

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\log |y|_1}{\log |y|_2} =: s \in \mathbb{R}_{>0}, \qquad \forall x \in K^\times$$

hence $|x|_1 = |x|_2^s$. But

$$|y|_1 > 1 \implies \left|\frac{1}{y}\right|_1 < 1 \implies \left|\frac{1}{y}\right|_2 < 1 \implies |y|_2 > 1.$$

Therefore $s = \frac{\log |y|_1}{\log |y|_2} > 0$, which finishes the proof. □

In the above proof we have only used $|x|_1 < 1 \implies |x|_2 < 1$ to show that there exist $s > 0$ such that $|x|_1 = |x|_2^s$ for every $x \in K$. Obviously the converse is true. Therefore we have:

**Corolary I.1.3.** *Two absolute values $|\ \ |_1$ and $|\ \ |_2$ on $K$ are equivalent if and only if:*

$$|x|_1 < 1 \implies |x|_2 < 1 \quad \forall x \in K.$$

*Proof.* □

**Definition I.1.4.** *An absolute value $|\ \ |$ on $K$ is called* ***nonarchimedean*** *if $|n|$ stays bounded for all $n \in \mathbb{N}$. Otherwise is called archimedean.*

Of course, every absolute value in a field of positive characteristic is nonarchimedean.

**Proposition I.1.5.** *An absolute value $|\ \ |$ is nonarchimedean if and only if it satisfies the* ***strong triangle inequality***

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

*Proof.* If the absolute value satisfies the strong triangle inequality then:

$$|n| = |1 + \cdots + 1| \leq 1.$$

Conversely, assume that there exists $N \in \mathbb{N}$ such that $|n| \leq N$ for every $n \in N$. Let $x, y \in K$ and without loss of generality suppose $|x| \geq |y|$. Then $|x|^k |y|^{n-k} \leq |x|^n$ for $k \geq 0$ and we have:

$$|x + y|^n \leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k} \leq \left(\sum_{k=0}^{n} \left|\binom{n}{k}\right|\right) |x|^n \leq N(n+1)|x|^n$$

and hence

$$|x+y| \le N^{1/n}(1+n)^{1/n}|x| = N^{1/n}(1+n)^{1/n}\max(|x|,|y|)\,.$$

By letting $n \to \infty$ this shows $|x+y| \le \max(|x|,|y|)$. □

**Proposition I.1.6.** *The strong triangle inequality implies that*

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

*Proof.* Without any loss of generality assume that $|x| > |y|$. Then

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

So all inequalities are equalities. We have used that $\max\{|y+x|\,,|y|\} = |y+x|$ since otherwise we would have $|x| \le |y|$. □

**Definition I.1.7.** *A function $v : K \to \mathbb{R}\cup\{\infty\}$ verifying the properties:*

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

*is called a (exponential) valuation of $K$, where we establish the following intuitive conventions for the symbol $\infty$ and every $a \in K$:*

$$a < \infty, \quad a + \infty = \infty, \quad \infty + \infty = \infty.$$

It is easily shown to verify $v(1) = 0$ and $v(x^{-1}) = -v(x)$. And since

$$2v(-x) = v((-x)^2) = v(x^2) = 2v(x)$$

we see that $v(x) = v(-x)$.

**Proposition I.1.8.** *Let $|\ \ |$ be a non-archimedean absolute value of $K$. Then the function*

$$v(x) = -\log|x| \quad \textit{for } x \ne 0, \quad \textit{and} \quad v(0) = \infty$$

*is a valuation of $K$.*

*Proof.* Properties 1 and 2 in Definition I.1.7 are immediately verified. For Property 3 we use that $|x+y| \le \max\{|x|\,,|y|\}$ and the fact that $-\log$ is a monotonically decreasing function:

$$v(x+y) = -\log|x+y| \ge -\log(\max\{|x|\,,|y|\}) = \min\{-\log|x|\,,-\log|y|\} = \min\{v(x), v(y)\}\,.$$

□

**Remark I.1.9.** Two equivalent absolute values $|\ \ |_1$ and $|\ \ |_2 = |\ \ |_1^s$, $s \in \mathbb{R}_{>0}$, produce the same valuation except for the scalar factor $s$:

$$v_2(x) = -\log |x|_2 = -s \log |x|_1 = s v_1(x).$$

This motivates the following definition.

**Definition I.1.10.** *Two valuations $v_1, v_2$ of $K$ are called equivalent if there exists $s > 0$ such that $v_1 = s v_2$.*

**Proposition I.1.11.** *Let $v$ be an exponential valuation of $K$. Then for each real number $q > 1$ the function:*

$$|x| = q^{-v(x)}$$

*is a nonarchimedean absolute value of $K$. We understand that $|0| = q^{-\infty} = 0$.*

*Proof.* It is an easy verification:

1) $|x| \geq 0$ and $|x| = 0 \iff v(x) = \infty \iff x = 0$.

2) $|xy| = q^{-v(xy)} = q^{-v(x)-v(y)} = |x|\,|y|$.

3) $|x+y| = q^{-v(x+y)} \leq q^{-\min\{v(x),v(y)\}} = \max\left\{q^{-v(x)}, q^{-v(y)}\right\} = \max\{|x|, |y|\}$.

□

**Remark I.1.12.** For a fixed $q > 1$, equivalent valuations $v_1 = s v_2$ produce equivalent absolute values:

$$|x|_1 = q^{-v(x)_1} = q^{-sv(x)_2} = |x|_2^s.$$

We have now seen that we can assign an exponential valuation to every nonarchimedean absolute value and viceversa. Furthermore, equivalent absolute values are sent to equivalent valuations and viceversa.

What happens when, starting with a nonarchimedean absolute value $|\ \ |$, we apply these two processes? Would we recover our original absolute value $|\ \ |$?

The answer depends on the real number $q > 1$ that we choose to create the exponential valuation. We can write $q = e^s$ for some $s > 0$. Then, from $|\ \ |$ we create $v(x) = -\log |x|$, and from it the valuation $|\ \ |'$ verifying:

$$|x|' = q^{-v(x)} = e^{-s \log |x|} = |x|^s.$$

Which proves that, in general, we recover an absolute value equivalent to the original one, and exactly the original one if $q = e$. Exactly the same can be said if we star with the exponential valuation $v$.

Since every valuation $v$ comes from an absolute value, Proposition I.1.6, tell us that:

$$v(x) \neq v(y) \implies v(x+y) = \min\{v(x), v(y)\}.$$

We need to recall a concept followed by a basic result:

**Definition I.1.13.** *Let $R$ be a ring and $K$ its field of fractions. $R$ is called a valuation ring if for every nonzero $x \in K$, either $x \in R$ or $x^{-1} \in R$.*

**Proposition I.1.14.** *A valuation ring $R$ is integrally closed.*

*Proof.* Let $K$ be the field of fractions of $R$ and let $x \in K$ be an integral element over $R$. This means that $x$ satisfies an equation:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \quad a_i \in R.$$

If $x \notin R$, then $x^{-1} \in R$. Therefore, multiplying by $x^{1-n}$ the above equation we get:

$$x = -a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0 x^{-n+1} \in R$$

a contradiction. □

The next three propositions also serve as important definitions.

**Proposition I.1.15.** *Let $|\ \ |$ be a nonarchimedean absolute value of a field $K$ and $v$ an associated valuation. Then the subset*

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid |x| \leq 1\}$$

*is a valuation ring, whose field of fractions is $K$, with group of units*

$$\mathcal{O}^\times = \{x \in K \mid v(x) = 0\} = \{x \in K \mid |x| = 1\}$$

*and the unique maximal ideal*

$$\mathfrak{p} = \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x| < 1\}.$$

*These* invariants *do not change if we replace $|\ \ |$ with an equivalent absolute value or $v$ with an equivalent valuation.*

*Proof.* All are easy checks. Obviously if we replace $v$ with $sv$ for a real number $s > 0$ the sets $\mathcal{O}, \mathcal{O}^\times, \mathfrak{p}$ do not change. If we replace $|\ \ |$ with $|\ \ |^s$, $s > 0$, then

$$|x| \leq 1 \iff |x|^s \leq 1; \quad |x| = 1 \iff |x|^s = 1 \quad \text{and} \quad |x| < 1 \iff |x|^s < 1$$

showing that the sets $\mathcal{O}, \mathcal{O}^\times, \mathfrak{p}$ are again preserved.

Let's prove that $\mathcal{O}$ is a ring. Obviously $0, 1 \in \mathcal{O}$. Let $x, y \in \mathcal{O}$. Then

$$|x + y| \leq \max\{|x|, |y|\} \leq 1$$
$$|xy| = |x|\,|y| \leq 1$$

So $\mathcal{O}$ is a ring. To see that $\mathcal{O}$ is a valuation ring, notice that every element $x \in K$ verifies either $|x| \leq 1$ or $|x| > 1$ (so that $\left|x^{-1}\right| < 1$). This is equivalent to $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

The units of $\mathcal{O}$ are those $x \in \mathcal{O}$ such that $x^{-1} \in \mathcal{O}$. But since $|x| \leq 1$ implies $\left|x^{-1}\right| \geq 1$, we must have $\mathcal{O}^\times = \{x \in K \mid |x| = 1\}$.

Next notice that $\mathfrak{p}$ is an ideal:

$$\begin{aligned} x, y \in \mathfrak{p} &\implies |x+y| \leq \max\{|x|, |y|\} < 1 \\ x \in \mathfrak{p}, y \in \mathcal{O} &\implies |xy| = |x|\,|y| < |y| \leq 1. \end{aligned}$$

Furthermore, every element of $\mathcal{O}$ not in $\mathfrak{p}$ is a unit. This implies that $\mathfrak{p}$ is a maximal ideal an the only one of $\mathcal{O}$, making $\mathcal{O}$ into a local ring.

All that remains to prove is that $\operatorname{Frac}(\mathcal{O}) = K$. Of course $\operatorname{Frac}(\mathcal{O}) \subset K$ because $K$ is a field containing $\mathcal{O}$. Conversely, let $x \in K$. Then, since $\mathcal{O}$ is a valuation ring, either $x \in \mathcal{O} \subset \operatorname{Frac}(\mathcal{O})$ or $x^{-1} \in \mathcal{O}$. In this later case, $x = \dfrac{1}{x^{-1}} \in \operatorname{Frac}(\mathcal{O})$. □

The field $k := \mathcal{O}/\mathfrak{p}$ is called **the residue class field** of $\mathcal{O}$ (or even of $K$ or $v$).

The valuation ring is sometimes called the ring of integers of $K$. I have personally avoided that nomenclature because it could lead to assuming that $R$ is the integral closure of $\mathbb{Z}$ in $K$, which is not.

**Proposition I.1.16.** *If $v : K \to \mathbb{R} \cup \{\infty\}$ is an exponential valuation, then the set $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$ called the* ***value group of*** *$K$*

*Proof.* $v(1) = 0$ is the zero element. And if $v(x), v(y) \in v(K^\times)$ then

$$\begin{gathered} v(x) + v(y) = v(xy) \in v(K^\times) \\ -v(x) = v(x^{-1}) \in v(K^\times). \end{gathered}$$

□

**Definition I.1.17.** *A valuation $v : K \to \mathbb{R} \cup \{\infty\}$ is called* ***discrete*** *if it admits a smallest positive value $s$. In that case the value group is $v(K^\times) = s\mathbb{Z}$.*

*Proof.* Let $x \in K$ such that $v(x) = s$ is the smallest positive value in $v(K^\times)$. Then for every $m \in \mathbb{Z}$, $v(x^m) = ms$, which shows that $s\mathbb{Z} \subset v(K^\times)$.

To prove that $v(K^\times) \subset s\mathbb{Z}$, we proceed by contradiction. Assume that there exists $y \in K^\times$ such that $v(y) = a \notin s\mathbb{Z}$. We can assume that $a$ is positive, because if $a$ were negative, we always could have choosen $0 < -a = v(y^{-1}) \notin s\mathbb{Z}$ instead. Now, let $m$ be greatest integer such that $a - ms > 0$, so that in particular $a - ms < s$. Then $v(yx^{-m}) = a - ms \in v(K^\times)$ is positive and smaller than $s$, a contradiction. □

A discrete valuation with smallest positive value $s$ is called **normalized** if $s = 1$. If $s \neq 1$ we can always divide by $s$ to get an equivalent valuation without changing the invariants $\mathcal{O}, \mathcal{O}^\times, \mathfrak{p}$. Having done so, let

$$\pi \in \mathcal{O}, \text{ such that } v(\pi) = 1.$$

Then every element $x \in K$ can be uniquely written in the form

$$x = u\pi^m \text{ for some } u \in \mathcal{O}^\times, m \in \mathbb{Z}$$

for if $v(x) = m$ then $v(x\pi^{-m}) = 0$, hence $x\pi^{-m} = u$ for some $u \in \mathcal{O}^\times$, which proves the claim.

With this notation we clearly have

$$\begin{aligned} \mathcal{O} &= \left\{u\pi^m : m \geq 0, u \in \mathcal{O}^\times\right\} \\ \mathfrak{p} = \pi\mathcal{O} &= \left\{u\pi^m : m \geq 1, u \in \mathcal{O}^\times\right\}. \end{aligned}$$

This shows that every element $\pi \in \mathcal{O}$ such that $v(\pi) = 1$ is a generator of $\mathfrak{p}$, which means that $\pi$ must be a **prime element** of $\mathcal{O}$ since $\mathfrak{p}$ is a maximal ideal. Furthermore, every prime element $\pi' \in \mathcal{O}$ must verify $v(\pi') = 1$, since by definition $\pi'$ is not an unit, hence $\pi|\pi'$ and we can write $\pi' = u\pi^m$ for some $u \in \mathcal{O}^\times, m \geq 1$. This means that $\pi'$ divides $\pi^m$, and since $\pi'$ is a prime element, $\pi'$ must divide $\pi$. Therefore $\pi$ and $\pi'$ are associates and $v(\pi) = v(\pi') = 1$. The prime elements $\pi$ are also called **uniformizers for $\mathcal{O}$**.

An important extension of this information is collected in the next proposition.

**Proposition I.1.18.** *If $v$ is a normalized discrete exponential valuation of $K$, then*

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} = \left\{u\pi^m : m \geq 0, u \in \mathcal{O}^\times\right\}$$

*is a principal ideal domain (hence a discrete valuation ring*)*

*Furthermore, the nonzero ideals of $\mathcal{O}$ are given by*

$$\mathfrak{p}^n = \pi^n\mathcal{O} = \{x \in K \mid v(x) \geq n\}, \quad n \geq 0$$

*where $\pi$ is a prime element, i.e., $v(\pi) = 1$. Finally, one has*

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}.$$

*Proof.* Let $I \neq 0$ be an ideal of $\mathcal{O}$ and $x \neq 0$ an element in $I$ with smallest positive value $v(x) = n$. then $x = u\pi^n, u \in \mathcal{O}^\times$, which means that $\pi^n\mathcal{O} \subset I$. Now let $y = w\pi^m, w \in \mathcal{O}^\times$ be an arbitrary element of $I$. Then $m = v(y) \geq n$, hence $y = (w\pi^{m-n})\pi^n \in \pi^n\mathcal{O}$, so that $I = \pi^n\mathcal{O}$. This proves that the only ideals of $\mathcal{O}$ are of the form $\pi^n\mathcal{O}$, which also implies that $\mathcal{O}$ is a principal ideal domain.

Finally, the morphism $\mathfrak{p}^n \to \mathcal{O}/\mathfrak{p}$ given by $a\pi^n \mapsto a \bmod \mathfrak{p}$, is clearly surjective (since $a$ can be any element of $\mathcal{O}$). Its kernel is the set of elements $a\pi^n \in \mathfrak{p}^n$ such that $a \in \mathfrak{p}$, i.e., the kernel is $\mathfrak{p}^{n+1}$. So it induces an isomorphism

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}.$$

□

*A local principal ideal domain whose only maximal ideal is nonzero. As a converse to this result, in any discrete valuation ring a discrete exponential valuation can be easily defined.

We have just seen that in a discretely valued field $K$, all the ideals of the valuation ring $\mathcal{O}$ form a decreasing chain:

$$\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \cdots$$

These ideals are also a basis of neighbourghoods of 0. Indeed, if $|\ \ | = q^{-v(\ )}, q > 1$ is an absolute value associated to $v$

$$\mathfrak{p}^n = \left\{ x \in K : |x| \leq \frac{1}{q^n} \right\} = \left\{ x \in K : |x| < \frac{1}{q^{n-1}} \right\}.$$

In order to get a basis of neighbourhoods of $1 \in K$ we define:

$$U^{(0)} = \mathcal{O}^\times, \qquad U^{(n)} = 1 + \mathfrak{p}^n, n \geq 1$$

Which are called the **n-th higher unit groups**. Of course:

$$\mathcal{O}^\times = U^{(0)} \supset U^{(1)} \supset \cdots$$

First we note that

$$x \in 1 + \mathfrak{p}^n \iff 1 - x \in \mathfrak{p}^n \iff |1 - x| < \frac{1}{q^{n-1}}, n \geq 1.$$

Therefore, an alternative definition of $U^{(n)}$ is

$$U^{(n)} = \left\{ x \in K^\times : |1 - x| < \frac{1}{q^{n-1}} \right\}.$$

Each of these open sets contains the element $1 \in K$. They are effectively subgroups of $\mathcal{O}^\times$ since:

$$x = 1 + a \in 1 + \mathfrak{p}^n \implies v(x) = \min(v(1), v(a)) = v(1) = 0 \implies x \in \mathcal{O}^\times$$

and

$$1 + x, 1 + y \in U^{(n)} \implies (1 + x)(1 + y) = 1 + x + y + xy \in 1 + \mathfrak{p}^n = U^{(n)}$$
$$x \in U^{(n)} \implies \left|1 - x^{-1}\right| = \underbrace{|x|^{-1}}_{=1} |x - 1| = |1 - x| < \frac{1}{q^{n-1}} \implies x^{-1} \in U^{(n)}.$$

**Proposition I.1.19.** *If $v$ is a discrete valuation, for every $n \geq 1$ we have*

$$\frac{\mathcal{O}^\times}{U^{(n)}} \cong \left( \frac{\mathcal{O}}{\mathfrak{p}^n} \right)^\times \quad \textit{and} \quad \frac{U^{(n)}}{U^{(n+1)}} \cong \frac{\mathcal{O}}{\mathfrak{p}}.$$

*Proof.* The first isomorphism is induced by the canonical group morphism

$$\mathcal{O}^\times \to \left( \frac{\mathcal{O}}{\mathfrak{p}^n} \right)^\times, \quad u \mapsto u \bmod \mathfrak{p}^n.$$

It is surjective, for if $\bar{x} \in \left(\dfrac{\mathcal{O}}{\mathfrak{p}^n}\right)^\times$, then there exists $\bar{y} \in \dfrac{\mathcal{O}}{\mathfrak{p}^n}$ such that $\bar{x}\bar{y} = 1 \in \dfrac{\mathcal{O}}{\mathfrak{p}^n}$. If $x, y \in \mathcal{O}$ are respective preimages of $\bar{x}$ and $\bar{y}$ for the surjective quotient map $\mathcal{O} \to \mathcal{O}/\mathfrak{p}^n$, then we have $xy \in 1 + \mathfrak{p}^n \subset \mathcal{O}^\times$. And if $xy$ is a unit, so are $x$ and $y$, so that $x \in \mathcal{O}^\times$.

Obviously the kernel of the canonical morphism mentioned above is $U^{(n)}$, so it induces an isomorpism $\dfrac{\mathcal{O}^\times}{U^{(n)}} \cong \left(\dfrac{\mathcal{O}}{\mathfrak{p}^n}\right)^\times$.

Our second isomorphism, once a prime element $\pi$ is chosen, is induced by the map:

$$U^{(n)} = 1 + \pi^n\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}, \quad 1 + \pi^n a \longmapsto a \bmod \mathfrak{p}$$

It is surjective, because the quotient map $\mathcal{O} \to \mathcal{O}/\mathfrak{p}$ is surjective.

It is a group morphism between the multiplicative group $U^{(n)}$ and the additive group $\dfrac{\mathcal{O}}{\mathfrak{p}}$, since $(1+\pi^n a)(1+\pi^n b) = 1+\pi^n(a+b+\pi^n ab)$ is mapped to $a+b+\pi^n ab \equiv a+b \bmod \mathfrak{p}$. Furthermore, the kernel is clearly $U^{(n+1)}$, so it induces an isomorphism $\dfrac{U^{(n)}}{U^{(n+1)}} \cong \dfrac{\mathcal{O}}{\mathfrak{p}}$. □

## I.2 Completions

**Definition I.2.1.** *A valued field $(K, |\ \ |)$ is called* ***complete*** *if every Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$ converges to an element $a \in K$.*

As usual, $\{a_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence if for every $\varepsilon > 0$ there exist $N \in \mathbb{N}$ such that

$$|a_n - a_m| < \varepsilon \quad \text{for all } m, n \geq N.$$

If $(K, |\ \ |)$ is any valued field, we can always find a complete valued field $(\widehat{K}, |\ \ |)$ such that $K \subset \widehat{K}$ and the valuation of $\widehat{K}$ extends that of $K$. This is obtained by the process of **completion**, which is carried out in the same way as the field of real numbers is constructed from the field of rational numbers, as the set of all limits of rational sequences, or equivalently, the set of all Cauchy sequences (with limit not necessarily in $\mathbb{Q}$) under the equivalent relation: "*having the same limit*". This can be expressed more conveniently in algebraic language.

*The Cauchy sequences of $K$ form a ring $R$, the nullsequences form a maximal ideal $\mathfrak{m}$, and we define the completion of $K$ as the field:*

$$\widehat{K} = R/\mathfrak{m}.$$

First we need to make sense of these claims.

We see the set of all sequences of $(K, |\ \ |)$ as the infinite product $\prod_{n=1}^{\infty} K$. This is a ring, with addition and multiplication being component-wise and where the zero and unit element are respectively $\underline{0} = (0, 0, 0, \dots)$ and $\underline{1} = (1, 1, 1, \dots)$.

**Proposition I.2.2.** *The set $R$ of Cauchy sequences of $(K, |\ \ |)$ is a subring of the infinite product $\prod_{n=1}^{\infty}$.*

*The subset $\mathfrak{m} \subset R$ of nullsequences is a maximal ideal.*

*Proof.* Constant sequences are convergent, hence they are Cauchy, so $\underline{0}, \underline{1} \in R$. If $\underline{x} = \{x_n\}_{n\in\mathbb{N}}$ and $\underline{y} = \{y_n\}_{n\in\mathbb{N}}$ are two Cauchy sequences, then they are bounded, i.e. $|x_n| \leq c_x, |y_n| \leq c_y$ for all $n \in \mathbb{N}$. Furthermore, there exist $N_1, N_2 \in \mathbb{N}$ such that for every $\varepsilon > 0$

$$|x_n - x_m| < \frac{\varepsilon}{2c_y} \text{ for all } m, n \leq N_1$$
$$|y_n - y_m| < \frac{\varepsilon}{2c_x} \text{ for all } m, n \leq N_2.$$

Let $N = \max\{N_1, N_2\}$. Then we have

$$\begin{aligned}|x_n y_n - x_m y_m| &= |x_n(y_n - y_m) + y_m(x_n - x_m)| \leq |x_n|\,|y_n - y_m| + |y_m|\,|x_n - x_m| \\ &< c_x\frac{\varepsilon}{2c_x} + c_y\frac{\varepsilon}{2c_y} = \varepsilon \quad \text{ for all } m, n \geq N\end{aligned}$$

and of course

$$|x_n + y_n - x_m - y_m| \leq |x_n - x_m| + |x_n - y_n|$$

which shows that $\underline{xy} \in R$ and $\underline{x} + \underline{y} \in R$, respectively. So $R$ is a ring.

The set $\mathfrak{m}$ is clearly closed under addition. And if $|x_n| \to 0, \{y_n\}_n \in R$, then, since $\{y_n\}_n$ is bounded, let us say by $c > 0$, then:

$$|x_n y_n| \leq c\,|x_n| \to 0 \implies \{x_n y_n\}_n \in \mathfrak{m}.$$

To see that $\mathfrak{m}$ is maximal it is better to show that $R/\mathfrak{m}$ is a field. In $R/\mathfrak{m}$ it does not matter how a sequence begins. More precisely, for every $n \in N$:

$$(x_1, x_2, ..., x_n, x_{n+1}, ...) \equiv (y_1, y_2, ..., y_n, x_{n+1}, x_{n+2}, ...) \mod \mathfrak{m}.$$

Let $\overline{x} \in R/\mathfrak{m}, \overline{x} \neq 0$. This means $\overline{x}$ is the class of a Cauchy sequence $x = \{x_n\}_n$ that is not a nullsequence. Therefore, it cannot have a subsequence that is a nullsequence (since otherwise $x$ would be a nullsequence). This implies that there exists $n_0$ such that $x_n \neq 0$ for every $n \geq n_0$ which means that in $R/\mathfrak{m}$:

$$\overline{(x_1, x_2, ..., x_{n_0}, x_{n_0+1}, ...)} = \overline{(1, 1, ..., 1, x_{n_0}, x_{n_0+1}, ...)}.$$

So an inverse for $\overline{x}$ is

$$\overline{(1, 1, ..., 1, x_{n_0}^{-1}, x_{n_0+1}^{-1}, ...)}$$

proving that $R/\mathfrak{m}$ is a field. □

Now we embed $K$ in $\widehat{K} = R/\mathfrak{m}$ associating to every $a \in K$ the class of the constant sequence $(a, a, ..., a, ...)$, since it simply is the class of the sequences whose limit is $a$.

The absolute value $|\ \ |$ of $K$ is easily **extended** to $\widehat{K}$. If $a \in \widehat{K}$ is represented by the Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$ we give it the absolute value

$$|a| = \lim_{n\to\infty} |a_n|\,.$$

This limit exists since $||a_n| - |a_m||_\infty \leq |a_n - a_m|$ implies that $|a_n|$ is a Cauchy sequence of $\mathbb{R}$ with the usual absolute value $|\ \ |$, so it must converge to an element of $\mathbb{R}$. This extension does not depend on the representative of $a$, for if we take any other representative $\{a_n + b_n\}_n$, where $\{b_n\}_n$ is a nullsequence, then

$$|a_n| - |b_n| \leq |a_n + b_n| \leq |a_n| + |b_n|$$

which together with $\lim\limits_{n\to\infty} |b_n| = 0$ implies that $\{a_n\}_n$ and $\{a_n + b_n\}_n$ have the same limit.

As always $||a_n| - |a_n||_\infty \leq |a_n - a_m|$ also shows that the absolute value $|\ \ | : \widehat{K} \to \mathbb{R}$ is a continuous function.

Then, one shows that $\widehat{K} = R/\mathfrak{m}$ is complete with respect the extended absolute value and that each $a \in \widehat{K}$ is the limit of a sequence $\{a_n\}$ in $K$. Finally, one proves that this completion is essentially unique, in the sense that if $(\widehat{K}', |\ \ |')$ is another complete valued field that contains $(K, |\ \ |)$ as a dense subfield, then the map[*]:

$$\sigma : \widehat{K} \to \widehat{K}', \qquad \lim_{n\to\infty} a_n \longmapsto \lim_{n\to\infty} a_n$$

[*] The first limit is taken with respect to $|\ \ |$ and the second limit with respect to $|\ \ |'$.

is a $K$-isomorphism that preserves the absolute value, i.e., $|a| = |\sigma(a)|'$. This is proven in the same way that one does when the real numbers are constructed from $\mathbb{Q}$. A proof can be found in [5, Theorem 1.1.4, pages 9-12]

The next results shows why we won't be interested in fields complete with respect to archimedean valuations: they are essentially $\mathbb{R}$ or $\mathbb{C}$. Some books, like [12], call it Ostrowski's Theorem but this name is often reserved in the literature for the classification of the absolute values of $\mathbb{Q}$ (Theorem II.3.2).

**Theorem I.2.3.** *Let $K$ be a field complete with respect to an archimedean absolute value $|\ \ |$. Then there is an isomorphism $\sigma$ from $K$ onto $\mathbb{R}$ or $\mathbb{C}$ satisfying*

$$|a| = |\sigma(a)|^s \quad \forall \quad a \in K$$

*for some $s \in (0, 1]$.*

*Proof.* [12, Ch. II, Theorem 4.2, page 124] □

The last result justifies why we will restrict our attention to nonarquimedean absolute values. In these cases is customary, and sometimes more convenient, to work with the exponential valuation $v$ directly. That is why it is worth mentioning how to extend it to $\widehat{K}$.

So let $v$ be an exponential valuation of a field $K$ and $|\ \ |$ an associated absolute value. $v$ can be canonically continued to a valuation $\widehat{v}$ of the completion $\widehat{K}$ by setting $\widehat{v}(0) = \infty$ and assigning for each nonzero $a = \lim_{n\to\infty} a_n \in \widehat{K}, a_n \in K$, the value:

$$\widehat{v}(a) = \lim_{n\to\infty} v(a_n). \tag{I.1}$$

Since $|a - a_n| \to 0 \implies v(a - a_n) \to \infty$, there exist $n_0$ such that for $n \geq n_0$ we have $v(a - a_n) > \widehat{v}(a)$. Now using that $v(x) \neq v(y) \implies v(x + y) = \min\{v(x), v(y)\}$ we get:

$$v = (a_n) = \widehat{v}(a_n - a + a) = \min\{\widehat{v}(a_n - a), \widehat{v}(a)\} = \widehat{v}(a)$$

So that the sequence $v(a_n)$ is eventually stationary (for $n \geq n_0$) and $\widehat{v}(a) \in v(K^\times)$, which implies the next result.

**Proposition I.2.4.** *Let $K$ be a field and $\widehat{K}$ its completion with respect to an exponential valuation $v$ of $K$. Then the value groups of $K$ and $\widehat{K}$ are the same, i.e.*

$$v(K^\times) = \widehat{v}(\widehat{K}^\times).$$

*Proof.* □

Therefore, if $v$ is discrete and normalized, so is the extension $\widehat{v}$.

Every Cauchy sequence of $K$ converges in $\widehat{K}$. It is then worthwhile to notice the following.

**Proposition I.2.5.** *If the absolute value $|\ \ |$ of $K$ is nonarchimedean then $\{a_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence if and only if $a_{n+1} - a_n$ is a nullsequence.*

*Proof.* The Cauchy condition for $\{a_n\}_{n\in\mathbb{N}}$ in particular implies that $a_{n+1}-a_n$ is a nullsequence.

Conversely, let $m \geq n$. Then we have:

$$\begin{aligned} |a_n - a_m| &= |a_n - a_{n-1} + a_{n-1} - a_{n-2} + \cdots + a_{m+1} - a_m| \\ &\leq \max\{|a_n - a_{n-1}|, \ldots, |a_{m+1} - a_m|\}. \end{aligned}$$

which shows that if $a_{n+1} - a_n$ is a nullsequence, $\{a_n\}_n$ is a Cauchy sequence. □

**Corolary I.2.6.** *Let $(K, |\ |)$ be a nonarchimedean valued field. Then an infinite series $\sum_{n=1}^{\infty} a_n$ is convergent in $\widehat{K}$ if and only if $\{a_n\}_n$ is a nullsequence.*

*Proof.* Let $s_n = \sum_{k=1}^{n} a_k$. Then by Proposition I.2.5, $s_n$ converges in $\widehat{K}$ if and only if $s_{n+1} - s_n = a_{n+1}$ is a nullsequence. □

**Proposition I.2.7.** *Let $\mathcal{O}$ and $\widehat{\mathcal{O}}$ be the valuation rings of $(K, v)$ and $(\widehat{K}, \widehat{v})$ respectively, with respective maximal ideals $\mathfrak{p}$ and $\widehat{\mathfrak{p}}$. Then one has*

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$$

*and if $v$ is discrete, one has furthermore*

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n \quad \textit{for} \quad n \geq 1.$$

*Proof.* The construction of the completion $\widehat{K}$ and the extension $\widehat{v}$ tell us that $\widehat{\mathcal{O}} \cap K = \mathcal{O}$ and $\widehat{\mathfrak{p}} \cap K = \mathfrak{p}$, since

$$\begin{aligned} \widehat{\mathcal{O}} &= \left\{x \in \widehat{K} : \widehat{v}(x) \geq 0\right\} \\ \widehat{\mathfrak{p}} &= \left\{x \in \widehat{K} : \widehat{v}(x) > 0\right\}. \end{aligned}$$

Which means that the ring morphism

$$\mathcal{O} \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}, \qquad a \mapsto a \mod \widehat{\mathfrak{p}}$$

is well defined. It is surjective since for every $x \in \widehat{\mathcal{O}}$, its class $\overline{x} = x + \widehat{\mathfrak{p}}$ is an open neighbourhood of $x$. By the density of $K$ in $\widehat{K}$, $(x+\widehat{\mathfrak{p}}) \cap K \neq \emptyset$. Any $y \in (x+\widehat{\mathfrak{p}}) \cap K \neq \emptyset$ is sent to $\overline{x}$ by this map. Crearly, the kernel is $\mathfrak{p}$. Therefore it induces an isomorphism $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$.

As we proved, if $v$ is discrete and normalized, then so it is $\widehat{v}$. Let $\pi \in \mathcal{O}$ be a prime element ($v(\pi) = 1 = \widehat{v}(\pi)$). Then the only ideals of $\widehat{\mathcal{O}}$ are $\widehat{\mathfrak{p}}^n = \pi^n \widehat{\mathcal{O}}, n \geq 0$. The map

$$\mathcal{O} \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}^n}, \qquad a \mapsto a \mod \pi^n \widehat{\mathcal{O}}$$

is ring morphism. It is surjective for the same reason as before: since $K$ is dense in $\widehat{K}$, for every $\in \widehat{\mathcal{O}}$ we have $\emptyset \neq (x + \widehat{\mathfrak{p}}^n) \cap K \subset \mathcal{O}$, because $x + \widehat{\mathfrak{p}}^n$ is an open neighbourhood of $x$. So that there exists $y \in \mathcal{O}$ such that $y \equiv x \mod \pi^n \widehat{\mathcal{O}}$. Since $\mathfrak{p}^n = \pi^n \mathcal{O} = \widehat{\mathfrak{p}}^n \cap \mathcal{O}$, the kernel is clearly $\mathfrak{p}^n$, so it induces an isomorphism $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n$ for $n \geq 1$. □

**Proposition I.2.8.** *Let $(K, v)$ be a discretely valued field. Let $S \subset \mathcal{O}$ be a system of representatives for the residue field $k = \mathcal{O}/\mathfrak{p}$ such that $0 \in S$, and let $\pi \in \mathcal{O}$ be a prime element. Then every $x \in \widehat{K}^{\times}$ admits a unique representation as a convergent series:*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

*where $a_i \in S, a_0 \neq 0, m \in \mathbb{Z}$.*

*Proof.* Let $\widehat{v}$ be the extension of $v$ to $\widehat{K}$. Since $\widehat{v}(\widehat{K}^{\times}) = v(K^{\times})$, $\pi$ is also a prime element of $\widehat{\mathcal{O}}$. We will construct the coefficients $a_i$ by induction.

Let $x = \pi^m u \in \widehat{\mathcal{O}}$ with $u \in \widehat{\mathcal{O}}^{\times}$. By the last Proposition we have $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$, wich means that the class of $u$ modulo $\widehat{\mathfrak{p}}$ has a unique representative $a_0 \in S, a_0 \neq 0$ (since $u$ is a unit).We thus have $u = a_0 + \pi b_1$. Assume now that for $n \geq 1$ we have found $a_0, ..., a_{n-1} \in S$, uniquely determined by $u$, such that:

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \pi^n b_n$$

for some $b_n \in \widehat{\mathcal{O}}$. Let $a_n \in S$ be the only representative of the class $b_n + \widehat{\mathfrak{p}} \in \widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$, so that $b_n = a_n + \pi b_{n+1}$ for some $b_{n+1} \in \widehat{\mathcal{O}}$. Hence:

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + \pi^{n+1}b_{n+1}.$$

In this way we construct an infinite series $\sum_{n=0}^{\infty} a_n\pi^n$ uniquely determined by $u$. Of course, it does converge (Proposition I.2.6), since the general term $a_n\pi^n$ tends to zero ($\widehat{v}(a_n\pi^n) \geq n$ for every $n \in \mathbb{N}$). It converges to $u$ since if $s_n = \sum_{\nu=0}^{n} a_\nu\pi^\nu$, then $u - s_n \in \widehat{\mathfrak{p}}^{n+1}$, which again means $u - s_n \to 0$ as $n \to \infty$. □

This last result also allows us to give the following meaningful example.

**Example I.2.9.** Let $k$ be a field. The polynomial ring in one variable $k[t]$ is a unique factorization domain. For every $a \in k$, we get a maximal ideal $(t - a)$, and for each one of them we can define a discrete valuation on its field of fractions $k(t)$ as follows. Let $f \in k(t), f \neq 0$. We extract from $f$ as many powers of $(t - a)$ as posible, i.e., we write $f$ as:

$$f(t) = (t-a)^m \frac{g(t)}{h(t)}, \quad \text{with } (g(t)h(t), (t-a)) = 1, \quad m \in \mathbb{Z}$$

and define

$$v_a(f) = m, \qquad v(0) = \infty.$$

This valuation (which has been defined in the same way the $p$-adic valuation will be defined in the next chapter) has $k[t]_{(t-a)}$ (the localization al $(t - a)$) as the valuation ring of $k(t)$. Of course, $v_a(t - a) = 1$. Proposition I.2.8, tell us that every nonzero element of the completion $\widehat{k(t)}$ is of the form:

$$f(t) = (t-a)^m \left(a_0 + a_1(t-a) + a_2(t-a)^2 + \cdots\right), \quad m \in \mathbb{Z}, a_i \in k$$

Which is to say that, if $x = t - a$, then $\widehat{k(t)} = k((x))$, the field of formal power series, also known as the **field of Laurent series**.

At this point one can already read Chapter 2 of this text. I say this because the last Proposition generalizes, to any discretely valued field, the fact that one can always express a non-zero $p$-adic number in the form

$$x = p^m(a_0 + a_1 p + \cdots), \qquad a_i \in \{0, ..., p-1\}, a_0 \neq 0, m \in \mathbb{Z}$$

$p$-adic integers can also be identified with $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, and it comes as no surprise the fact that we can obtain a similar result in this more general context of valuation theory.

For the rest of this section, let $K$ be a field, complete with respect to a discrete normalized valuation $v$. Let $\mathcal{O}$ be its valuation ring with maximal ideal $\mathfrak{p}$. For every $n \geq 1$, we have the canonical quotient maps $\mathcal{O} \to \mathfrak{p}^n$ and the natural projections:

$$\mathcal{O}/\mathfrak{p} \xleftarrow{\lambda_1} \mathcal{O}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \mathcal{O}/\mathfrak{p}^3 \xleftarrow{\lambda_3} \cdots$$

which induce a ring morphism $\mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n$, where of course:

$$\varprojlim_n \mathcal{O}/\mathfrak{p}^n = \left\{ (x_n) \in \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n \mid \lambda_n(x_{n+1}) = x_n \right\}.$$

If we consider the rings $\mathcal{O}/\mathfrak{p}^n$ as topological rings for the discrete topology, then $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ becomes a topological ring too, as a subspace of $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$ which has the product topology.

**Proposition I.2.10.** *Let $K$ be a complete discretely valued field. The canonical ring morphism*

$$\phi : \mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n, \qquad x \longmapsto (x \mod \mathfrak{p}^n)_{n\in\mathbb{N}}$$

*is an isomorphism and a homeomorphism. It also induces a group*

$$\mathcal{O}^\times \cong \varprojlim_n \mathcal{O}/U^{(n)}$$

*Proof.* The kernel of $\phi$ is $\bigcap_{n=1}^{\infty} \mathfrak{p}^n = 0$, so it is injective. For surjectivity, recall that we are working with a discrete valuation, so that $\mathfrak{p} = \pi\mathcal{O}$, and let $R \subset \mathcal{O}$ be a system of representatives of $\mathcal{O}/\mathfrak{p}$ that contains 0. By Proposition I.2.8, each residue $a \in \mathcal{O}/\mathfrak{p}$ can be uniquely written in the form:

$$a \equiv a_0 + a_1\pi + a_2\pi^2 + \cdots a_{n-1}\pi^{n-1} (\mathrm{mod}\, \mathfrak{p}^n), \quad a_i \in R$$

Therefore, every $s \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ is given by a coherent (for the natural projections) sequence of sums:

$$s_n = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}, n \in \mathbb{N}$$

which means that $s = \phi(x)$ where $x = \lim_{n\to\infty} s_n = \sum_{n=0}^{\infty} a_n\pi^n$.

We have proved that $\phi$ is an isomorphism. To prove that it is an homeomorphism it suffices* to show that a basis of neighbourhoods of $0 \in \mathcal{O}$ maps bijectively to a basis of neighbourhoods of $0 \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$.

First note that the sets

$$P_n = \prod_{k=1}^{n-1} \{0\} \times \prod_{k=n}^{\infty} \mathcal{O}/\mathfrak{p}^k, n \in \mathbb{N}$$

form a basis of neighbourhoods of $0 \in \prod_{k=1}^{\infty} \mathcal{O}/\mathfrak{p}^k$. Then, the bijection $\phi : \mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ maps the basic neighbourhood $\mathfrak{p}^n$ of $0 \in \mathcal{O}$ to the basic neighbourhood $P_n \cap \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ of $0 \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$. This proves that $\phi$ is a homeomorphism.

It induces an isomorphism when restricted to $\mathcal{O}^\times$:

$$\mathcal{O}^\times \cong \left(\varprojlim_n \mathcal{O}/\mathfrak{p}^n\right)^\times = \varprojlim_n (\mathcal{O}/\mathfrak{p}^n)^\times \cong \varprojlim_n \mathcal{O}^\times/U^{(n)}.$$

where the last isomorphism is given component-wise by Proposition I.1.19. □

Now let $K$ be a complete, nonarchimedean valued field (not necessarily discrete) and let $k = \mathcal{O}/\mathfrak{p}$ be its residue class field. The usual quotient map $\mathcal{O} \to k, x \mapsto \overline{x}$, induces a map $\mathcal{O} \to k[x]$ reducing the coefficients modulo $\mathfrak{p}$:

$$f(x) = a_0 + a_1x + \cdots a_nx^n \mapsto \overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$$

We still treat this operation as reducing modulo $\mathfrak{p}$, i.e., we write $\overline{f} = f \bmod \mathfrak{p}$ instead of $\bmod\, \mathfrak{p}[x]$.As it is customary, if $\lambda \in \mathcal{O}$, reduction mod $\lambda$ stands for reduction modulo the ideal $\lambda\mathcal{O}$.

**Definition I.2.11.** *A polynomial $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathcal{O}[x]$ is called **primitive** if*

$$|f| := \max\{|a_0|, \ldots, |a_n|\} = 1$$

In other words a polynomials $f \in \mathcal{O}[x]$ is primitive if at least one of the coefficients is in $\mathcal{O}^\times$, or equivalently, if $\overline{f} \neq 0$.

Now we can prove the main result of this chapter.

**Hensel's Lemma I.2.12.** *Let $K$ be complete with respect a nonarchimedean absolute value $|\ \ |$. Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial that admits a factorization modulo $\mathfrak{p}$:*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{\mathfrak{p}}$$

*This is a basic fact about topological groups. If $(G, +)$ is such a group, and $\{U_n\}_n$ is a basis of neighbourhoods of $0 \in G$, then for each $x \in G$, $\{x + U_n\}_n$ is a basis of neighbourhoods of $x$. In other words, a basis of neighbourhoods of $x \in G$ is obtained translating by $x$ a basis of 0.

*into relatively prime polynomials $\overline{g}, \overline{h} \in k[x]$. Then this factorization can be* **lifted up** *into a factorization of $f(x)$:*

$$f(x) = g(x)h(x)$$

*where $g, h \in \mathcal{O}[x]$ verify*

$$\deg(g) = \deg(\overline{g}); \qquad g(x) \equiv \overline{g}(x) \pmod{\mathfrak{p}} \quad \textit{and} \quad h(x) \equiv \overline{h}(x) \pmod{\mathfrak{p}}.$$

*Proof.* Let $d = \deg(f), m = \deg(\overline{g})$. First note that $\deg(\overline{f}) = \deg(\overline{g}) + \deg(\overline{h})$ because $k$ is a domain. Then

$$d = \deg(f) \geq \deg(\overline{f}) = \deg(\overline{g}) + \deg(\overline{h})$$

which means that $d - m \geq \deg(\overline{h})$. Now we lift $\overline{g}, \overline{h}$ by just lifting their coefficients, i.e., we choose polynomials $g_0, h_0 \in \mathcal{O}[x]$ such that $g_0 \equiv \overline{g} \pmod{\mathfrak{p}}, h_0 \equiv \overline{h} \pmod{\mathfrak{p}}$ verifying $\deg(g_0) = \deg(\overline{g}) = m, \deg(h_0) = \deg(\overline{h}) \leq d - m$. Of course $f \equiv g_0 h_0 \pmod{\mathfrak{p}}$. Since $(\overline{g}, \overline{h}) = 1$, there exist polynomials $a(x), b(x) \in \mathcal{O}[x]$ such that $ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}}$. Among the coefficients of $f - g_0 h_0 \in \mathfrak{p}[x]$ and $ag_0 + bh_0 - 1 \in \mathfrak{p}[x]$, we choose one of minimal valuation, and call it $\lambda$. This means that we have

$$\begin{cases} f(x) - g_0(x)h_0(x) \equiv 0 \pmod{\lambda} \\ a(x)g_0(x) + b(x)h_0(x) - 1 \equiv 0 \pmod{\lambda} \end{cases}$$

and not only modulo $\mathfrak{p}$.

We are going to look for the polynomials $g$ and $h$ in the form

$$g = g_0 + p_1\lambda + p_2\lambda^2 + \cdots, \quad h = h_0 + q_1\lambda + q_2\lambda^2 + \cdots \tag{I.2}$$

where $p_i, q_i \in \mathcal{O}[x]$ are polynomials of degree $< m$ and $\leq d - m$ respectively. If we were to find expressions as in (I.2), then $p_1\lambda + p_2\lambda^2 + \cdots$ and $q_1\lambda + q_2\lambda^2 + \cdots$ would indeed define polynomials in $\mathcal{O}[x]$ of degree $< m$ and $\leq d - m$, since grouping the coefficients of the monomial $x^t$ (for $t < m$ ó $t \leq d - m$) of each term of the infinite sums in (I.2), we would get a power series in $\lambda$: $\sum_{\ell=1}^{\infty} a_k\lambda^k, a_k \in \mathcal{O}$, that converges in $\mathcal{O}$ because $K$ is complete and $\lambda \in \mathfrak{p}$. This way we would have $\deg(g) = m, \deg(h) \leq d - m$, and hence $\deg(\overline{f}) \leq d$.

In order to construct these expressions we are going to successively determine the polymonials

$$g_{n-1} = g_0 + p_1\lambda + \cdots + p_{n-1}\lambda^{n-1}, \quad h_{n-1} = h_0 + q_1\lambda + \cdots + q_{n-1}\lambda^{n-1} \quad n \geq 1 \tag{I.3}$$

in a way that they verify

$$f \equiv g_{n-1}h_{n-1} \pmod{\lambda^n}.$$

This way, if we let $n \to \infty$, we would get $f = gh$ since $g_n \to g$ and $h_n \to h$, which would be a factorization of $f$ with the desired properties.

Recall that $f \equiv g_0 h_0 \pmod{\lambda}$, so we have already found the first couple of the polynomials (I.3) we are looking for (the case $n = 1$). Assume that we have already found these polynomials up to some $n \geq 1$ satisfying the desired congruence. Now we are looking for $g_n$ and $h_n$, or equivalently, $p_n$ and $q_n$. The relations:

$$g_n = g_{n-1} + p_n\lambda^n, \quad h_n = h_{n-1} + q_n\lambda^n$$

transform the condition $f \equiv g_n h_n \pmod{\lambda^{n+1}}$ into an equivalent condition for $p_n$ and $q_n$:

$$f \equiv g_{n-1}h_{n-1} + (g_{n-1}q_n + h_{n-1}p_n)\,\lambda^n \pmod{\lambda^{n+1}}$$

since if $p_n$ and $q_n$ were to satisfy the last congruence, and we define $g_n := g_{n-1} + p_n\lambda^n, h_n := h_{n-1} + q_n\lambda^n$, then of course the condition $f \equiv g_n h_n \pmod{\lambda^{n+1}}$ would hold.

So we must find $p_n$ and $q_n$ such that:

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\,\lambda^n \pmod{\lambda^{n+1}}.$$

Dividing by $\lambda^n$ in the above expression and writing $f_n = \lambda^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}[x]$, we get:

$$f_n \equiv g_{n-1}q_n + h_{n-1}p_n \equiv g_0 q_n + h_0 p_n \pmod{\lambda}.$$

This is the condition that $p_n$ and $q_n$ must satisfy. Since $ag_0 + bh_0 \equiv 1 \pmod{\lambda}$, we have:

$$af_n g_0 + bf_n h_0 \equiv f_n \pmod{\lambda} \tag{I.4}$$

and taking $q_n = af_n$ and $p_n = bf_n$ would apparently give us what we need, but the degrees may be higher that we can allow (remember, we want $\deg(p_n) < m$ and $\deg(q_n) \leq d - m$). For this reason, we use Euclidean division:

$$b(x)f_n(x) = q(x)g_0(x) + p_n(x)$$

obtaining polynomials $p_n(x)$ and $q(x)$ such that $\deg(p_n) < \deg(g_0) = m$. The highest order coefficient of $g_0$ is a unit since since $g_0 \equiv \overline{g} \pmod{\mathfrak{p}}$ and $\deg(\overline{g}) = \deg(g_0)$, hence $q(x) \in \mathcal{O}[x]$. Now, substituting this division in (I.4), we have the congruence

$$g_0\,(af_n + h_0 q) + h_0 p_n \equiv f_n \pmod{\lambda}.$$

Let $q_n$ be the polynomial obtained from $af_n + h_0 q$ by removing all coefficients divisible by $\lambda$. This way $\deg(q_n) = \deg(q_n \bmod \lambda)$ and $g_0 q_n + h_0 p_n \equiv f_n \pmod{\lambda}$. Recalling that $\deg(f_n) \leq d, \deg(g_0) = m$ and $\deg(h_0 p_n) < (d-m) + m = d$, from this last congruence we deduce that $\deg(q_n) \leq d - m$, as we wanted.

□

The following corollary tell us that we can lift roots of primitive polynomials $f \in \mathcal{O}[x]$ modulo $p$ to actual roots of $f$.

**Corolary I.2.13.** *Let $K$ be a field complete with respect to a nonarchimedean absolute value $|\ \ |$. Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial and let $\overline{\alpha} \in k$ such that*

$$f(\overline{\alpha}) \equiv 0 \pmod{\mathfrak{p}}$$

*but*

$$f'(\overline{\alpha}) \not\equiv 0 \pmod{\mathfrak{p}}$$

*i.e., $\overline{\alpha}$ is a root of the reduction of $f$ but not of the reduction of its formal derivative. Then, there exists $\alpha \in \mathcal{O}$ such that $\alpha \equiv \overline{\alpha}$ and $f(\alpha) = 0$.*

*Proof.* The fact that $\overline{f}(\overline{\alpha}) = 0$ means we can write:

$$\overline{f}(x) = (x - \overline{\alpha})\overline{f}_0(x)$$

The condition $\overline{f'}(\overline{\alpha}) \neq 0$ means that $\overline{\alpha}$ is a simple root of $\overline{f}$. In other words, $(x - \overline{\alpha})$ and $\overline{f}_0(x)$ are coprime. Now we can apply Hensel's lemma to $\overline{g}(x) = (x - \overline{\alpha})$ and $\overline{h}(x) = \overline{f}_0(x)$ to obtain polynomials $g, h \in \mathcal{O}[x]$ that factor $f$ and $\deg(g) = 1$. If $g(x) = ax + b$, since it reduces to $(x - \overline{\alpha})$, we have $a \equiv 1 \pmod{\mathfrak{p}}$ and $b \equiv \overline{\alpha} \pmod{\mathfrak{p}}$. In particular, $a \in \mathcal{O}^\times$. Therefore we can write:

$$f(x) = a(x - b/a)h(x).$$

Taking $\alpha = b/a$ we clearly have $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{p}}$ and $f(\alpha) = 0$. □

**Corolary I.2.14.** *Let $K$ be a field complete with respect to a nonarchimedean valuation $|\ |$. Then, every irreducible polynomial $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ with $a_0, a_n \neq 0$, verifies*

$$|f| = \max\{|a_0|, |a_n|\}.$$

*In particular, $a_n = 1$ and $a_0 \in \mathcal{O}$ imply that $f \in \mathcal{O}[x]$.*

*Proof.* Let $a_i$ be a coefficient of $f$ such that $|a_i| = |f| = \max\limits_{1\leq j\leq n}\{|a_j|\}$. If we multiply $f$ by $a_i^{-1}$, the new coefficients $b_j = a_i^{-1}a_j$ are in $\mathcal{O}$ and $b_i = 1$, i.e., $a_i^{-1}f \in \mathcal{O}[x]$ and $\left|a_i^{-1}f\right| = 1$. Let $b_r$ be the the first of the coefficients of $a_i^{-1}f$ such that $|b_r| = 1$. Then we have:

$$a_i^{-1}f(x) \equiv x^r(b_r + b_{r+1}x + \cdots + b_nx^{n-r}) \pmod{\mathfrak{p}}.$$

If we had $\max\{|b_0|, |b_n|\} < 1$, then $0 < r < n$, and applying Hensel's lemma to the above congruence would yield a factorization of $a_i^{-1}f(x)$ into two non-trivial factors, hence a factorization of $f(x)$, a contradiction.

So we must have $\max\{|b_0|, |b_n|\} = 1$, or equivalently

$$\max\{|a_0|, |a_n|\} = |a_i| = |f|.$$

□

This corollary, together with the following general result and lemma, will allow us to prove an important result about the extensions of valuations.

**Proposition I.2.15.** *Let $K$ be complete with respect to the absolute value $|\ |$ and let $V$ be an $n$-dimensional normed vector space over $K$. Then, for any basis $\{v_1, \ldots, v_n\}$ of $V$, the maximum norm*

$$\|x_1v_1 + \cdots + x_nv_n\| = \max\{|x_1|, \ldots, |x_n|\}, \quad x_i \in K$$

*is equivalent to the given norm on $V$. In particular, $V$ is complete and the isomorphism*

$$K^n \longrightarrow V, \quad (x_1, \ldots, x_n) \longmapsto x_1 v_1 + \cdots + x_n v_n$$

*is a homeomorphism.*

*Proof.* [12, Ch. II, Proposition 4.9, page 133] □

**Lemma I.2.16.** *Let $A$ be an integrally closed domain, $K$ its field of fraction and $B$ the integral closure of $A$ over a finite extension $L|K$, then*

$$x \in B \implies N_{L|K}(x) \in A.$$

*Proof.* Let $S$ be the set of all the $K$-embeddings of $L$ into $\overline{K}$. Of course, $A = B \cap K$. If $x \in B$, then its conjugates $\sigma x$ are also integral over $A$, hence $\sigma x \in B$ for every $\sigma \in S$. Recall (see, for example [13, Lemma C-5.67, page 457]) that

$$N_{L|K}(x) = \left( \prod_{\sigma \in S} \sigma x \right)^{[L:K(x)]}.$$

So that $N_{L|K}(x) \in B$. And of course $N_{L|K}(x) \in K$. Therefore $N_{L|K}(x) \in A = B \cap K$. □

**Theorem I.2.17.** *Let $K$ be complete with respect to an absolute value $|\ \ |_K$. Then $|\ \ |_K$ may be extended in a unique way to an absolute value of any given algebraic extension $L \mid K$. This extension is given by the formula*

$$|\alpha|_L = \sqrt[n]{\left|N_{L|K}(\alpha)\right|_K}$$

*when $L \mid K$ has finite degree $n$. In this case $L$ is again complete.*

*If $|\ \ |_K$ is nonarchimedean, the valuation ring of $(L, |\ \ |_L)$ is the integral closure of $\mathcal{O}$ in $L$.*

*Proof.* If $|\ \ |_K$ is archimedean, then by Theorem I.2.3, $K = \mathbb{R}$ or $\mathbb{C}$. $\mathbb{C}$ is algebraically closed, so every algebraic extension of $\mathbb{C}$ is $\mathbb{C}$ again. Since $\mathbb{C}$ is the only proper algebraic extension of $\mathbb{R}$ ([8, Corollary 3.20, page 267]), the only non-trivial case we have to consider is $K = \mathbb{R}, L = \mathbb{C}$, and then $[\mathbb{C} : \mathbb{R}] = 2$. From classical analysis we know that every norm in $\mathbb{R}$ and $\mathbb{C}$ is equivalent to their usual absolute values, which make them complete. The only thing left to show is that the formula actually extends the absolute value of $\mathbb{R}$ to the absolute value of $\mathbb{C}$, but this is obvious since for every $z \in \mathbb{C}$ we have

$$N_{\mathbb{C}|\mathbb{R}}(z) = z\overline{z} = |z|_{\mathbb{C}}^2.$$

So we may assume that $|\ \ |_K$ is nonarchimedean. Also, since every algebraic extension is the composition of its finite subextensions, we only need to prove the existence of a unique extension of $|\ \ |_K$ in the case where the extension $L|K$ is finite, of degree $n = [L : K]$.

**Existence of the extended valuation.** Let $\mathcal{O}$ be the valuation ring of $K$ and $\widetilde{\mathcal{O}}$ its integral closure in $L$. We are going to prove that:

$$\widetilde{\mathcal{O}} = \left\{ \alpha \in L \mid N_{L|K}(\alpha) \in \mathcal{O} \right\}. \tag{I.5}$$

The implication $\alpha \in \widetilde{\mathcal{O}} \implies N_{L|K}(\alpha) \in \mathcal{O}$ is given by Lemma I.2.16 since we know that the valuation ring $\mathcal{O}$ is integrally closed. (Proposition I.1.14).

For the other direction, let $\alpha \in L^{\times}$ such that $N_{L|K}(\alpha) \in \mathcal{O}$. Also, let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$$

be the minimal polynomial of $\alpha$ over $K$. Then* $N_{L|K}(\alpha) = \pm a_0^m \in \mathcal{O}$, which means that $|a_0|_K \leq 1$, hence $a_0 \in \mathcal{O}$. Then Corollary I.2.14 implies that $f \in \mathcal{O}[x]$, and since $\mathcal{O}$ is integrally closed, $\alpha \in \mathcal{O}$.

As the statement of this theorem suggests, we define for every $\alpha \in L$:

$$|\alpha|_L = \sqrt[n]{\left|N_{L|K}(\alpha)\right|_K}.$$

$|\ |_L$ does indeed extend the absolute value $|\ |_K$, since for every $x \in K$ we have $N_{L|K}(x) = x^n$. The fact that $N_{L|K}(\alpha) = 0 \iff \alpha = 0$ and $N_{L|K}(\alpha\beta) = N_{L|K}(\alpha)N_{L|K}(\beta)$ imply the two properties:

$$|\alpha|_L = 0 \iff \alpha = 0; \qquad |\alpha\beta|_L = |\alpha|_L\,|\beta|_L\,.$$

To show that $|\ |_L$ is a non archimedean absolute value on $L$, it only remains to prove the strong triangle inequality.

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

Without loss of generality, assume that $\max\left\{|\alpha|_L, |\beta|_L\right\} = |\alpha|_L$. We then multiply by $|\alpha|_L^{-1} = \left|\alpha^{-1}\right|_L$ the above inequality to get:

$$\left|1 + \frac{\beta}{\alpha}\right|_L \leq 1.$$

Since $\left|\dfrac{\beta}{\alpha}\right|_L \leq 1$, we have just shown that the strong triangle inequality is equivalent to:

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

Notice that for every $x \in L$

$$x \in \widetilde{\mathcal{O}} \iff N_{L|K}(x) \in \mathcal{O} \iff \left|N_{L|K}(x)\right|_K \leq 1 \iff |x|_L \leq 1 \tag{I.6}$$

*Recall that for $x \in L$, the norm $N_{L|K}(x)$ is, up a to sign, the coefficient of the zero-degree term of the characteristic polynomial of the automorphism *multiply-by-$x$* of $L$. This characteristic polynomial is also a $m$-th power of the minimal polynomial of $x$ over $K$, where $m = [K(x) : K]$. All this can be found in [12, Ch. I, §2].

This shows that

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

is equivalent to $\alpha \in \widetilde{\mathcal{O}} \implies \alpha + 1 \in \widetilde{\mathcal{O}}$, which is trivially true. This way the strong triangle inequality has been proven, making $|\ \ |_L$ into a nonarchimedean valuation of $L$. Equation (I.6) also shows that the valuation ring of $(L, |\ \ |_L)$ is $\widetilde{\mathcal{O}}$, the integral closure of $\mathcal{O}$ in $L$, as we wanted.

**Uniqueness of the extended valuation.** Let $|\ \ |'_L$ be another extension of $|\ \ |_K$ to $L$ with valuation ring $\mathcal{O}'$. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the maximal ideals of $\widetilde{\mathcal{O}}$ and $\mathcal{O}'$ respectively. We plan on showing that $\widetilde{\mathcal{O}} \subset \mathcal{O}'$. So assume that there exists $\alpha \in \widetilde{\mathcal{O}} \setminus \mathcal{O}'$, and let

$$f(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d$$

be its minimal polynomial over $K$. Above we showed that if $\alpha \in \widetilde{\mathcal{O}}$, then $f(x) \in \mathcal{O}[x]$, which means that $a_i \in \mathcal{O} \subset \mathcal{O}'$. Furthermore

$$\alpha \notin \mathcal{O}' \implies |\alpha|'_L > 1 \implies \alpha^{-1} \in \mathfrak{m}'.$$

Then, by multiplying by $\alpha^{-d}$ the equation $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} + \alpha^d = 0$ and rearranging we get:

$$1 = -a_{d-1}\alpha^{-1} - \cdots - a_1\left(\alpha^{-1}\right)^{d-1} - a_0\left(\alpha^{-1}\right)^d \in \mathfrak{m}',$$

a contradiction, because $\mathfrak{m}'$ is a maximal ideal. So we must have $\widetilde{\mathcal{O}} \subset \mathcal{O}'$. In other words, $|x|_L \leq 1 \implies |x|'_L \leq 1$. This implies that both valuations are equivalent, because otherwise, by Corollary I.1.3 there would exist $y \in L$ such that $|x|_L \leq 1$ but $|y|'_L > 1$, a contradiction. So there exists $s > 0$ such that $|x|_L^s = |x|'_L$ for every $x \in L$, but since $|\ \ |_L$ and $|\ \ |'_L$ agree on $K$, we must have $s = 1$, so that both absolute values are the same.

Finally, the fact that $L$ is again complete follows from Proposition I.2.15, because $L$ is an $n$-dimensional vector space over $K$. □

Due to the relation we established between nonarchimedean absolute values and exponential valuations, if $|\ \ |$ were non-archimedean, the above result could also be stated with an associated exponential valuation $v$ instead of an absolute value. In this case, if $n = [L : K] < \infty$, the extension $w$ of $v$ is given by the formula:

$$w(\alpha) = \frac{1}{n} v\left(N_{L|K}(\alpha)\right)$$

obtained from the one given by the theorem taking logarithms. And indeed, for every $x \in K$, $N_{L|K}(x) = x^n$, so that

$$v(x) = w(x) \qquad \forall x \in K.$$

Furthermore, we see that if $L|K$ is a finite extension then, if $v$ is discrete, the extension $w$ is again discrete.

**Observation I.2.18.** Let $K$ be a field complete with respect a nonarquimedean valuation $v$. Extend the valuation to the algebraic extension $L|K$. Then, their valuation rings $\mathcal{O}_L, \mathcal{O}_K$ and its respective maximal ideals, $\mathfrak{p}_L, \mathfrak{p}_K$, obviously verify

$$\mathcal{O}_K \subset \mathcal{O}_L \qquad \text{and} \qquad \mathfrak{p}_K \subset \mathfrak{p}_L.$$

But we furthermore have that $k_K \subset k_L$, i.e., an extension for the residue class field of $L$ and $K$. This is because the map:

$$\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{p}_L, \qquad x \mapsto \overline{x}$$

has $\mathfrak{p}_K$ as its kernel, so that it induces a natural injection $k_K = \mathcal{O}_K/\mathfrak{p}_K \hookrightarrow \mathcal{O}_L/\mathfrak{p}_L = k_L$.

# Chapter II

# $p$-adic Numbers

Throughout this chapter $p \in \mathbb{N}$ will be a prime number. We will give several definitions of $p$-adic numbers, showing of course that they are all the same.

## II.1 Classic Definition of $p$-adic Numbers

Let us recall that every positive integer $f \in \mathbb{N}$ has a unique expression in base $p$:

$$f = a_0 + a_1 p + \cdots + a_n p^n$$

where $a_i \in \{0, 1, \ldots, p-1\}$, a system of representatives of $\mathbb{F}_p$. We will call it the **p-adic expansion** of $f$. It is easily computed by succesively dividing $f$ by $p$.

$$\begin{array}{rcl} f & = & a_0 + f_1 p \\ f_1 & = & a_1 + f_2 p \\ & \vdots & \\ f_{n-1} & = & a_{n-1} + f_n p \\ f_n & = & a_n. \end{array}$$

Of course $a_i \in \{0, 1, \ldots, p-1\}$. In other words $a_i \equiv f_i (\operatorname{mod} p)$.

We can do something similar for every $f \in \mathbb{Z}_{(p)}$, i.e. for rational numbers whose denominator is not a multiple of $p$, since

$$\frac{\mathbb{Z}_{(p)}}{p^n \mathbb{Z}_{(p)}} = \mathbb{Z}/p^n\mathbb{Z}.$$

But for non integer rational numbers, or even for negative integers, we would get an infinite series

$$\sum_{k=0}^{\infty} a_k p^k = a_0 + a_1 p + \ldots$$

At least for now, this notation should be understood in a purely formal sense. That means that $\sum_{k=0}^{\infty} a_k p^k$ is just the sequence of partial sums:

$$s_n = \sum_{k=0}^{n} a_k p^k.$$

All this motivates the definition:

**Definition II.1.1.** *Let $p$ be a prime number. A* ***p-adic integer*** *in a formal series*

$$\sum_{k=0}^{\infty} a_k p^k = a_0 + a_1 p + \dots$$

*where $a_i \in \{0, 1, \dots, p-1\}$ for every $i = 0, 1, \dots$.*
*The set of all $p$-adic integers is denoted $\mathbb{Z}_p$.*

To associate a $p$-adic expansion to any $f \in \mathbb{Z}_{(p)}$, we can use the following elementary result:

**Proposition II.1.2.** *Let $a \in \mathbb{Z}$. For every $n \in \mathbb{N}$, the residue class of $a \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely represented in the form*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \dots + a_{n-1} p^{n-1} (\operatorname{mod} p^n)$$

*where $a_i \in \{0, 1, \dots, p-1\}$ for every $i = 0, 1, \dots, n-1$*

*Proof.* We proceed by induction on $n$. For $n = 1$ this simply means that each element of $\mathbb{Z}/p\mathbb{Z}$ has a unique representative in $\{0, 1, \dots, p-1\}$, which is obviously true. Assume that the result holds for $n-1$, then

$$a = a_0 + a_1 p + a_2 p^2 + \dots + a_{n-1} p^{n-2} + g p^{n-1}, \text{ for some } g \in \mathbb{Z}.$$

Now we just take $a_{n-1}$ as the only representative in $\{0, 1, \dots, p-1\}$ of $g \bmod p$, so that

$$a \equiv a_0 + a_1 p + a_2 p^2 + \dots + a_{n-1} p^{n-2} + a_{n-1} p^{n-1} \pmod{p^n}.$$

Since this $a_{n-1}$ is uniquely determined by $a$, the proposition holds. □

Since $\frac{\mathbb{Z}_{(p)}}{p^n \mathbb{Z}_{(p)}} = \mathbb{Z}/p^n\mathbb{Z}$, every rational number $f \in \mathbb{Z}_{(p)}$ defines a sequence of residue classes mod $p^n$:

$$\bar{s}_n := f \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1, 2, \dots$$

By the preceding proposition, we find uniquely determined $a_i \in \{0, 1, \dots, p-1\}$ such that:

$$\begin{array}{rcl} \bar{s}_1 & = & a_0 \bmod p \\ \bar{s}_2 & = & a_0 + a_1 p \bmod p^2 \\ \bar{s}_3 & = & a_0 + a_1 p + a_2 p^2 \bmod p^3 \\ & \vdots & \end{array}$$

The $a_i$ are the same for every equation because $\bar{s}_n$ is a coherent sequence for the canonical projections $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$. This sequence of integers:

$$s_n = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1}$$

defines a $p$-adic number $\sum_{k=0}^{\infty} a_k p^k$. This is the $p$-adic expansion of $f$. We have seen that:

$$\mathbb{Z}_{(p)} \subset \mathbb{Z}_p.$$

Now, in analogy with the Laurent series, we define:

**Definition II.1.3.** *A $p$-adic number is an expression of the form:*

$$\sum_{k=-m}^{\infty} a_k p^k = a_{-m}p^{-m} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + \cdots$$

*where $m \in \mathbb{Z}$ and $a_i \in \{0, 1, \ldots, p-1\}$. The set of all $p$-adic numbers is denoted $\mathbb{Q}_p$.*

Of course $\mathbb{Z}_p \subset \mathbb{Q}_p$.

We can write every rational number $f \in \mathbb{Q}$ as $f = \dfrac{g}{h}p^{-m}$ where $(gh, p) = 1$, so in particular $g/h \in \mathbb{Z}_{(p)}$. If $a_0 + a_1 p + a_2 p^2 + \ldots$ is the $p$-adic expansion of $g/h$, then we can assign to $f = \dfrac{g}{h}p^{-m}$ the $p$-adic expansion:

$$a_0 p^{-m} + a_1 p^{-m+1} + \cdots + a_m + a_{m+1}p + \cdots \in \mathbb{Q}_p.$$

We have just showed that $\mathbb{Q} \subset \mathbb{Q}_p$.

The $p$ adic number $\sum_{k=-m}^{\infty} a_k p^k = a_{-m}p^{-m} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + \cdots$ is usually denoted as

$$(a_{-m}a_{-m+1}\ldots a_0.a_1 a_2 \ldots)_p$$

or

$$(\ldots a_2 a_1 a_0.a_{-1}a_{-2}\ldots a_{-m})_p$$

I will use the latter since it is more consistent with the usual base $n$ notation. For example, $43.2_5 = 4 \cdot 5 + 4 + 2 \cdot 5^{-1} = \frac{122}{5}$. Furthermore, with this notation, the $p$-adic integers are precisely the expressions without *decimal* part, i.e. the expressions of the form $\ldots a_2 a_1 a_0.0000$, which is more intuitive.

It is possible to define addition and multiplication in $\mathbb{Z}_p$ that turn it into a ring and $\mathbb{Q}_p$ into its field of fractions. Addition works in the same way as the addition of two decimal expansion of real numbers: with the usual carry-over rules for digits in base $p$. For example, if, in $\mathbb{Z}_7$, we have $a = 1 + 4 \cdot 7 = 41_7, b = 6 + 5 \cdot 7 = 56_7$ then $a + b = 0 + 3 \cdot 7 + 7^2 = 130_7$.

For multiplication we can first formally multiply the power series defining two $p$-adic integers:

$$\left(\sum_{k=0}^{\infty} a_k p^k\right)\left(\sum_{k=0}^{\infty} b_k p^k\right) = \sum_{k=0}^{\infty} c_k p^k, \qquad \text{where } c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

Of course it could happen that $c_k > p-1$. In that case we write: $c_k = \widetilde{c_k} + d_k p$ with $\widetilde{c_k} \in \{0, 1, \ldots, p-1\}$, and therefore $c_k p^k = \widetilde{c_k} p^k + d_k p^{k+1}$. This way the new coefficient of $p^k$ and $p^{k+1}$ are $\widetilde{c_k}$ and $d_k + c_{k+1}$, respectively. Again, if $d_k + c_{k+1} \notin \{0, 1, \ldots, p-1\}$, we can repeat this proccess with this coefficient. Appliying successively this procedure starting with $c_0$, we get the $p$-adic expression of $ab$.

Showing that these operations turn $\mathbb{Z}_p$ into a ring is not difficult but very messy and it is an unnecesary effort, since it will follow immediately from the definition of $\mathbb{Z}_p$ as the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$ that we will give in the next section.

With these operations, the units of $\mathbb{Z}_p$ are the elements of the form

$$u = a_0 + a_1 p + \cdots \text{ where } a_0 \neq 0.$$

This is a direct consequence of Proposition IV.2.1. We can formally invert the power series in $p$ that defines $u$ and then proceed as with the multiplication two paragraphs above (the carry-over rules in base $p$) to get the coefficients of $u^{-1}$ to lie in $\{0, 1, ..., p-1\}$.

$\mathbb{Q}_p$ **is the quotient field of** $\mathbb{Z}_p$, which is another way to define $\mathbb{Q}_p$. This follows from the fact that every element of $\mathbb{Q}_p$ is of the form $p^m u$ with $m \in \mathbb{Z}$, i.e., $u \in \mathbb{Z}_p^\times$, so that every nonzero element of $\mathbb{Q}_p$ is invertible. Now, since $\mathbb{Q}_p$ is a field, it contains the field of fractions of $\mathbb{Z}_p$. Conversely, if $a/b \in \mathrm{Frac}(\mathbb{Z}_p)$, with $a, b \in \mathbb{Z}_p$, extract as high a power of $p$ from $b$ as possible, so that we can write $b = p^m u, u \in \mathbb{Z}_p$. Then $a/b = ap^{-m}u^{-1} \in \mathbb{Q}_p$. *This is exactly the reasoning used to show that the field of fractions of $k[[t]]$ (where $k$ is a field and $t$ an indeterminate) is just the field of Laurent series $k((t))$.*

All this results will also follow immediately from the (more practical) definition of the $p$-adic numbers as the completion of $\mathbb{Q}$ for the $p$-adic metric, that we will give in Section 3 of this chapter.

## II.2 $p$-adics as an Inverse Limit

Another representation of the $p$-adic numbers arise from viewing them not as sequences of partial sums of integers $\sum_{k=0}^{\infty} a_k p^k$, but as sequences of residue clases (these two things are the same thanks to Proposition II.1.2):

$$\bar{s}_n = s_n \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

These are coherent sequences $(\bar{s}_n)_{n\in\mathbb{N}} \in \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ for the canonical projections:

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} \cdots$$

Which just means that $\lambda_n(\bar{s}_{n+1}) = \bar{s}_n$

Anyone already familiarized with this concept already knows that the set we are talking about is the **projective limit** of the rings $\mathbb{Z}/p^n\mathbb{Z}$, i.e.

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \lambda_n\left(x_{n+1}\right) = x_n, \forall n \in \mathbb{N} \right\}.$$

We immediately have:

**Proposition II.2.1.** *There is a bijection*

$$\phi : \mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

*that arises from associating to every $p$-adic number $\sum_{k=0}^{\infty} a_k p^k$ the sequence of residues*

$$\bar{s}_n = \sum_{k=0}^{n-1} a_k p^k \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}.$$

*Proof.* Indeed, for each $p$-adic number the sequence $(\bar{s}_n)_{n\in\mathbb{N}}$ from the statement of the proposition is in $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Conversely, each sequence $(\bar{s}_n)_{n\in\mathbb{N}} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is of the form

$$\bar{s}_n = \sum_{k=0}^{n-1} a_k p^k \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$$

thanks to Proposition II.1.2, so it defines a $p$-adic integer $\sum_{k=0}^{\infty} a_k p^k$. □

The inverse limit has the advantage of clearly being a subring of the direct product $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. Therefore, this bijection $\phi$ gives $\mathbb{Z}_p$ the ring structure we seeked.

If one would decide to define the $p$-adic integers first this way, then for this to agree with the previous definitions, one would simply have to define the $p$-adic numbers $\mathbb{Q}_p$ as the fraction field of $\mathbb{Z}_p$.

It is worth mentioning that one of the more prominent applications of $p$-adic numbers is in Diophantine equations. These equations are of the form $F(x_1, \dots, x_n) = 0$ where $F \in \mathbb{Z}[x_1, \dots, x_n]$. The problem is then weakened considering all the congruences:

$$F(x_1, \dots, x_n) \equiv 0 \pmod{m}, \qquad m \in \mathbb{Z}.$$

Or, by the Chinese remainder theorem, only the congruences modulo all prime powers:

$$F(x_1, \dots, x_n) \equiv 0 \pmod{p^k}, \qquad p \text{ primo}, k \in \mathbb{N}.$$

In this line, we have the next result, which we will not use in this text but is worth mentioning.

**Proposition II.2.2.** *Let $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ and let $p$ be a prime number. Then the congruence:*

$$F(x_1, \dots, x_n) \equiv 0 \pmod{p^k}$$

*is solvable for every $k \geq 1$ if and only if the equation:*

$$F(x_1, \dots, x_n) = 0$$

*has a solution in $p$-adic integers.*

*Proof.* [12, Ch. II, §1, Proposition 1.4, page 105] □

We can already see some examples of explicit computations of the $p$-adic expansions of some rational numbers.

**Example II.2.3.** Euclidean division of $-1$ by $p$ results in $-1 = p - 1 + (-1)p$. Using this successively we see that:

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

Effectively we have

$$-1 \equiv p - 1 + (p-1)p + (p-1)p^2 + \dots + (p-1)p^{n-1} (\bmod\, p^n) \qquad \text{for every } n \in \mathbb{N}.$$

**Example II.2.4.** For every $n \in \mathbb{N}$ we have

$$1 = (1 + p + \dots + p^{n-1})(1-p) + p^n.$$

Therefore

$$\frac{1}{1-p} \equiv 1 + p + \dots + p^{n-1} (\bmod\, p^n) \qquad \text{for every } n \in \mathbb{N}.$$

This implies that the $p$-adic expansion of $\frac{1}{1-p}$ is $1 + p + p^2 + \dots$.

## II.3 $p$-adics as a Completion of $\mathbb{Q}$

When working on the field $\mathbb{Q}$, the usual absolute value $|\ |$ is denoted by $|\ |_\infty$, which is clearly archimedean. We also have the $p$**-adic absolute values** $|\ |_p$, defined as follow:

Let $a = b/c \in \mathbb{Q}^\times, a, b \in \mathbb{Z}$. We extract from $b$ and $c$ the highest possible power of the prime number $p$, resulting in:

$$a = p^m \frac{b'}{c'}, \quad (b'c', p) = 1$$

and we define

$$v_p(a) = m \qquad \text{and} \qquad |a|_p = \frac{1}{p^m}.$$

We also establish $v_p(0) = \infty$. Then, it is easily checked that $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ verifies the properties:

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

So $v_p$ is an exponential valuation, called the $p$**-adic valuation** and $|\ |_p$ is called the $p$**-adic absolute value**, which is a nonarchimedean absolute value (Proposition I.1.11). They obviously verify

$$|a|_p = p^{-v_p(a)} \qquad \text{and} \qquad v_p(a) = -\log_p |a|_p\,.$$

**Proposition II.3.1.** *The absolute values* $|\ |_p$ *and* $|\ |_\infty$ *of* $\mathbb{Q}$ *are pairwise inequivalent.*

*Proof.* For a given prime number $p$, $|p|_p = 1/p < 1$ and $|p|_q = 1$ for every $q \neq p$. So it does not exist $s > 0$ such that $|p|_p = |p|_q^s$. Of course, the archimedean absolute value $|\ |_\infty$ is not equivalent to any of the nonarchimedean $p$-adic absolute values, since, for example, $|2|_p \leq 1$ for every prime number $p$ but $|n|_\infty = 2 > 1$, so, again, it does not exist $s > 0$ such that $|2|_p = |2|_\infty^s$. □

The next proposition shows that the $p$-adic valuations and $|\ |_\infty$ are the only possible valutions of $\mathbb{Q}$ up to equivalence.

**Theorem II.3.2.** *(Ostrowski) Every non-trivial mutiplicative valuation of* $\mathbb{Q}$ *is equivalent to one of the valuations* $|\ |_p$ *or* $|\ |_\infty$.

*Proof.* Let $\|\ \|$ be a nonarchimedean absolute value. Then $\|n\| = \|1 + \cdots + 1\| \leq 1$ and there must be at least one prime number $p$ such that $\|p\| < 1$, because otherwise the unique prime factorization of integers would imply $\|x\| = 1$ for every $x \in \mathbb{Q}^\times$, and we had discarded the trivial valuation.

The set $A = \{a \in \mathbb{Z} \mid \|a\| < 1\}$ is clearly a proper ideal of $\mathbb{Z}$, satisfying $p\mathbb{Z} \subset A$. Since $p\mathbb{Z}$ is maximal, we must have $A = p\mathbb{Z}$. In particular, this shows that there was only one prime number $p$ with $\|p\| < 1$. Let $a \in \mathbb{Z}$ and write $a = bp^m$ with $p \nmid b$, so that $b \notin A$. Therefore $\|b\| = 1$ and

$$\|a\| = \|b\| \, \|p^m\| = \|p\|^m = |a|_p^s$$

where $s = -\log \|p\| / \log p$. Therefore, $\| \quad \|$ is equivalent to $| \quad |_p$.

Now let $\| \quad \|$ be an archimedean absolute value. We are going to see that for every $m, n \in \mathbb{Z}_{>1}$ we have

$$\|m\|^{1/\log m} = \|n\|^{1/\log n}. \tag{II.1}$$

First we write $m$ in base $n$:

$$m = a_0 + a_1 n + \cdots + a_r n^r, \qquad a_i \in \{0, 1, \ldots, n-1\}, n^r \leq m$$

Hence, $\|a_i\| = \|1 + \cdots + 1\| \leq a_i \|1\| \leq n - 1$ and $r \leq \log m / \log n$, so we have:

$$\begin{aligned} \|m\| &\leq \sum_{i=0}^{r} \|a_i\| \, \|n\|^i \leq \sum_{i=0}^{r} \|a_i\| \max\left\{\|n\|^r, 1\right\} \leq (1+r)(n-1) \max\left\{\|n\|^{\frac{\log m}{\log n}}, 1\right\} \\ &\leq \left(1 + \frac{\log m}{\log n}\right)(n-1) \max\left\{\|n\|^{\frac{\log m}{\log n}}, 1\right\} \end{aligned}$$

We have used that for $i \leq r$, $\|n\|^i \leq \max\left\{\|n\|^r, 1\right\}$, since we do not know if $\|n\| \geq 1$ or $\|n\| < 1$. What we do know is that there exists a $n_0 \in \mathbb{Z}_{>1}$ such that $\|n_0\| > 1$, because otherwise by the unique factorization of natural numbers, we would have $\|n\| \leq 1$ for every $n \in \mathbb{N}$, which is not possible because $\| \quad \|$ is archimedean.

Now we use the above inequality for $m^k$ instead of $m$, resulting in:

$$\|m\|^k \leq \left(1 + k\frac{\log m}{\log n}\right)(n-1) \max\left\{\|n\|^{k\frac{\log m}{\log n}}, 1\right\}.$$

Taking $k$-th roots on both sides results in:

$$\|m\| \leq \left(1 + k\frac{\log m}{\log n}\right)^{1/k} (n-1)^{1/k} \max\left\{\|n\|^{\frac{\log m}{\log n}}, 1\right\}.$$

And if we let $k$ tend to infinity we get:

$$\|m\| \leq \max\left\{\|n\|^{\frac{\log m}{\log n}}, 1\right\}.$$

Which is valid in particular for $m = n_0$. This means:

$$1 < \|n_0\| \leq \max\left\{\|n\|^{\frac{\log n_0}{\log n}}, 1\right\} = \max\left\{\|n\|, 1\right\}^{\frac{\log n_0}{\log n}},$$

where the equality is due to $\frac{\log n_0}{\log n} > 0$. The above equation tells us that $\max\left\{\|n\|, 1\right\}$ cannot be 1, therefore we have arrived at

$$\|n\| > 1.$$

And more importantly

$$\|m\| \leq \|n\|^{\frac{\log m}{\log n}} \qquad \text{or } \|m\|^{1/\log m} \leq \|n\|^{1/\log n}.$$

The same procedure swapping the roles of $m$ and $n$ gives

$$\|n\|^{1/\log n} \leq \|m\|^{1/\log m}.$$

Therefore we have proved (II.1) for every $m, n > 1$.

Putting $c = \|n\|^{1/\log n}$ (since it is constant for every $n \geq 2$), and $c = e^s$ for a real number $s > 0$, we have:

$$\|m\| = e^{s \log m} = |m|_\infty^s \text{ for every } m > 1.$$

This proves that $\| \ \ \|$ and $| \ \ |_\infty^s$ coincide on $\mathbb{Z}$, thus they coincide on its field of fractions $\mathbb{Q}$ . □

**Proposition II.3.3.** *For every nonzero rational number $a \neq 0$, one has:*

$$\prod_p |a|_p = 1.$$

*where $p$ varies over all prime numbers and the symbol $\infty$.*

*Proof.* We can factor each nonzero rational number as:

$$a = \pm \prod_{p \neq \infty} p^{v_p(a)}.$$

The sign of $a$ equals $\frac{a}{|a|_\infty}$. Then we may write

$$a = \frac{a}{|a|_\infty} \prod_{p \neq \infty} \frac{1}{|a|_p}$$

and cancelling $a \neq 0$ in both sides yields the desired formula. □

Now we define the $p$-adic numbers as a completion, as we promised. We are going to reset the notation momentarily and use $\mathbb{Q}_p$ and $\mathbb{Z}_p$ for these new definitions, but later we will show that they coincide with the $p$-adic numbers and $p$-adic integers defined in the last section.

**Definition II.3.4.** *The field of $p$-adic numbers is the completion with respect to the $p$-adic absolute value $| \ \ |_p$ of the field of rational numbers.*

The completion is made as described in **Chapter I, §2**. The $p$-adic absolute value and valuation are extended from the ones that we have defined for $\mathbb{Q}$ in the same way that we explained in **Chapter I, §2**, so there is no need to explain it here again. Only recall that if $0 \neq x = \lim\limits_{n\to\infty} x_n \in \mathbb{Q}_p$, for a Cauchy sequence $\{x_n\}_n$ of $\mathbb{Q}$, then the sequence $v_p(x_n)$ must eventually become stationary[*], i.e., there exist some $n_0 \in \mathbb{N}$ such that $v_p(x_n) = v_p(x_{n_0})$ for every $n \geq n_0$. Therefore, the same can be said about $|x_n|_p$. Then the extensions are given by:

$$v_p(x) := \lim_{n\to\infty} v_p(x_n) = v_p(x_{n_0})$$
$$|x|_p := \lim_{n\to\infty} |x_n|_p = |x_{n_0}|_p \, .$$

And therefore $v_p(\mathbb{Q}_p^\times) = v_p(\mathbb{Q}^\times) = \mathbb{Z}$ (Proposition I.2.4).

**Definition II.3.5.** *We define the $p$-adic integers as the valuation ring of $\mathbb{Q}_p$:*

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \right\} = \{ x \in \mathbb{Q}_p | v(x)_p \geq 0 \} \, .$$

**Proposition II.3.6.** $\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p | \, |x|_p \leq 1 \right\}$ *is the closure with respect to $| \ \ |_p$ of the ring $\mathbb{Z}$ in the field $\mathbb{Q}_p$.*

*Proof.* If $\{x_n\}_n$ is a Cauchy sequence in $\mathbb{Z}$ and $x = \lim\limits_{n\to\infty} x_n \in \mathbb{Q}_p$, then

$$|x_n|_p \leq 1 \quad \forall n \in \mathbb{N} \implies |x|_p \leq 1$$

hence $x \in \mathbb{Z}_p$ (note that $|x|_p$ refers to the extended valuation in $\mathbb{Q}_p$). This shows that $\overline{\mathbb{Z}}^{| \cdot |_p} \subset \mathbb{Z}_p$.

Conversely, let $x = \lim\limits_{n\to\infty} x_n \in \mathbb{Z}_p$, where $\{x_n\}_n$ is a Cauchy sequence of $\mathbb{Q}$. We know that there exists $n_0 \in \mathbb{N}$ such that $v_p(x_n)$ is stationary for $n \geq n_0$, and the same goes for $|x|_p$. Therefore $|x_n|_p = |x|_p \leq 1$ for every $n \geq n_0$, so we can write $x_n = \frac{a_n}{b_n}$, with $a_n, b_n \in \mathbb{Z}$ and $(b_n, p) = 1$. Now, for each $n \geq n_0$, choose a solution $y_n \in \mathbb{Z}$ of the congruence $b_n y_n \equiv a_n \pmod{p^n}$ (which exists because $b_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$). Since $\left|\frac{1}{b_n}\right|_p = 1$, this means that

$$|a_n - b_n y_n| \leq \frac{1}{p^n} \implies |x_n - y_n|_p = \left|\frac{1}{b_n}\right|_p |a_n - b_n y_n|_p \leq \frac{1}{p^n}$$

and hence $x = \lim\limits_{n\to\infty} y_n$, so that $x \in \overline{\mathbb{Z}}^{| \cdot |_p}$. □

Our work in the previous Chapter on the more general context of Valuation Theory let us deduce almost instantly many important results about $p$-adic numbers. We collect them below.

**Proposition II.3.7.** *(a) The maximal ideal, $\mathfrak{p}$, of the discrete valuation ring $(\mathbb{Z}_p, | \ \ |_p)$ is generated by $p$, i.e.*

$$\mathfrak{p} = p\mathbb{Z}_p.$$

[*] Also recall that this only occurs because the valuation is nonarchimedean

(b) *The units of* $\mathbb{Z}_p$ *are the elements that are not a multiple of* $p$*, i.e.*

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \smallsetminus p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v(x)_p = 0\}\,.$$

(c) *Every element* $x \in \mathbb{Q}_p^\times$ *admits a unique representation:*

$$x = p^m u \qquad \text{with } m \in \mathbb{Z} \text{ for some } u \in \mathbb{Z}_p^\times.$$

*where* $m = v(x)_p$*.*

(d) *The nonzero ideals of the ring* $\mathbb{Z}_p$ *are the principal ideals*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq n\}\,.$$

(e) *The residue class field of* $\mathbb{Z}_p$ *is*

$$k_p = \frac{\mathbb{Z}_p}{p\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

*More generally, for every* $n \geq 1$*, we have:*

$$\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}.$$

(f) *Every* $x \in \mathbb{Q}_p^\times$ *has a unique representation as a convergent series:*

$$x = p^m(a_0 + a_1 p + a_2 p^2 + \cdots)$$

*where* $a_i \in 0, 1, \ldots, p-1, a_0 \neq 0, m \in \mathbb{Z}$*.*

(g) *There is a canonical isomorphism*

$$\mathbb{Z}_p \cong \varprojlim_n \frac{\mathbb{Z}}{p^n\mathbb{Z}}.$$

*Proof.* (a) $p$ is a prime element of $\mathbb{Z}_p$ since $v(p) = 1$, so it generates its maximal ideal.

(b) A direct consequence of (a).

(c) We saw in Chapter I that this is true for any discretely valued field, but we repeat it here: if $v_p(x) = m$, then $v_p(xp^{-m}) = 0$ so that $xp^{-m} = u$ for some $u \in \mathbb{Z}_p^\times$, which proves our claim.

(d) Proposition I.1.18.

(d) The valued field $(\mathbb{Q}, |\ \ |_p)$ has as its valuation ring

$$\mathcal{O} = \{x \in \mathbb{Q} : v_p(x) \geq 0\} = \mathbb{Z}_{(p)}$$

the rational numbers whose denominator is not divisible by $p$. Of course, the maximal ideal of $\mathbb{Z}_{(p)}$ is $p\mathbb{Z}_{(p)}$, and $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^n\mathbb{Z}$. Then, since $\mathbb{Q}_p$ is the completion of $(\mathbb{Q}, |\ \ |_p)$, Proposition I.2.7 tells us:

$$\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \frac{\mathbb{Z}_{(p)}}{p^n\mathbb{Z}_{(p)}} \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}, \qquad \forall n \geq 1$$

(f) Proposition I.2.8, using that the residue class field $k \cong \mathbb{Z}/p\mathbb{Z}$ of $\mathbb{Q}_p$ has $\{0, 1, \dots, p-1\}$ as a system of representatives.

(g) Since $\mathbb{Q}_p$ is complete, Proposition I.2.10 tell us that there is a canonical isomorphism

$$\mathbb{Z}_p \cong \varprojlim_n \frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}.$$

The result then follows from (e).

□

In the previous proposition, (g) allows us to connect the definition of $\mathbb{Q}_p$ from this section with the one of Section 2, and by transitivity (or by Proposition II.3.7 (f)), it also connects with our definition in Section 1. Therefore, we may use $\mathbb{Q}_p$ and $\mathbb{Z}_p$ to denote $p$-adic numbers and $p$-adic integers for any of its definitions, without creating any confusion.

Yet another interesting result about $\mathbb{Q}_p$ is:

**Proposition II.3.8.** *The ring of $p$-adic integers $\mathbb{Z}_p$ contains the $(p-1)$-roots of unity.*

*Proof.* Since $x^{p-1} \equiv 1 \pmod{p}$ for every $x \in \mathbb{F}_p^\times = \mathbb{Z}/p\mathbb{Z}$ and $\left|F_p^\times\right| = p-1$, the polynomial $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ splits into distinct linear factors over the residue class field $\mathbb{F}_p$. Applying repeatedly Hensel's lemma (I.2.12) or its Corollary I.2.13, we see that $x^{p-1} - 1$ also splits into distinct linear factors over $\mathbb{Z}_p$ (the factors over $\mathbb{Z}_p$ must be different, otherwise the factors over $\mathbb{F}_p$ wouldn't be distinct). □

To end this section, we compute some more $p$-adic expansions.

**Example II.3.9.** In this example, we want to compute the 5-adic expansion of $2/3$ and $-2/3$.

First observe that by Fermat's Little Theorem, $3 \mid 5^{2n} - 1$ for every $n \in \mathbb{N}$. With our notation, for example, $5^{2n} = 100_5 = 44_5 + 1$. We have

$$\frac{44_5}{3} = \frac{5^2 - 1}{3} = 8 = 13_5$$

Using this, we can compute:

$$\frac{5^4-1}{3} = \frac{10000_5 - 1}{3} = \frac{4444_5}{3} = \frac{44_5 \cdot 100_5 + 44_5}{3} = 13_5 100_5 + 13_5 = 1313_5$$

In general we have:

$$\frac{5^{2n}-1}{3} = \frac{\overbrace{44\dots44_5}^{2n \text{ digits}}}{3} = \underbrace{1313\dots13_5}_{2n \text{ digits}}$$

Letting $n$ tend to $\infty$, we see $-1/3 = \dots131313_5$ because $\lim\limits_{n\to\infty} = 5^{2n} = 0$ in the 5-adic metric.

$$\frac{2}{3} = -\frac{1}{3} + 1 = \dots131314_5$$

And using the usual carry-over rules (in base 5) we also have

$$-\frac{2}{3} = -\frac{1}{3} - \frac{1}{3} = \dots131313_5 + \dots131313_5 = \dots3131_5$$

As we can see, $2/3$ and $-2/3$ are 5-adic integers, which was expected since $2/3, -2/3 \in \mathbb{Z}_{(5)} \subset \mathbb{Z}_5$.

## II.4 $p$-adics as a Quotient Ring of Formal Power Series

Yet another, direct method to introduce $p$-adic numbers is stablished in the next proposition.

**Proposition II.4.1.** *There is a canonical ring isomorphism*

$$\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X-p).$$

*Proof.* The substitution $X \mapsto p$ gives a surjective morphism $\mathbb{Z}[[X]] \to \mathbb{Z}_p$ that associates to each formal power series $\sum_{k=0}^{\infty} a_k X^k$ the $p$-adic number $\sum_{k=0}^{\infty} a_k p^k$ (it may be neccesary to use the usual carry-over rules in base $p$ to get the coefficients to lie in $\{0,1,\dots,p-1\}$). Of course, the ideal $(X-p)$ is in the kernel of this mapping, so it suffices to show that this is the whole kernel.

Let $f(X)=\sum_{k=0}^{\infty} a_k X^k$ be an element of this kernel, i.e., such that $f(p)=0$. This means:

$$a_0 + a_1 p + \dots + a_{n-1}p^{n-1} \equiv 0 \pmod{p^n}$$

for every $n \in \mathbb{N}$. Therefore, for each $n \geq 1$, there exist $b_{n-1} \in \mathbb{Z}$ such that

$$-b_{n-1}p^n = a_0 + a_1 p + \dots + a_{n-1}p^{n-1}$$

And they verify:

$$\begin{array}{rcl} a_0 & = & \quad -pb_0, \\ a_1 & = & b_0 - pb_1 \\ a_2 & = & b_1 - pb_2 \\ & \vdots & \end{array}$$

Which then implies

$$a_0 + a_1 X + a_2 X^2 + \dots = (X-p)(b_0 + b_1 X + b_2 X^2 + \dots)$$

so that $f(X)$ belongs to the ideal $(X-p)$ □

When working with formal power series it is worth having in mind Proposition IV.2.1. In this case serves to see again the relation between the units of $\mathbb{Z}_p$

$$\mathbb{Z}_p^{\times} = \left\{a_0 + a_1 p + a_2 p^2 + \dots \mid a_i \in \{0,1,\dots,p-1\}, a_0 \neq 0\right\}$$

and the invertible elements of a formal power series ring.

# Chapter III

# Local Fields, Ramification and Inertia

## III.1 Local Fields

**Global fields** are either:

- Algebraic number fields: finite extensions of $\mathbb{Q}$.
- Global function fields: finite extensions of $\mathbb{F}_q(t)$, the field of rational functions over a finite field with $q$ elements. These arise as the function field of an algebraic curve over a finite a field.

Their completions with respect to nonarchimedean valuations play an important role in number theory. For example $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$. These complete fields, with finite residue class fields, are the first examples of **local fields**, which we define as follows.

**Definition III.1.1.** *A field $K$ is said to be a **local field** if it is complete with respect to a nonarchiemedean discrete valuation and its residue class field is finite.*

If $v$ is the (normalized) valuation of such a field, we usually take as an associated absolute value:

$$|x| = q^{-v(x)}$$

where $q = p^r$ is the number of elements of the residue class field.

The valuation ring is denoted $\mathcal{O}$, with maximal ideal $\mathfrak{p}$, and residue class field $k$, as before.

**Lemma III.1.2.** *The inverse limit $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ is a closed subset of $X = \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$, where each $\mathcal{O}/\mathfrak{p}^n$ have the discrete topology.*

*Proof.* This is a general fact ([12, Ch. IV, §2, page 266]) on inverse limits. We prove it in this case. First note that:

$$\varprojlim_n \mathcal{O}/\mathfrak{p}^n = \bigcap_{n\in\mathbb{N}} X_n$$

where
$$X_n = \left\{ (x_i)_{i\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n \mid \lambda_n(x_{n+1}) = x_n \right\}$$
and $\lambda_n : \mathcal{O}/\mathfrak{p}^{n+1} \to \mathcal{O}/\mathfrak{p}^n$ are the natural projections, which are continuous since each $\mathcal{O}/\mathfrak{p}^n$ is discrete. Now consider the projections $p_i : X \to \mathcal{O}/\mathfrak{p}^i$, which are continuous by the definition of the product topology on $X$. Call $f_n = \lambda_n \circ p_{n+1}$ and $g_n = p_n$. Then
$$X_n = \left\{ x = (x_i)_{i\in\mathbb{N}} \in X \mid f_n(x) = g_n(x) \right\}.$$
The spaces $\mathcal{O}/\mathfrak{p}^n$ have the discrete topology, so they are Haussdorf, which means that $X$ is also Hausdorff. Therefore, $X_n$ is a closed subset of $X$, because $f_n$ and $g_n$ are continuous, hence the equation $f_n(x) = g_n(x)$ defines a closed set in Hausdorff spaces.

Since $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ is an intersection of closed sets, it is itself closed.

□

**Proposition III.1.3.** *A local field $K$ is locally compact. Its valuation ring $\mathcal{O}$ is compact.*

*Proof.* By Proposition I.2.10 $\mathcal{O}$ is isomorphic as a ring and homeomorphic to $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$, with the discrete topology on $\mathcal{O}/\mathfrak{p}^n$. By Proposition I.1.18, we have group isomorphisms $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$ for every $n \geq 1$. Then we have:
$$\frac{\mathcal{O}}{\mathfrak{p}} \times \frac{\mathfrak{p}}{\mathfrak{p}^2} \times \frac{\mathfrak{p}^2}{\mathfrak{p}^3} \times \cdots \times \frac{\mathfrak{p}^{n-1}}{\mathfrak{p}^n} \cong \frac{\mathcal{O}}{\mathfrak{p}^n} \times \frac{\mathfrak{p}}{\mathfrak{p}} \times \frac{\mathfrak{p}^2}{\mathfrak{p}^2} \times \cdots \times \frac{\mathfrak{p}^{n-1}}{\mathfrak{p}^{n-1}} \cong \frac{\mathcal{O}}{\mathfrak{p}^n},$$
which means that $\#\left(\frac{\mathcal{O}}{\mathfrak{p}^n}\right) = \#\left(\frac{\mathcal{O}}{\mathfrak{p}}\right)^n = q^n < \infty$ where $q$ is the cardinality of $k$. Hence for every $n$, $\frac{\mathcal{O}}{\mathfrak{p}^n}$ is compact (since they are finite spaces with the discrete topology). Then, by Tychonov's theorem*, the product $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$ is compact. As a subset of the infinite product, the direct limit $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ is closed by Lemma III.1.2, hence compact. Therefore $\mathcal{O}$ is compact.

For every $a \in K$, the neighbourhood $A = a + \mathcal{O}$ is both open and closed since
$$A = \{x \in K \mid v(x-a) \geq 0\} = \{x \in K \mid |x-a| \leq 1\} \quad (\text{ closed ball})$$
but also, since $|x| = q^{-v(x)}$:
$$A = \{x \in K \mid v(x-a) > -1\} = \{x \in K \mid |x-a| < q\} \quad (\text{ open ball}).$$
We have just used that $v$ is discrete. The same argument shows that in a discretely valued field, every ball is both closed and open.

The translation $A \to \mathcal{O}, x \mapsto x - a$ is clearly a homeomorphism. Which means that $A$ is compact, hence $K$ is locally compact. □

*It states that the product of any collection of compact topological spaces is again compact for the product topology.

**Lemma III.1.4.** *Let $L|K$ be a finite extension of a nonarchimedean valued field $K$ such that the valuation of $K$ extends to $L$, and let $k_L|k_K$ be the extension of their respective residue class fields. Then*

$$[k_L : k_K] \leq [L : K].$$

*In particular, the extension $k_L|k_K$ is finite.*

*Proof.* It suffices to show that if $\overline{x}_1, \dots, \overline{x}_n \in k_L$ are linearly independent over $k_K$ then any choice of preimages $x_1, \dots, x_n \in L$ are linearly independent over $K$. Indeed, if we were to have a non trivial relation $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0, \lambda_i \in K$, then dividing by the coefficient $\lambda_i$ with highest absolute value would yield a nontrivial combination of $x_1, \dots, x_n$ over $K$ that equals 0, with coefficients in $\mathcal{O}_K$ and at least one of the coefficients equals 1. This means that after reducing modulo $\mathfrak{p}_K$ we would obtain a nontrivial linear combination of $\overline{x}_1, \dots, \overline{x}_n$ over $k_K$ equal to 0, which is a contradiction. □

**Theorem III.1.5.** *The local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$, and the fields $\mathbb{F}_{p^r}((t))$ for $r \geq 1$.*

*Proof.* We know that $\mathbb{Q}_p$ and $\mathbb{F}_{p^r}((t))$ are complete. The later is the completion of $\mathbb{F}_{p^r}(t)$ with respect to the valuation associated to the prime ideal $(t)$ of $\mathbb{F}_{p^r}[t]$(Example I.2.9). In both cases, the valuation is discrete. Let $K = \mathbb{Q}_p$ or $\mathbb{F}_{p^r}((t))$. Its residue class field $k_K$ is $\mathbb{F}_p$ or $\mathbb{F}_{p^r}$, respectively. So $K$ is a local field. Now let $L|K$ be a finite extension and $k_L$ the residue class field of $L$. By Theorem I.2.17, $L$ is again complete with respect to the extended valuation $w$, which is again discrete , as we commented earlier, due to the formula

$$w(\alpha) = \frac{1}{n} v\left(N_{L|K}(\alpha)\right)$$

. Furthermore, by Lemma III.1.4, the extension $k_L|k_K$ is finite, and since $k_K$ is finite, so is $k_L$, which means that $L$ is indeed a local field.

Conversely, let $K$ be a local field and $v$ its discrete valuation. Let $p$ be the characteristic of its residue class field $k$, which must be positive since $k$ is finite. There are two cases.

- If $\operatorname{char}(K) = 0$, then $\mathbb{Q} \subset K$. Furthermore, the restriction of $v$ to $\mathbb{Q}$ is equivalent to the $p$-adic valuation $v_p$. To see this first note that $v(p) > 0$ (because $p \equiv 0 \pmod{\mathfrak{p}}$), and $v|_{\mathbb{Q}}$ being a nonarchimedean valuation of $\mathbb{Q}$, it must be equivalent to one of the $q$-adic valuations (Theorem II.3.2), where $q$ is a prime number. Since the only one that assigns a positive value to $p$ is $v_p$, $v$ must be equivalent* to $v_p$. Taking into account that $K$ is complete, the closure of $\mathbb{Q}$ in $K$ is the completion of $\mathbb{Q}$ with respect to $v_p$, i.e. $\mathbb{Q}_p \subset K$. The fact that the extension $K|\mathbb{Q}_p$ is finite follows by a result we will give later (Proposition III.2.7) since $K|\mathbb{Q}_p$ is separable ($\operatorname{char}(K) = 0$). But it also follows from a general result of topological vector spaces ([4, Ch.1, §2, nº4, Theorem 3]), using that $K$ is locally compact by Proposition III.1.3.

*This can also be shown directly. We do not only have $v(p) = s > 0$, but also $v(q) = 0$ for every prime $q \neq p$, since $\operatorname{char}(k) = p$ implies $q \not\equiv 0 \pmod{\mathfrak{p}}$. Using the unique factorization of natural numbers, this yields that $v(n) = s v_p(n)$ in $\mathbb{N}$, hence also in $\mathbb{Z}$. And since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, this extends to $\mathbb{Q}$, showing that $v|_{\mathbb{Q}}$ is equivalent to $v_p$.

- If $\mathrm{char}(K) > 0$ then it has to equal $p$, for if $\mathrm{char}(K) = m$, reducing $\underbrace{1_K + \cdots + 1_K}_{m \text{ times}} = 0$ shows that $p$ divides the prime number $m$, so that $m = p$.

  $k$ is a finite field of characteristic $p$, i.e. $k = \mathbb{F}_p(\overline{\alpha})$ for some $\overline{\alpha}$ algebraic over $\mathbb{F}_p$. Let $f(x) \in \mathbb{F}_p[X]$ be the minimal polynomial of $\overline{\alpha}$ over $\mathbb{F}_p$. $f$ can also be seen as a polynomial in $K[X]$, since $\mathbb{F}_p \subset K$. By Hensel's lemma (I.2.12), we can lift up the root $\overline{\alpha} \in k$ of $f(x)$ to a root $\alpha$ of $f$ over $K$(since $k$ is finite so that $\overline{f}$ is separable and $\overline{\alpha}$ is a simple root. In fact, we can lift to $K$ the entire factorization of $f$ over $k$). This way, we can see $k$ as a subfield of $K$ ($\mathbb{F}_p(\alpha) \subset K$), so $k$ can be its own system of representatives. Now, applying Proposition I.2.8, the elements of $K$ are Laurent series in $t$ with coefficients in $k$, where $t$ is a prime element if $K$ (i.e., $v(t) = 1$). In other words $K = k((t))$. Of course, if $r$ is the degree of $f$, then $K = \mathbb{F}_{p^r}((t))$.

□

We have concluded that the local fields of characteristic 0 are the finite extensions of $\mathbb{Q}_p$, which are called ***p*-adic number fields**. The local fields of characteristic $p$ are the finite extensions of $\mathbb{F}_p((t))$, i.e. the power series fields $\mathbb{F}_{p^r}((t))$ with $r > 1$. We will be more interested in the formers.

To finish this section, we have:

**Proposition III.1.6.** *The multiplicative group of a local field $K$ admits the decomposition:*

$$K^\times = (\pi) \times \mu_{q-1} \times U^{(1)}$$

*where $(\pi) = \left\{\pi^k \mid k \in \mathbb{Z}\right\}, q = \#k$ is the cardinality of the residue class field, $\pi$ is an uniformizant (or prime element of $\mathcal{O}$), $\mu_{q-1}$ is the group of $(q-1)$-roots of unity and $U^{(1)}$ is the group of principal units.*

*Proof.* We can write in a unique way every $\alpha \in K^\times$ as $\alpha = \pi^n u$ with $u \in \mathcal{O}^\times$, which means that

$$K^\times = (\pi) \times \mathcal{O}^\times.$$

Now note that $X^{q-1} - 1$ splits into different linear factors over $k = \mathbb{F}_q$, because this polynomial is relatively prime with its derivative, $x^{q-1} = 1$ for every $x \in \mathbb{F}_q^\times$ and $\#(\mathbb{F}_q^\times) = q - 1$. Then, using Hensel's Lemma (I.2.12), we lift this factorization to $\mathcal{O}$, which shows that $\mathcal{O}^\times$ contains the multiplicative group $\mu_{q-1}$ of $(q-1)$-roots of the unity.

The reduction map $\mathcal{O}^\times \to k^\times, u \mapsto \overline{u} = u \bmod \mathfrak{p}$, is a group morphism that clearly has $U^{(1)}$ as its kernel. Of course, it maps the subgroup $\mu_{q-1} \subset \mathcal{O}^\times$ bijectively onto $k^\times$ since every $x \in \mathbb{F}_q^\times$ is already a $(q-1)$-root of unity, i.e., $k^\times = \mathbb{F}_q^\times \cong \mu_{q-1}$. This implies

$$\frac{\mathcal{O}^\times}{U^{(1)}} \cong k^\times \cong \mu_{q-1} \qquad \text{hence} \qquad \mathcal{O}^\times = \mu_{q-1} \times U^{(1)}$$

and we have our claim. □

## III.2 Ramification

Before delving into this section, we are going to discuss briefly the notion of Henselian field. It will not be strictly necessary to progress, since in Chapter V (our main objective) we will always work with complete fields, but it will allow us to generalize our results to a bigger class of fields.

**Definition III.2.1.** *A* ***Henselian field*** *is a field with a nonarchimedean valuation $v$ whose valuation ring $\mathcal{O}$ satisfies Hensel's Lemma (I.2.12). One also calls the valuation $v$ or the valuation ring $\mathcal{O}$ Henselian.*

Of course, every complete nonarchimedean valued field is Henselian, but we do not require Henselian fields to be complete. Since most results on complete valued fields can be deduced solely from the fact that they satisfy Hensel's lemma, we can broad the range of application of our results by working with the bigger class of Henselian fields.

If $(K, v)$ is any nonarchimedean valued field, and $(\widehat{K}, \widehat{v})$ its completion, we can always find a Henselian field in between: the separable closure $K_v$ of $K$ in $\widehat{K}$. Its valuation ring always verifies Hensel's lemma (see [12, Ch. II,§6, page 143] for more details), although $K_v$ will not, in general, be complete with respect to the extended valuation. $K_v$ will is also called the *Henselization* of $K$.

As an example of the utility of Hensenlian fields, we have the analogous of Theorem I.2.17.

**Theorem III.2.2.** *Let $K$ be a Henselian field with respect to the nonarchimedean absolute value $|\ \ |$. Then $|\ \ |$ can be uniquely extended to any given algebraic extension $L|K$. If $L|K$ has finite degree $n$, then the extension of $|\ \ |$ is given by*

$$|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|}.$$

*The valuation ring of the extended valuation is always the integral closure in $L$ of the valuation ring of $K$.*

*Proof.* In proving Theorem I.2.17, the only place where we directly used that $K$ was complete was to prove that $L$ was again complete. Now, in this version of the theorem, we do not make that claim, because $K$ is not necessarily complete. The rest of Theorem I.2.17 (which is the theorem as stated here), followed only from Hensel's lemma or its corollaries, so there is nothing new to prove here. □

Of course, if $(K, v)$ is Henselian and $L|K$ is an extension of finite degree $n$, the valuation is again extended from $v$ as:

$$w(\alpha) = \frac{1}{n} v(N_{L|K}(\alpha)), \quad \alpha \in L$$

which is obtained taking logarithms in the formula for the extension of the absolute value.

Clearly, Corollary I.2.14 also holds for $K$ Henselian instead of complete, since we only used Hensel's Lemma in order to prove it.

Only as a curiosity, we comment the surprising result that for Henselian fields we have a converse of Theorem III.2.2:

**Theorem III.2.3.** *A nonarchimedean valued field $(K, |\ \ |)$ is Henselian if and only if the absolute value can be uniquely extended to any algebraic extension $L|K$.*

*Proof.* [12, Ch. II, §6, Theorem 6.6, page 147] □

We state now two results of commutative algebra that will come in handy later.

**Proposition III.2.4.** *Let $A$ be an integrally closed domain with field of fractions $K$. Let $L|K$ be a finite separable extension, $B$ the integral closure of $A$ in $L$ and assume that $A$ is a principal ideal domain. Then every finitely generated $B$-submodule $M \neq 0$ is a free $A$-module of rank $[L : K]$.*

*Proof.* [12, Ch. I, Proposition 2.10, page 12] □

**Lemma III.2.5.** ***(Nakayama's Lemma).*** *Let $A$ be a local ring with maximal ideal $\mathfrak{m}$, let $M$ be and $A$-module and $N \subset M$ a submodule such that $M/N$ is finitely generated. Then one has the implication:*

$$M = N + \mathfrak{m}M \implies M = N.$$

*Proof.* There are many different statements of this lemma. The version I am using here is from [12, Ch. I, §11, Exercise 7]. □

**NOTATION:** When working with extensions of nonarchimedean valued fields $L|K$, we will denote by $k_L$ and $k_K$ the residue class fields of $L$ and $K$ respectively. If the valuation $w$ extends the valuation $v$ of $K$ then of course:

$$v(K^\times) \subset w(L^\times) \quad \text{and} \quad k_K \subset k_L.$$

The notation $\mathcal{O}_L, \mathcal{O}_K, \mathfrak{p}_L, \mathfrak{p}_K$ is self-explanatory.

**Definition III.2.6.** *Let $(K, v)$ be a nonarchimedean valued field and $L|K$ an extension such that the valuation $v$ can be extended uniquely to a valuation $w$ of $L$. Then, we define the* ***ramification index*** *of the extension $L|K$ as the index*

$$e = e(w|v) = (w(L^\times) : v(K^\times)).$$

*And the* ***inertia degree*** *is the degree of the extension $k_L|k_K$, i.e.*

$$f = f(w|v) = [k_L : k_K].$$

In particular, the above defintion applies if $K$ is Henselian. If $v$ is discrete, so is $w = \dfrac{1}{n} v \circ N_{L|K}$. In that case and in what follows, $\Pi$ will stand for a prime element of $L$ (an element of $\mathcal{O}_L$ with minimum positive valuation $w(\Pi)$), and $\pi$ for a prime element of $K$. Of course, if $v$ is normalized $v(\pi) = 1$, but this does not mean that $w(\Pi) = 1$, since the inclusion $v(K^\times) \subset w(L^\times)$ may be strict and in that case there are positive values smaller than 1 in $w(K^\times)$. This is measured by the ramification index. Indeed

$$e = 1 \iff v(K^\times) = w(L^\times)$$

and in this case we could take $\Pi := \pi$. But if $e \neq 1$, then $v(K^\times) \subsetneq w(L^\times)$ and $w(\Pi) < v(\pi)$. In general, by definition, we have:

$$e = (w(\Pi)\mathbb{Z} : v(\pi)\mathbb{Z})$$

so that $v(\pi) = ew(\Pi) = w(\Pi^e)$. This means that there exist $u \in \mathcal{O}_L^\times$ such that $\pi = u\Pi^e$. From this we deduce a (maybe more familiar) interpretation of the ramification index: when we extend the ideal $\mathfrak{p} = \pi\mathcal{O}_K$ to $\mathcal{O}_L$, since it must be a power of the ideal $\mathfrak{p}_L$, the ramification index can be defined as the exponent of this power (see [12, Ch. I, §§8 and 9]). In other words:

$$\mathfrak{p}_K\mathcal{O}_L = \pi\mathcal{O}_L = \Pi^e\mathcal{O}_L = \mathfrak{p}_L^e.$$

Sometimes simply written as $\mathfrak{p}_K = \mathfrak{p}_L^e$.

**Proposition III.2.7.** *Let $K$ be a Henselian field and $L|K$ an algebraic extension. Then we have*

$$[L : K] \geq ef$$

*and if $v$ is discrete and $L|K$ separable, the equality holds*

$$[L : K] = ef$$

*and it is called the **fundamental identity**.*

*Proof.* Let $\omega_1, \ldots, \omega_f \in \mathcal{O}_L^\times$ be representatives of a basis of $k_L$ as a $k_K$-vector space. Let $\lambda_1, \ldots, \lambda_e \in L^\times$ such that $w(\lambda_1), \ldots, w(\lambda_e)$ form a system of representatives of the cosets in $w(L^\times)/v(K^\times)$. If $v$ is discrete, we can take $\lambda_i = \Pi^{i-1}, i = 1, ..., e$.

We are going to show that

$$\{\omega_j\lambda_i \mid j = 1, \ldots, f, i = 1, \ldots, e\}$$

is a linearly independent set over $K$ (and later, if $v$ is discrete and $L|K$ is separable, it will even be a basis of $L|K$). So let

$$\sum_{i=1}^{e}\sum_{j=1}^{f} a_{ij}\omega_j\lambda_i = 0, \qquad a_{ij} \in K$$

be a nontrivial $K$-linear combination of the $w_j\lambda_i$, i.e., not all $a_{ij} = 0$. We write this linear combination as

$$\sum_{i=1}^{e} s_i\lambda_i = 0 \quad \text{where} \quad s_i = \sum_{j=1}^{f} a_{ij}\omega_j.$$

The $\omega_j$ are linearly independent over $K$ (see the proof of Lemma III.1.4). Then we see that some of the sums $s_i$ must be nonzero, because otherwise we would have that every $a_{ij} = 0$.

We are going to show that if $s_i \neq 0$, then $w(s_i) \in v(K^\times)$. Indeed, dividing $s_i$ by the coefficient $a_{i\ell}$ of biggest absolute value, we get a linear combination of $\omega_1, \dots, \omega_f$ with coefficients in $\mathcal{O}_K$, one of which equals 1. This means that this linear combination, $s_i/a_{i\ell}$ does not reduces to 0 in $\mathfrak{p}_L$, hence $s_i/a_{i\ell} \in \mathcal{O}_L^\times$. In other words, $w(s_i/a_{i\ell}) = 0$, which means that $w(s_i) = w(a_{i\ell}) \in v(K^\times)$.

Since $\sum_{i=1}^{e} s_i\lambda_i = 0$, there must be at least two nonzero $s_i$ so their terms can cancel out. Also, two of the nonzero summands $\sum_{i=1}^{e} s_i\lambda_i = 0$ must have the same value, because otherwise, using that $w(x) \neq w(y) \implies w(x+y) = \min\{w(x), w(y)\}$, we would have

$$w(0) = w\left(\sum_{i=1}^{e} s_i\lambda_i\right) = \min_{\substack{1\le i\le e \\ s_i\neq 0}} \{w(s_i w_i)\} \neq w(0).$$

So we must have $w(s_i\lambda_i) = w(s_j\lambda_j)$ for some $i \neq j$, which then would imply

$$w(\lambda_i) = w(\lambda_j) + w(s_j) - w(s_i) \equiv w(\lambda_j) \pmod{v\left(K^\times\right)}$$

a contradiction with our election of $\lambda_1, ..., \lambda_f$. This shows that the $\omega_j\lambda_i$, for $i = 1, \dots, e, j = 1, \dots, f$, are linearly independent over $K$, which means that

$$[L : K] \geq ef.$$

Now assume that $v$ is discrete and $L|K$ separable. We construct the $\mathcal{O}_K$-module

$$M = \sum_{i=1}^{e}\sum_{j=1}^{f} \omega_j\lambda_i\mathcal{O}_K.$$

To show that these $\omega_j\lambda_i$ form a basis of $L$ over $K$, it suffices to show that $M = \mathcal{O}_L$ (i.e., the $\omega_j\lambda_i$ form a system of generators of $\mathcal{O}_L$), since then the result follows by passing to the fields of fractions.

As we commented earlier, in this case we can choose $\lambda_i = \Pi^{i-1}$. We have the $\mathcal{O}_K$-submodule of $M$

$$N = \sum_{i=1}^{e} \mathcal{O}_K\omega_j$$

verifying $M = N + \Pi N + \cdots + \Pi^{e-1}N$. Since the $\omega_j$ are a basis of $k_L = \mathcal{O}_L/\Pi\mathcal{O}_L$ over $k_K$, every $x \in \mathcal{O}_L$ can be written as

$$x \equiv \underbrace{a_1\omega_1 + \cdots + a_f\omega_f}_{\in N} \pmod{\Pi\mathcal{O}_L}, \quad a_i \in \mathcal{O}_K.$$

This then implies that $\mathcal{O}_L = N + \Pi\mathcal{O}_L$, and successively substituting this equation into itself we get:

$$\mathcal{O}_L = N + \Pi(N + \Pi\mathcal{O}_L) = \cdots = N + \Pi N + \cdots + \Pi^{e-1}N + \Pi^e\mathcal{O}_L = M + \Pi^e\mathcal{O}_L.$$

We have proven that $\mathcal{O}_L = M + \mathfrak{p}_L^e = M + \mathfrak{p}_K\mathcal{O}_L$. The extension $L|K$ being separable implies that $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module (apply Proposition III.2.4 to $B = \mathcal{O}_L, M = \mathcal{O}_L, A = \mathcal{O}_K$. All hypothesis are easily satisfied). Then, Nakayama's Lemma* (Lemma III.2.5) implies that $\mathcal{O}_L = M$. □

**Remark III.2.8.** In the above result, when $v$ is discrete we can drop the condition of $L|K$ being separable and replace it with $K$ being complete. In this case, in the above proof we would deduce that $M = \mathcal{O}_L$ from $\mathcal{O}_L = N + \mathfrak{p}_K\mathcal{O}_L$ not by means of Nakayama's Lemma, but using that for every $i \geq 1$ we have $\mathfrak{p}_K^i M \subset M$ which then implies:

$$\mathcal{O}_L = M + \mathfrak{p}_K(M + \mathfrak{p}_K\mathcal{O}_L) = M + \mathfrak{p}_K^2\mathcal{O}_L = \cdots = M + \mathfrak{p}_K^m\mathcal{O}_L$$

for every $m \geq 1$, and since $\{\mathfrak{p}_K^m\mathcal{O}_L\}_{m\in\mathbb{N}}$ is a basis of neighbourhoods of 0 in $\mathcal{O}_L$, this last equation shows that $M$ is dense in $\mathcal{O}_L$. By Proposition I.2.15, $L \cong K^n$, where $n = \dim_K(L)$, the isomorphism being also a homeomorphism. Since $\mathcal{O}_K$ is closed in $K$ and $M \cong \mathcal{O}_K^n$ (by construction), we see that $M$ is closed in $K^n$. This implies that $M$ is closed in $\mathcal{O}_L$, so that $M = \mathcal{O}_L$.

We know that every algebraic extension of a field of characteristic zero or a finite field is separable. So most extensions that we will encounter will be separable. In the above proposition, if $K = \mathbb{Q}$ or $K = \mathbb{Q}_p$ with one of the $p$-adic valuations, then the fundamental identity holds.

**For the rest of the section,** $K$ **will be Henselian** unless stated otherwise, so that its valuation can be uniquely extended to any algebraic extension $L|K$ and sometimes we will use Hensel's Lemma and its consequences.

**Proposition III.2.9.** *Let $\overline{K}$ be an algebraic closure of $(K, v)$. Then the residue class field $k_{\overline{K}} = \frac{\mathcal{O}_{\overline{K}}}{\mathfrak{p}_{\overline{K}}}$ of $\overline{K}$ is algebraically closed, so it is an algebraic closure of the residue class field $k_K = \frac{\mathcal{O}_K}{\mathfrak{p}_K}$ of $K$.*

*Proof.* Let $v$ be the valuation of $K$ and $w$ its extension to $\overline{K}$. Let $\overline{p}(x) \in k_{\overline{K}}[x]$ be any polynomial, $\overline{p}(x) = \sum_{i=0}^n \overline{a_i}x^i$, where $\overline{a_i} \in k_{\overline{K}}, \overline{a_n} \neq 0$. Then lift this polynomial to some $p(x) = \sum_{i=0}^n a_i x^i \in \mathcal{O}_{\overline{K}}[x]$. In particular, each $\overline{a_i} \neq 0$ is lifted to some $a_i \in \mathcal{O}_{\overline{K}}^\times$ and if $\overline{a_i} = 0$, then $a_i = 0$. Since $\overline{K}$ is algebraically closed, there exists $\alpha \in \overline{K}$ such that $p(\alpha) = 0$. Let us see that $\alpha \in \mathcal{O}_{\overline{K}}$. By dividing the equation $p(\alpha) = 0$ by $\alpha^{n-1}$ we get:

$$a_n\alpha = -\left(a_{n-1} + a_{n-2}\alpha^{-1} + \cdots + a_0\alpha^{-n+1}\right).$$

*Of course, if $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module, so is $\mathcal{O}_L/M$, so that we can apply our version of Nakayama's Lemma.

If $w(\alpha) < 0$, since $a_n \in \mathcal{O}_{\overline{K}}^{\times}$, we would have

$$0 > w(\alpha) = w(a_n\alpha) = \min\{-w(\alpha), \dots, -(n-1)w(\alpha)\} = -w(\alpha) \geq 0!!!$$

so it must be $w(\alpha) \geq 0$. Then reducing $\alpha$ modulo $p$ yields a root $\overline{\alpha} \in k_{\overline{K}}$ of $\overline{p}(x)$, which finishes the proof. □

**Definition III.2.10.** *A finite extension $L|K$ is called* ***unramified*** *if the extension of the residue class fields $k_L|k_K$ is separable and:*

$$[L : K] = [k_L : k_K].$$

*An arbitrary algebraic extension $L|K$ is called unramified if it is the union of finite unramified extensions.*

It is not strictly necessary in the above definition for $K$ to be Henselian. It suffices that its valuation extends uniquely to $L$.

From Proposition III.2.7 and the remark that follows it, if $K$ is a local field and $L|K$ is an algebraic extension, then the fundamental identity holds, since the valuation in the complete field $K$ is discrete.

In general, if the fundamental identity $[L : K] = ef$ holds for an algebraic extension $L|K$ and $k_L|k_K$ is separable, we have

$$L|K \text{ is unramified } \iff e(L|K) = 1$$

which is a more direct definition. As commented above, this holds for extensions of local fields, or also for any field complete with respect to a nonarchimedean discrete valuation. In general, the implication that we always have is:

$$L|K \text{ is unramified } \implies e(L|K) = 1$$

since, restricting ourselves to finite extensions, we see that

$$[L : K] \geq e[k_L : k_K] = e[L : K] \implies e = 1.$$

**Lemma III.2.11.** *Let $(K, |\ \ |)$ be Henselian and let $L|K$ be an algebraic extension. Then for every $\alpha \in \mathcal{O}_L$, the minimal polynomial $f(x) \in K[x]$ of $\alpha$ over $K$ is in fact in $\mathcal{O}_K[x]$.*

*Proof.* Let $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$ be the (monic) minimal polynomial of $\alpha \in \mathcal{O}_L$ over $K$. Corollary I.2.14 (which as we comented also holds for Henselian fields), tells us that

$$|f| = \max\{|a_n|, |a_0|\} = \max\{1, |a_0|\}.$$

This in particular shows that $|a_j| \leq 1$ for $j = 1, ..., n$, i.e, $|a_j| \in \mathcal{O}_K \subset \mathcal{O}_L$ for $j = 1, ..., n$. But then, since $f(\alpha) = 0$, we have:

$$a_0 = -\left(a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n\right) \in \mathcal{O}_L$$

so that $a_0 \in K \cap \mathcal{O}_L = \mathcal{O}_K$, hence $f(x) \in \mathcal{O}_K[x]$. □

Recall that if $L|K$ and $F|K$ are two extensions, then the product $LF$ is the smallest extension of $K$ that contains both $L$ and $F$.

**Proposition III.2.12.** *Let $L|K$ and $F|K$ be two extensions inside an algebraic closure $\overline{K}|K$ and let $E = LF$. Then one has*

$$L|K \text{ unramified} \implies E|F \text{ unramified.}$$

*Proof.* Let $L|K$ be such an unramified extension. We can asume that $L|K$ is finite, otherwise it would be a union of finite unramified extensions and we could do the same reasoning we are about to do with each of those. Then $k_L|k_K$ is finite (Lemma III.1.4), and separable by hypothesis. Therefore, by the Primitive Element Theorem, there exists $\overline{\alpha} \in k_L$ such that $k_L = k_K(\overline{\alpha})$. Lift $\overline{\alpha}$ to some $\alpha \in \mathcal{O}_L^\times$, and let $f(x) \in \mathcal{O}[x]$ the minimal (monic) polynomial of $\alpha$ over $K$ (Lemma III.2.11). Then let $\overline{f}(x) \in k_K[x]$ be the reduction of $f$ modulo $\mathfrak{p}_K$. Of course, $[k_L : k_K] \le \deg(\overline{f})$ since $\overline{f}(\alpha) = 0$ (so that the minimal polynomial of $\overline{\alpha}$ over $k_K$ divides $\overline{f}$), and also $\deg(\overline{f}) = \deg(f)$. We then have

$$[k_L : k_K] \le \deg(\overline{f}) = \deg(f) = [K(\alpha) : K] \le [L : K] = [k_L : k_K]$$

so that all inequalities are in fact equalities. In particular, we have $L = K(\alpha)$. This implies that $E = F(\alpha)$: from $\alpha \in L \subset E, F \subset E$, we see that $F(\alpha) \subset E$, and $F \subset F(\alpha), L = K(\alpha) \subset F(\alpha)$ implies that $E = LF \subset F(\alpha)$.

We still need to show that $E|F$ is unramified. Let $g(x) \in \mathcal{O}_F[x]$ be the minimal polynomial of $\alpha$ over $F$, and $\overline{g}(x) \in k_F[x]$ the reduction of $g$ modulo $\mathfrak{p}_F$. Since $f(x)$, regarded as a polynomial in $F[x]$, satisfies $f(\alpha) = 0$, $g(x)$ must be a factor of $f(x)$. This implies that $\overline{g}(x)$ must be a factor of $\overline{f}(x)$, so that $\overline{g}(x)$ is separable. $\overline{g}(x)$ is also irreducible over $k_F$, since otherwise, by Hensel's Lemma, $g(x)$ would be reducible over $F$, hence $g(x)$ is the minimal polynomial of $\overline{\alpha}$ over $k_F$. We then have

$$[k_E : k_F] \overset{III.1.4}{\le} [E : F] = \deg(g) = \deg(\overline{g}) = [k_F(\overline{\alpha}) : k_F] \le [k_E : k_F]$$

so that again all inequalities are equalities. In particular $[E : F] = [k_E : k_F]$ and $k_E = k_F(\overline{\alpha})$ (so $k_E|k_F$ is separable), hence $E|F$ is unramified. □

**Corolary III.2.13.** *Each subextension of an unramified extension is unramified.*

*Proof.* Let $L'|K$ be a subextension of the unramified extension $L|K$. The above proposition, for $F = L', E = LL' = L$, tells us that $L|L'$ is unramified, so that $[k_L : k_{L'}] = [L : L']$. Then:

$$[k_L : k_K] = [L : K] = [L : L'][L' : K] = [k_L : k_{L'}][L' : K]$$

but also

$$[k_L : k_K] = [k_L : k_{L'}][k_{L'} : k_K].$$

These two equations together show that $[L' : K] = [k_{L'} : k_K]$, and since $k_{L'}|k_K$ is a subextension of $k_L|k_K$, the extension $k_{L'}|k_K$ is also separable, thus $L'|K$ is unramified. □

**Corolary III.2.14.** *The composite of two unramified extensions of $K$ is again unramified.*

*Proof.* Let $L|K$ and $L'|K$ be two unramified extensions. Since both are the composite of finite unramified subextensions, $LL'$ is also the composite of finite unramified subextensions of $LL'|K$. This means, by Definition III.2.10, that it suffices prove the result in the case where $L|K$ and $L'|K$ are finite extensions.

If $L|K$ is unramified, so is $LL'|L'$ by Proposition III.2.12. Then, since we are dealing with finite extensions, we have

$$[LL' : K] = [LL' : L'][L' : K] = [k_{LL'} : k_{L'}][k_{L'} : k_K] = [k_{LL'} : k_K]$$

and $k_{LL'}|k_K$ is separable by the transitivity of separability, so that $LL'|K$ is unramified. □

The last result allows to define:

**Definition III.2.15.** *Let $L|K$ be an algebraic extension. Then the composite $T|K$ of all unramified subextensions of $L|K$ is called the* ***maximal unramified subextension*** *of $L|K$.*

When $L = \overline{K}$, it is denoted $K^{nr}$ ($nr$ stands for "*non ramifiée*") and called the **maximal unramified extension** of $K$.

**Proposition III.2.16.** *Let $T$ be the maximal unramified subextension of $L|K$. Then the residue class field of $T$ is $k_s$, the separable closure of $k_K$ in $k_L$. The value group of $T$ equals that of $K$.*

*Proof.* Let $k_s$ be the separable closure of $k_K$ in $k_L$ and $k_T$ be the residue class field of $T$. $k_T|k_K$ is the composite of the separable residue class field extensions $k_{K'}|k_K$, where $K'|K$ ranges over all unramified subextensions of $L|K$, so it follows that $k_T|k_K$ is a separable subextension of $k_L|k_K$, hence $k_T \subset k_s$.

Conversely, let $\overline{\alpha} \in k_L$ be separable over $k_K$. We have to show that $\overline{\alpha} \in k_T$. Let $\overline{f}(x) \in k_K[x]$ the minimal polynomial of $\overline{\alpha}$ over $k_K$. Let $f(x) \in \mathcal{O}_K[x]$ be a monic polynomial that reduces to $\overline{f}$ modulo $\mathfrak{p}_K$. Since it preserves its degree in the reduction, $f(x)$ is irreducible (for if $f(x)$ is the product of two nontrivial factors, so is $\overline{f}$ after the reduction). Then by Hensel's Lemma there exists $\alpha \in L$ such that $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{p}_L}$ and $f(\alpha) = 0$, so $f$ is the minimal polynomial of $\alpha$. Therefore,

$$[K(\alpha) : K] = [k_K(\overline{\alpha}) : k_K]$$

$k_K(\overline{\alpha}) = k_{K(\alpha)}$ is the residue field of $K(\alpha)$ and since $\overline{\alpha}$ is separable so is the extension $k_K(\overline{\alpha})|k_K$. This implies that $K(\alpha)|K$ is unramified, so that $K(\alpha) \subset T$, hence $\overline{\alpha} \in k_T$.

Finally, let $v$ be the valuation of $K$ and $w$ the valuation of $T$ extending $v$. In order to prove that $w(T^\times) = v(K^\times)$ we may suppose that $L|K$ is finite (since each element of $T^\times$ is in some finite subextension of $L|K$). Then

$$[T : K] \overset{III.2.7}{\geq} \left(w\left(T^\times\right) : v\left(K^\times\right)\right)[k_T : k_K] = \left(w\left(T^\times\right) : v\left(K^\times\right)\right)[T : K]$$

so that $(w(T^\times) : v(K^\times)) = 1$. □

There are other notions accompanying that of an unramified extension: *tamely ramified, wildly ramified, totally (or purely) ramified,...* We will not use them in this text. Nevertheless, is worth mentioning something about the first one, which is defined only when $\mathrm{char}(k_K)$ is positive.

**Definition III.2.17.** *An algebraic extension $L|K$, with maximal unramified subextension $T|K$, is called* ***tamely ramified*** *if*

1. $\mathrm{char}(k_K) = p > 0$.

2. *The extension $k_L \mid k_K$ of the residue class fields is separable.*

3. $([L : T], p) = 1$.

*In the infinite case, this latter condition is taken to mean that the degree of each finite subextension of $L|T$ is prime to $p$.*

**Proposition III.2.18.** *A finite extension $L \mid K$, with maximal unramified subextension $T|K$, is tamely ramified if and only the extension $L|T$ is generated by radicals*

$$L = T\left( \sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r}\right)$$

*such that $(m_i, p) = 1$. In this case the fundamental identity always holds:*

$$[L : K] = ef$$

*Proof.* [12, Ch. II, Proposition 7.7, page 155] □

We have analogous to Proposition III.2.12 and Corollary III.2.14.

**Corolary III.2.19.** *Let $L|K$ and $K'|K$ be two extensions inside the algebraic closure $\overline{K}|K$, and $L' = LK'$. Then we have:*

$$L|K \text{ tamely ramified } \Longrightarrow L'|K' \text{ tamely ramified}$$

*Every subextension of a tamely ramified extension is tamely ramified.*

*Proof.* [12, Ch. II, Proposition 7.8, page 156] □

**Corolary III.2.20.** *The composite of tamely ramified extensions is tamely ramified.*

*Proof.* [12, Ch. II, Proposition 7.9, page 157] □

We can also define the **maximal tamely ramified subextension** $V|K$ of an algebraic extension $L|K$ as the composite of every tamely ramified subextension of $L|K$.

## III.3 The Inertia subgroup

In Chapter V, to prove the Néron-Ogg-Shafarevich Criterion, we will work with a field $K$ complete with respect to a nonarchimedean discrete valuation $v$. In particular, the valuation can be extended uniquely to any algebraic extension $L|K$, and the fundamental identity III.2.7 holds. We will also require for $K$ and its residue class field to be perfect, so that their algebraic extensions are separable. Nevertheless, most of the the time, this last condition of $K$ and $k_K$ being perfect will not be needed.

Of course, local fields satisfy the previous conditions. In practice, most results will be applied to local fields, in particular to $\mathbb{Q}_p$ and its finite extensions.

If $E|F$ is an algebraic field extension, we will use the notation $\mathrm{Aut}_F(E)$ for the group of automorphism of $E$ that fix $K$ pointwise. $E|F$ is a Galois extension if it is normal and separable, and in this case we write $\mathrm{Aut}_F(E) = \mathrm{Gal}(E/F)$. If $E|F$ is finite, other well known equivalent conditions for the extension $E|K$ to be Galois are:

- $\# \mathrm{Aut}_F(E) = [E : F]$.
- $F$ is the fixed field of $\mathrm{Aut}_F(E)$.

**Remark III.3.1.** We are going to work with Galois extensions that are not necessarily finite. Therefore, it is necessary to understand the basics of infinite Galois theory. The reference I used to introduce myself to this topic was [12, Ch. IV, §1, pages 261-264]. As a brief overview, if $L|K$ is an infinite Galois, then the fundamental theorem of (finite) Galois theory concerning the 1-1 correspondence between subgroups of $\mathrm{Gal}(L/K)$ and the intermediate extensions of $L|K$, ceases to hold, because there are more subgroups than intermediate fields. To salvage this, one considers a canonical topology on the group $\mathrm{Gal}(L/K)$, called the **Krull topology**. It is defined by assigning to each $\sigma \in \mathrm{Gal}(L/K)$ the (local) basis of neighbourhoods $\sigma\,\mathrm{Gal}(L/M)$, where $M|K$ ranges over the finite Galois subextensions of $L|K$. (If $L|K$ were to be finite, then the finite group $\mathrm{Gal}(L|K)$ turns into a discrete topological group). The elements of $\sigma\,\mathrm{Gal}(L/M)$ are simply the $K$-automorphisms of $L$ that behave as $\sigma$ over $M$. This topology turns $\mathrm{Gal}(L/K)$ **into a compact Hausdorff space** ([12, Ch. IV, Proposition 1.1, page 262]). Then the fundamental theorem of (infinite) Galois theory can be stated as:

**Theorem III.3.2.** *Let $L|K$ be a (finite or infinite) Galois extension. Then the assigment*

$$F \longmapsto \mathrm{Gal}(L/F)$$

*is a 1-1 correspondece between the subextensions $F|K$ of $L|K$ and the closed subgroups of $\mathrm{Gal}(L/K)$. The open subgroups of $\mathrm{Gal}(L/K)$ correspond precisely to the finite subextensions of $L|K$.*

*Proof.* [12, Ch. IV, Theorem 1.2, page 263] □

**Throughout this entire section, $L|K$ will be a Galois extension (finite or infinite)** of a Henselian field $(K, v)$. In particular, the valuation $v$ can be uniquely extended to a valuation $w$ of $L$. If the extension of the valuation was not unique, a slight modification of the theory that follows would be needed, which implies working with the **decomposition group**[*] instead of the whole $\mathrm{Gal}(L/K)$ (see [12, Ch.2, §8 & §9]). Nevertheless, our scarce results on the inertia group will only be applied to fields as mentioned at the beginning of this section, so this generality is sufficient. The extension $\overline{K}|K$ should be our main focus.

**NOTATION:** $G := \mathrm{Gal}(L/K)$ will be the Galois group of the Galois extension $L|K$.

**Proposition III.3.3.** *For every $\sigma \in G$ we have*

$$w \circ \sigma = w.$$

*Proof.* Since $L|K$ is the composite of its finite Galois subextensions, if we prove the result when $L|K$ is finite, we would have proven it in general. If $[L : K] = n$ is finite, we have a formula for the extension $w$ (Theorem III.2.2).

$$w(\alpha) = \frac{1}{n} v(N_{L|K}(\alpha)) \quad \text{for every} \quad \alpha \in L^\times.$$

Let $\sigma \in G$. Of course, $w(x) = w(\sigma x)$ for every $x \in K$. Since $L|K$ is Galois, we have:

$$N_{L|K}(x) = \prod_{\delta \in G} \delta x.$$

This implies that $N_{L|K}(\alpha) = N_{L|K}(\sigma\alpha)$, for if $\delta$ ranges through $G$, so does $\delta\sigma$. Therefore we have $w(\alpha) = w(\sigma\alpha)$, as we wanted.

□

The last proposition also shows that every $\sigma \in G$ is a **continuous** map $L \to L$.

**Definition III.3.4.** *The inertia group of $L|K$ is*

$$I_w = I_w(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma x \equiv x \pmod{\mathfrak{p}_L} \ \ \forall x \in \mathcal{O}_L\}.$$

In other words, the elements of the inertia group $I_w$ are the $\sigma \in \mathrm{Gal}(L/K)$ that act as the identity in the residue class field $k_L$ (this is precised below). It is clearly a subgroup of $G$. Recall that $w$ stands for the extended valuation of $L$.

We have $w = w \circ \sigma$ for every $\sigma \in G$ (Proposition III.3.3), hence $\sigma\mathcal{O}_L = \mathcal{O}_L$ and $\sigma\mathfrak{p}_L = \mathfrak{p}_L$. This immediately implies that every $\sigma \in G$ induces a well defined ring endomorphism of $k_L$:

$$\overline{\sigma} : \mathcal{O}_L/\mathfrak{p}_L \longrightarrow \mathcal{O}_L/\mathfrak{p}_L, \quad x \bmod \mathfrak{p}_L \longmapsto \sigma x \bmod \mathfrak{p}_L.$$

We have just described a **canonical group morphism** from $G$ to $\mathrm{Aut}_{k_K}(k_L)$:

$$\varphi : \mathrm{Gal}(L/K) \to \mathrm{Aut}_{k_K}(k_L), \qquad \sigma \longmapsto \overline{\sigma}$$

whose kernel is clearly $I_w$.

[*] For an extension $w$ of $v$, the decomposition group is defined as

$$G_w = G_w(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid w \circ \sigma = w\}$$

When $K$ is Henselian, $G_w = \mathrm{Gal}(L/K)$ as Proposition III.3.3 shows.

**Proposition III.3.5.** *$I_w = I_w(L/K)$ is a closed subgroup of $G = \mathrm{Gal}(L/K)$.*

*Proof.* Let $\sigma \in G$ be an element of the closure of $I_w$. This means that for every finite Galois subextension $M|K$ of $L$ there is some $\delta_M \in I_w \cap \sigma \, \mathrm{Gal}(L/M)$, because $\sigma \, \mathrm{Gal}(L/M)$ is a neighbourhood of $\sigma$. Since $\delta_M \in \sigma \, \mathrm{Gal}(L/M)$, we have $\delta_M|_M = \sigma|_M$. Therefore

$$\sigma x = \delta_M x \equiv x \pmod{\mathfrak{p}_L} \text{ for every } x \in M \cap \mathcal{O}_L$$

and this holds for every finite Galois subextension $M|K$. Since every $x \in L$ is in at least one of these finite extensions $M$, the last equations yields

$$\sigma x \equiv x \pmod{\mathfrak{p}_L} \text{ for every } x \in \mathcal{O}_L.$$

which means that $\sigma \in I_w$. □

**Proposition III.3.6.** *Let $L|K$ be a Galois extension. Then $k_L|k_K$ is a normal extension.*

*Proof.* Let $\overline{\theta} \in k_L$ and let $\theta \in \mathcal{O}_L$ be a representative. Let $f(x) \in \mathcal{O}_K[X]$ be the minimal polynomial of $\theta$ over $K$ and $\overline{g}(x) \in k_K[x]$ the minimal polynomial of $\overline{\theta}$ over $k_K$. Reducing $f(\theta) = 0$ modulo $\mathfrak{p}_K$ we see that $\overline{f}(\overline{\theta}) = 0$, which means that $\overline{g}(x)$ divides $\overline{f}(x)$. Since $L|K$ is normal, $f(x)$ splits into lineal factors in $\mathcal{O}_L[x]$, and reducing modulo $\mathfrak{p}_K$ we see that $\overline{f}(x)$ also splits into linear factors over $k_K$ (and the same quantity because $\deg(f) = \deg(\overline{f})$). Thus, the same is true for $\overline{g}(x)$. This shows that $k_L|k_K$ is a normal extension. □

At this point is better to assume for the rest of the chapter that the extension $k_L|k_K$ is separable. This is the only thing that we need for this extension to be Galois, as the previous proposition shows. It is the case, for example, if $k_K$ is perfect or $L|K$ is unramified.

Our aim is to obtain an exact sequence:

$$1 \longrightarrow I_w \longrightarrow \mathrm{Gal}(L/K) \xrightarrow{\varphi} \mathrm{Gal}(k_L/k_K) \longrightarrow 1.$$

The only thing that remains to be shown is the surjectivity of $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$, but first we need to show that it is a continuous map.

**Proposition III.3.7.** *The canonical morphism $\varphi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(k_L/k_K), \sigma \to \overline{\sigma}$ is continuous.*

*Proof.* Let $\overline{\theta} \in k_L$, and let $\theta \in \mathcal{O}_L$ be a representative. Recall then that $\varphi(\sigma)$ is defined as $\varphi(\sigma)\overline{\theta} := \sigma\theta \mod \mathfrak{p}_L$.

Since $\mathrm{Gal}(k_L/k_K)$ is a topological group, it suffices to show that the preimage of a fundamental neighbourhood of $id_{k_L}$ is open, i.e. we want to see that $\varphi^{-1}(\mathrm{Gal}(k_L/\mu))$ is an open set of $\mathrm{Gal}(L/K)$, where $\mu|k_K$ is a finite subextension of $k_L|k_K$. The minimal polynomial over $k_K$ of every element of $\mu$ must be separable, because $k_L|k_K$ is separable. By the Primitive Element Theorem, there exists $\overline{\alpha} \in \mu \setminus k_K$ such that $\mu = k_K(\alpha)$. Let

$\overline{g}(x) \in k_K[x]$ be its minimal polynomial over $K$, which must be separable, and lift it to a monic polynomial $g(x) \in \mathcal{O}_K[x]$ of the same degree. $g(x)$ must be irreducible, since otherwise, after reducing modulo $k_K$, $\overline{g}(x)$ would be reducible. By Hensel's lemma, there exists a unique root $\alpha \in \mathcal{O}_L$ of $g(x)$ such that $\alpha \cong \overline{\alpha} \pmod{\mathfrak{p}_L}$ (The root $\alpha$ must be unique since otherwise, after reducing, the root $\overline{\alpha}$ of $\overline{g}(x)$ would not be simple, contradicting the fact that $\overline{g}$ is separable). Therefore, $g(x)$ is the minimal polynomial of $\alpha$ over $K$. Define $F = K(\alpha)$, which is a finite (unramified) extension of degree $[F : K] = [\mu : k_K]$. We are going to show that $\varphi^{-1}(\mathrm{Gal}(k_L/\mu)) = \mathrm{Gal}(L/F)$

Let $\sigma \in \mathrm{Gal}(L/K)$ and note that $\sigma \in \varphi^{-1}(\mathrm{Gal}(k_L/\mu))$ if and only if $\varphi(\sigma)$ is the identity over $\mu = k_K(\alpha)$, i.e. if and only if $\sigma(\alpha) \cong \alpha \pmod{\mathfrak{p}_L}$. Now, if $\sigma \in \mathrm{Gal}(L/F)$, then $\sigma\alpha = \alpha$, and hence $\sigma \in \varphi^{-1}(\mathrm{Gal}(k_L/\mu))$. Conversely, let $\sigma \in \varphi^{-1}(\mathrm{Gal}(k_L/\mu))$, so that $\sigma(\alpha) \cong \alpha \pmod{\mathfrak{p}_L}$. Then $\sigma\alpha = \gamma$, where $\gamma$ is a root of $g(x)$. We must have $\gamma = \alpha$, because otherwise, there would be two different roots of $g$ that reduce to $\overline{\alpha}$ , which is not possible since, as we said before, $\overline{\alpha}$ can be lifted to only one root of $g$.

□

As a curiosity, the following result is also true if $k_L|k_K$ is not separable (see [12, Ch. I, Proposition 9.4]), using $\mathrm{Aut}_{k_K}(k_L)$ instead of $\mathrm{Gal}(L/K)$, though we will not need this observation.

**Proposition III.3.8.** *If $L|K$ is a Galois extension and $k_L|k_K$ is separable, the canonical morphism*

$$\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$$

*is surjective. It is also injective (hence a isomorphism) if $L|K$ is unramified.*

*Proof.* Le us first deal with the finite case. If $L|K$ is finite, so is $k_L|k_K$ by Lemma III.1.4. Let $\delta \in \mathrm{Gal}(k_L|k_K)$. By the Primitive Element Theorem, there exists $\overline{\theta} \in k_L$ such that $k_L = k_K(\overline{\theta})$. Let $\overline{g}(x) \in k_K[x]$ the minimal polynomial of $\overline{\theta}$ over $k_K$, of degree $f = [k_L : k_K] = \#\,\mathrm{Gal}(k_L|k_K)$. Let $g(x) \in \mathcal{O}_K[x]$ be a monic polynomial of the same degree that reduces to $\overline{g}$ modulo $\mathfrak{p}_K$. $g(x)$ must be irreducible over $K$ since otherwise $\overline{g}(x)$ would be reducible. Hensel's Lemma allows us to lift the root $\overline{\theta} \in k_L$ of $\overline{g}(x)$ to a root $\theta \in \mathcal{O}_L$ of $g(x)$. We can do the same with the root $\delta\overline{\theta}$ of $\overline{g}$, lifting it to a root* $\theta' \in \mathcal{O}_L$ of $g$. There exist $\sigma \in \mathrm{Gal}(L/K)$ such that $\theta' = \sigma\theta$. Reducing modulo $\mathfrak{p}_L$, this means that

$$\varphi(\sigma)\overline{\theta} = \overline{\sigma\theta} = \overline{\theta'} = \delta\overline{\theta}$$

hence $\delta = \varphi(\sigma)$. This shows that $\varphi$ is surjective. Moreover, if $L|K$ is unramified then

$$\#\,\mathrm{Gal}(L/K) = [L : K] = [k_L : k_K] = \#\,\mathrm{Gal}(k_L/k_K)$$

which forces $\varphi$ to be injective and an isomorphism.

Now suppose that $L|K$ is an infinite Galois extension. In order to prove the surjectivity of $\varphi : G \to \mathrm{Gal}(k_L/k_K)$ it suffices to show that $\varphi(G)$ is dense in $\mathrm{Gal}(k_L/k_K)$,

*At this point it should be obvious that the $f$ roots of $g$ are in bijection with the $f$ roots of $g'$, since $\overline{g}$ splits into different linear factors over $k_L[x]$ and we can lift them to different factors of $g$.

because $\varphi(G)$, being the continuous image of a compact space, is itself a compact subset of $\mathrm{Gal}(k_L/k_K)$, hence closed since $\mathrm{Gal}(k_L/k_K)$ is Hausdorff. Let $\delta \in \mathrm{Gal}(k_L/k_K)$ and $\lambda|k_K$ be a finite Galois subextension of $k_L|k_K$, so that $\delta \,\mathrm{Gal}(k_L/\lambda)$ is a neighbourhood of $\delta$. All we have to prove is that this neighbourhood contains the image $\varphi(\sigma)$ of some $\sigma \in G$. Let $M|K$ be a finite subextension of $L|K$ whose residue class field $k_M$ contains $\lambda$. By the finite case we proved earlier, the canonical map $\mathrm{Gal}(M/K) \to \mathrm{Gal}(k_M/k_K)$ is surjective. Therefore, the composite:

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(k_M/k_K) \longrightarrow \mathrm{Gal}(\lambda/k_K)$$

is surjective, since all three maps are surjective. The first and last maps are induced by restrictions. For example $\alpha \in \mathrm{Gal}(L/K) \mapsto \alpha|_M \in \mathrm{Gal}(M/K)$, which are clearly surjective*. Call $\psi$ the above composition. There must exist some $\sigma \in \mathrm{Gal}(L/K)$ such that $\psi(\sigma) = \delta|_\lambda \in \mathrm{Gal}(\lambda/k_K)$. Since $\psi(\sigma) = \overline{\sigma}|_\lambda$, this means that $\varphi(\sigma) \in \delta \,\mathrm{Gal}(k_L/\lambda)$ ($\varphi(\sigma) = \overline{\sigma}$ is a $k_K$-automorphism of $k_L$ that behaves as $\delta$ on $\lambda$, and these are precisely the elements of $\delta \,\mathrm{Gal}(k_L/\lambda)$).

If $L|K$ is unramified, it is the union of finite unramified extensions. Injectivity of $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K)$ holds again thanks to the finite case: Assume there are $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$, $\sigma_1 \neq \sigma_2$ and $\varphi(\sigma_1) = \varphi(\sigma_2)$. Let $M|K$ be a finite unramified Galois subextension of $L|K$ such that $\sigma_1|_M \neq \sigma_2|_M$. Then, by the finite case,

$$\varphi_M : \mathrm{Gal}(M/K) \to \mathrm{Gal}(k_M|k_K)$$

is injective, which is a contradiction since then

$$\varphi(\sigma_1)|_{k_M} = \varphi_M(\sigma_1|_M) \neq \varphi_M(\sigma_2|_M) = \varphi(\sigma_2)|_{k_M}.$$

□

We now have the short exact sequence:

$$1 \longrightarrow I_w(L/K) \longrightarrow \mathrm{Gal}(L/K) \xrightarrow{\varphi} \mathrm{Gal}(k_L/k_K) \longrightarrow 1$$

and if $L|K$ is unramified, then

$$I_w(L/K) = 1 = \{id_L\} \quad \text{and} \quad \mathrm{Gal}(L/K) \overset{\varphi}{\cong} \mathrm{Gal}(k_L/k_K).$$

Now let $T$ be the maximal unramified subextension of $L$. Since the Galois closure of $T$ is the composite of the conjugates $\sigma T$, we see that $T|K$ **is a Galois extension**, because its conjugates $\sigma T$ are again unramified ($w \circ \sigma = w \implies e(\sigma T|K) = e(T|K) = 1$), hence $\sigma T \subset T$ and $T$ equals its Galois closure. Therefore,

$$I_w(T/K) = 1 \quad \text{and} \quad \mathrm{Gal}(T/K) \overset{\varphi}{\cong} \mathrm{Gal}(k_s/k_K)$$

because the residue class field of $T$ is $k_s$, the separable closure of $k_k$ in $k_L$ (Proposition III.2.16). Though under our assumptions, $k_s = k_L$.

*A basic result usually studied in Galois theory is that every $K$ automorphism of a field extension $M|K$ can be extended to a $K$-automorphism of a bigger field extension $L|K$.

**Definition III.3.9.** *The fixed field of $I_w(L/K)$ is*

$$T_w = \{x \in L \mid \sigma x = x \ \forall \sigma \in I_w\}.$$

Of course $I_w = \mathrm{Gal}(L/T_w)$.

**Proposition III.3.10.** *The fixed field of $I_w$ is the maximal unramified subextension, $T$, of $L|K$.*

*Proof.* As explained above, we have:

$$\mathrm{Gal}(T/K) \overset{\varphi}{\cong} \mathrm{Gal}(k_L/k_K).$$

And of course $\dfrac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/T)} \cong \mathrm{Gal}(T/K)$. Since $I_w = \mathrm{Gal}(L/T_w)$ is the kernel of $\mathrm{Gal}(L/K) \xrightarrow{\varphi} \mathrm{Gal}(k_L/k_K)$, we also have

$$\mathrm{Gal}(k_L/k_K) \cong \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/T_w)} \cong \mathrm{Gal}(L/T_w)$$

which means that $\mathrm{Gal}(L/T) \cong \mathrm{Gal}(L/T_w)$, hence $T_w = T$ (to the closed subgroup $I_w$ of $\mathrm{Gal}(L/K)$ only one intermediate extension of $L|K$ can be assigned). □

To finish this chapter, we sum up our results of the inertia group for the extension $\overline{K}|K$. Let $k$ be the residue class field of $K$, which we assume perfect. We will also denote by $v$ the unique extension of the valuation $v$ of $K$ to $\overline{K}$. The residue class field of $\overline{K}$ is $\overline{k}$, an algebraic closure of $k$ as Proposition III.2.9 shows. The residue class field of the maximal subramified extension of $K$, $K^{nr}$, is also $\overline{k}$ (Proposition III.2.16), since $k$ is perfect. We have the short exact sequence:

$$1 \longrightarrow I_v(\overline{K}/K) \longrightarrow \mathrm{Gal}(\overline{K}/K) \xrightarrow{\varphi} \mathrm{Gal}(\overline{k}/k) \longrightarrow 1$$

and also

$$I_v = \mathrm{Gal}(\overline{K}/K^{nr}) \quad \text{and} \quad \mathrm{Gal}(K^{nr}/K) \cong \mathrm{Gal}(\overline{k}/k).$$

The isomorphism $\mathrm{Gal}(K^{nr}/K) \cong \mathrm{Gal}(\overline{k}/k)$ is also an homeomorphism because is a continuous bijection between compact Hausdorff spaces. Therefore, by the fundamental theorem of (infinite) Galois Theory, the subextensions $M|K$ of $K^{nr}|K$ are in a $1-1$ correspondence with the subextensions $k_M|k_K$ of $\overline{k}|k$.

# Chapter IV

# Formal groups

## IV.1 Completion of a ring: the $I$-adic topology

This section is a brief compilation of results about topological rings and their completion at an ideal $I$, using the Krull topology, also called de **$I$-adic topology**. It is a generalization of the concept of completion with respect an absolute value (in the end, a metric) that we studied in Chapter I, as sometimes the $I$-adic topology will not come from a metric. Nevertheless, it will be clear that the completion, with this apparently new process, of a discretely valued field with respect to the maximal ideal of its valuation ring will be the same as the completion with respect to the nonarchimedean valuation.

Here I am going to be rather brief. More details can be found for example, in [2, Ch. 10]. This is because we mainly need a few concepts and vocabulary in order to comfortably state the main result of this section: Hensel's lemma in its $I$-adic form (IV.1.5).

**Definition IV.1.1.** *Let $R$ be a ring and $M$ an $R$-module. Then each ideal $I$ of $R$ determines a topology on $M$ called the $I$-adic topology defined as follows: a subset $U \subset M$ is open if and only if for each $x \in U$ there exist an integer $n > 0$ such that:*

$$x + I^n M \subset U.$$

*In other words, this topology is defined giving a nested basis of neighbourhoods of $x$, namely $\{x + I^n M : n > 0\}$.*

For this topology, the module operations are continuous. The closure of a submodule $N$ is $\bigcap_{n>0} (N + I^n M)$. The neighbourhoods $x + I^n M$ are both closed and open.

$M$ is a Hausdorff topological space with this topology if and only if $\cap_{n>0} I^n M = \{0\}$.

The *completion* of $M$ at $I$ is:

$$\widehat{M} = \varprojlim M/I^n M$$

with the topology being the initial topology for the canonical morphisms

$$\phi_k : \varprojlim M/I^n M \to M/I^k M$$

and the discrete topology on $M/I^kM$.

We regard $M$ as a subring of $\varprojlim M/I^nM$ in the obvious way: we assign to each $x \in R$ the class of the sequence $(x, x, \dots)$.

We will use these completions when $M = R$, i.e., we will be working with rings and their completions. So a ring complete with respect to an ideal $I$ is by definition one that satisfies:

$$R \cong \varprojlim R/I^n.$$

A Cauchy sequence in this context is a sequence $(x_n)_{n\in\mathbb{N}}$ verifying that for every $k \geq 0$, there exists $k' \geq 0$ such that for every $m, n \geq k'$, $x_m - x_n \in I^k$.

**Example IV.1.2.** If $R = K[X_1 \dots, X_n]$ is a polynomial ring over a field $K$, then the completion at the maximal ideal $\mathfrak{m} = (X_1, \dots, X_n)$ is $\widehat{R} = \varprojlim R/I^n = K[[X_1 \dots, X_n]]$, the ring of formal power series.

**Example IV.1.3. (Important)** If $R = \mathbb{Z}$ and $I = (p)$ where $p$ is a prime integer, then $\widehat{\mathbb{Z}} = \mathbb{Z}_p$, the $p$-adic numbers (Proposition II.2.1). In general, let $K$ be field, complete with respect to a discrete valuation. Its valuation ring $\mathcal{O}$ is also complete, as it is a closed subset of $K$. Then $\mathcal{O}$ is complete with respect to the maximal ideal $\mathfrak{p}$ of its valuation ring, since the $\mathfrak{p}$-adic topology and the topology originated from the valuation are the same. Proposition I.2.10 also shows directly that $\mathcal{O}$ is $\mathfrak{p}$-adically complete.

We have the following proposition, which is not true for an arbitrary ideal of a ring.

**Proposition IV.1.4.** *Let $A$ be a ring complete with respect to an ideal $I$. Then $1 + I \subset A^\times$. More generally, $A^\times + I = A^\times$.*

*Proof.* Let $x \in I$. If there exists $z = (1+x)^{-1}$, then $z = \sum_{\nu=0}^{+\infty}(-x)^\nu$. It remains only to show that if $S_n = \sum_{\nu=0}^{n}(-x)^\nu$ then $\{S_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence in $A$, and therefore corverges in $A$ to an element that must be $(1+x)^{-1}$. Let $k \geq 0$. For $m, n \geq k$ we have:

$$S_n - S_m = \sum_{\nu=m+1}^{n}(-x)^\nu \in I^{m+1} \subset I^m \subset I^k.$$

So $\{S_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence.

Finally, since the elements in $1 + I$ are units:

$$A^\times + I = A^\times(1 + I) = A^\times.$$

The first equality is due to the fact that if $u \in A^\times, x \in I$ then

$$u + x = u(1 + u^{-1}x) \in A^\times(1 + I) \quad \text{and} \quad u(1 + x) = u + ux \in A^\times + I.$$

□

Now we can give the following version of Hensel's lemma, which we will use several times throughout this chapter. The version I am giving here is slightly stronger than the version that can be found on Silverman's book [16, Ch. IV, Lemma 1.2], which I am following, since I am giving a proof valid for power series, not only polynomials, and I do not require that $R$ is a integral domain to obtain uniqueness.

**Lemma IV.1.5.** ***(Hensel's lemma, $I$-adic form).*** *Let $R$ be a ring that is complete with respect to some ideal $I \subset R$, and let $F(w) \in R[[w]]$ be a power series. Suppose that there are an integer $n \geq 1$ and an element $a \in I$ satisfying*

$$F(a) \in I^n \quad \textit{and} \quad F'(a) \in R^{\times}.$$

*Then for any $\alpha \in R$ satisfying $\alpha \equiv F'(a) \pmod I$, the sequence*

$$w_0 = a, \quad w_{m+1} = w_m - \frac{F(w_m)}{\alpha}$$

*converges to an element $b \in R$ satisfying*

$$F(b) = 0 \quad \textit{and} \quad b \equiv a \pmod{I^n},$$

*and $b$ is the only element of $R$ with this property.*

*Proof.* We first note that any $\alpha$ like the one in the statement of the lemma is a unit:

$$\alpha \in F'(a) + I \subset R^{\times} + I = R^{\times} \quad \text{(by Proposition IV.1.4).}$$

Define $\widetilde{F}(w) = F(w+a)/\alpha$, $\widetilde{w}_0 = 0$ and $\widetilde{w}_{m+1} = \widetilde{w}_m - \widetilde{F}(\widetilde{w}_m)$. Then by induction we see that $w_m - \widetilde{w}_m = a$ and $F(w_m)/\alpha = \widetilde{F}(\widetilde{w}_m)$. Indeed, for $m = 0$.

$$w_0 - \widetilde{w}_0 = a \quad \text{and} \quad F(w_0)/\alpha = F(a)/\alpha = F(0+a)/\alpha = \widetilde{F}(\widetilde{w}_0).$$

Assume that for $m \geq 0$ we have $w_m - \widetilde{w}_m = a$ and $F(w_m)/\alpha = \widetilde{F}(\widetilde{w}_m)$. Then

$$w_{m+1} - \widetilde{w}_{m+1} = w_m - \widetilde{w}_m - (F(w_m)/\alpha - \widetilde{F}(\widetilde{w}_m)) = a + 0.$$

Hence

$$F(w_{m+1})/\alpha = F(\widetilde{w}_{m+1} + a)/\alpha = \widetilde{F}(\widetilde{w}_{m+1}).$$

With this in mind, the conditions of the theorem translate into:

$$\widetilde{w}_0 = 0, \quad \widetilde{F}(0) = F(a)/\alpha \in I^n, \quad \widetilde{F}'(0) = F'(a)/\alpha \equiv 1 \pmod I.$$

Dropping the tildes to ease notation, we can now prove the theorem under the conditions:

$$w_0 = 0, \quad F(0) \in I^n, \quad F'(0) \equiv 1 \pmod I, \quad w_{m+1} = w_m - F(w_m).$$

At a practical level, replacing $F(w)$ with $F(w+a)\alpha^{-1}$ has allowed us to assume that $a = 0 = w_0$ and now $\alpha$ does not appear in our sequence. Of course, the $b$ we are now looking for must satisfy $b \equiv 0 \pmod{I^n}$.

We want to show that $w_m \in I^n$ for every $m \geq 0$. It is obviously true for $m = 0$. If we suppose it true for integers not greater than $m$, then $F(w_m) \in I^n$ (because $F(0) \in I^n$), and therefore we have the induction step:

$$w_{m+1} = w_m - F(w_m) \in I^n.$$

Now we will show by induction that

$$w_m \equiv w_{m+1} \pmod{I^{m+n}} \qquad \forall m \geq 0.$$

Which in particular proves that $w_m$ is a Cauchy sequence.

For $m = 0$ this just says that $F(0) \equiv 0 \pmod{I^n}$, which is one of our assumptions. Suposse that the congruence is true for all integers strictly smaller than $m$. If $X$ and $Y$ are independent variables, then we can factor:

$$F(X) - F(Y) = (X - Y)\left(F'(0) + XG(X,Y) + YH(X,Y)\right) \tag{IV.1}$$

for certain $G, H \in A[[Y,Z]]$. To see this we just have to look at the difference $F(X) - F(Y)$ monomial by monomial. If we denote by $c_n$ the $n$-th coefficient of $F$, the degree $n$ component of $F(X) - F(Y)$ is:

$$c_nX^n - c_nY^n = c_n(X - Y)\sum_{i+j=n-1} X^iY^j, \qquad \text{for every } n \geq 1,$$

which yields (IV.1) noticing that $c_1 = F'(0)$.

Then we have:

$$\begin{aligned} w_{m+1} - w_m &= (w_m - F(w_m)) - (w_{m-1} - F(w_{m-1})) \\ &= (w_m - w_{m-1}) - (F(w_m) - F(w_{m-1})) \\ &= \underbrace{(w_m - w_{m-1})}_{\in I^{m+n-1}} \left( \underbrace{1 - F'(0)}_{\in I} - \underbrace{w_mG(w_m, w_{m-1}) - w_{m-1}H(w_m, w_{m-1})}_{\in I^n} \right) \in I^{m+n}. \end{aligned}$$

And we have proven that:

$$w_m \equiv w_{m+1} \pmod{I^{m+n}} \quad \forall m \geq 0.$$

So, as we said, $w_m$ is a Cauchy sequence and therefore converges to an element $b \in R$. Since every $w_m \in I^n$, we must have $b \in I^n$ because $I^n$ is closed. And taking limits in the relation $w_{m+1} = w_m - F(w_m)$, we see that $b = b - F(b)$, so $F(b) = 0$ as we wanted.

For the uniqueness, assume that there are $b, c \in I^n$ with $F(b) = F(c) = 0$. Then:

$$0 = (b - c)(1 + bG(b,c) + cH(b,c))$$

which implies $b = c$ since $1 + I \subset A^\times$ by Proposition IV.1.4. □

Finally, we have the following useful lemma:

**Lemma IV.1.6.** *(Inverse for composition). Let $f(X) = \sum_{n=0}^{\infty} f_nX^n \in R[[X]]$ be a power series such that $f_0 = f(0) = 0, f_1 = f'(0) \in R^\times$. That is, $f(X)$ is of the form:*

$$f(X) = f_1X + (\textit{higher-order terms}), \quad f_1 \in R^\times.$$

*Then there is a unique power series $g(X) \in R[[X]]$ satisfying*

$$f(g(X)) = X.$$

*The series $g(X)$ also satisfies $g(f(X)) = X$.*

*Proof.* Let $A = R[[X]]$, $I = (X)$ the ideal with respect to which $A$ is complete, and define $F(Y) := f(Y) - X \in A[[Y]]$. Let $a = f_1^{-1}X \in A$. We have

$$F(a) = f(a) - X = f_2 f_1^{-2} X^2 + f_3 f_1^{-3} X^3 + \cdots \equiv 0 \pmod{I^2}$$
$$F'(a) = f_1 + (\text{higher-order terms}) \in A^\times.$$

Hensel's Lemma in its $I$-adic form (Proposition IV.1.5) applied to $a = f_1^{-1}X$, gives us a unique $b = g(X) \in A$ such that $F(g(X)) = 0$ and $g(x) \equiv a \pmod{I^2}$, which then translates into:

$$f(g(X)) = X \qquad g(X) = f_1^{-1}X + (\text{higher-order terms}).$$

The same argument applied to $g(X)$ instead of $f(X)$ tells us that there is a unique $h(X) = f_1 X + (\text{higher-order terms}) \in A$ such that $g(h(X)) = X$. Now:

$$f(X) = f(g(h(X))) = (f \circ g)(h(X)) = h(X)$$

and we have proven that $f(g(X)) = g(f(X)) = X$. □

## IV.2 General facts about formal groups

First we recall a basic fact about formal power series.

**Proposition IV.2.1.** *Let $A$ be a ring. Then $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$ is a unit if and only if $a_0 \in A^\times$. In that case, the coefficients of $f^{-1}$ can be computed inductively as:*

$$b_0 = a_0^{-1}, \qquad b_k = -a_0^{-1} \sum_{j=1}^{k} a_j b_{k-j}.$$

*Proof.* First recall that if $g(x) = \sum_{n=0}^{\infty} b_n x^n \in A[[x]]$, then:

$$f(x)g(x) = \sum_{n=0}^{\infty} \left( \sum_{j=0}^{n} a_j b_{n-j} \right) x^n.$$

Assume first that there exists $g$ such that $f(x)g(x) = 1$. Then, equating the degree 0 terms, we see that $a_0 b_0 = 1$, so $a_0$ is a unit.

Now assume that $a_0$ is a unit. We are going to construct the inverse $g(x) = \sum_{n=0}^{\infty} b_n x^n$ of $f(x)$ inductively. By equating the terms of degree 0 in $1 = f(x)g(x)$ we get that $b_0 = a_0^{-1}$. For $k \geq 1$, suppose we have computed the coefficients $b_j, j < k$ . Then, since the $k$-th coefficient of $f(x)g(x)$ must be 0, we have

$$\sum_{j=0}^{k} a_j b_{k-j} = 0 \implies b_k = -a_0^{-1} \sum_{j=1}^{k} a_j b_{k-j}$$

which finishes the proof. □

**Definition IV.2.2.** *A (one parameter) commutative formal group $\mathcal{F}$ over $R$ is a power series $F(X, Y) \in R[[X, Y]]$ with the following properties:*

*(a)* $F(X, Y) = X + Y + ($ *terms of degree* $\geq 2)$.

*(b)* $F(X, F(Y, Z)) = F(F(X, Y), Z)$ *(associativity).*

*(c)* $F(X, Y) = F(Y, X)$ *(commutativity).*

All formal groups that we are going to see are of this kind: *commutative one-parameter* formal groups, and we will simply call them formal groups. If we want to emphasize the ring $R$, we write $\mathcal{F}/R$. Sometimes we will write $(\mathcal{F}, F)$ if what we want to emphasize is the power series $F(X, Y)$.

We should think of formal groups as a way to define the group operation without the underlying set. The power series $F$ serves as the group operation ($F(X, Y)$ instead of $X + Y$ or $XY$).

From (a) and (b) in the last definition we deduce the following properties

**Proposition IV.2.3.** *If $F(X,Y) \in R[[X,Y]]$ defines a formal group over $R$, then:*

*(d)* $F(X,0) = X$ *and* $F(0,Y) = Y$.

*(e) There is a unique power series* $i(T) \in R[[T]]$ *satisfying* $i(T) \neq 0$ *and* $F(T, i(T)) = 0$ *(an "inverse" for $T$), and it has the form*

$$i(T) = -T + (\textit{higher-order terms}).$$

*Proof.* (a) We can write $F$ as

$$F(X,Y) = X + Y + \sum_{i+j\geq 2} c_{ij} X^i Y^j = f(X) + g(Y) + XYH(X,Y)$$

where

$$f(X) := F(X,0) = X + \sum_{i=2}^{+\infty} c_{i0} X^i$$
$$g(Y) := F(0,Y) = Y + \sum_{j=2}^{+\infty} c_{0j} Y^j.$$

By associativity we have $F(X, F(0,Y)) = F(F(X,0),Y)$, or equivalently:

$$f(X) + g(g(Y)) + Xg(Y)H(X, g(Y)) = f(f(X)) + g(Y) + f(X)YH(f(X),Y).$$

Equating the parts independent from $X$ and those independent from $Y$, we get, respectively:

$$f(X) = f(f(X)) \text{ and } g(Y) = g(g(Y)).$$

This implies that $f(X) = X$ and $g(Y) = Y$. Indeed, since $f(0) = 0, f'(0) = 1 \in R^\times$, by Lemma IV.1.6, there exists an inverse $f^{-1}$ of $f$ for composition, so:

$$f(X) = f(f(X)) \overset{f^{-1}\circ}{\Longrightarrow} X = f(X) \tag{IV.2}$$

and the same goes for $g(X)$.

(b) Let $A = R[[X]]$, complete with respect to the ideal $I = (X)$. Thanks to (a), we know that $F(X,Y) = X + Y + XYH(X,Y)$, with $H(X,Y) \in R[[X,Y]] = A[[Y]]$. We define $G(Y) = F(X,Y) \in A[[Y]]$. Then

$$G(-X) = -X^2 H(X,-X) \in I^2 \qquad G'(-X) = 1 + (\text{ higher-order terms in } X\ ) \in A^\times.$$

So Hensel's lemma in its $I$-adic form (Lemma IV.1.5), applied to $a = -X, n = 2$, tell us that there exists a unique power series $i(X) \in A$ such that $G(i(X)) = 0$ and $i(X) \equiv -X \pmod{I^2}$. Therefore, $F(X, i(X)) = 0$ and

$$i(X) = -X + (\text{higher-order terms})$$

as we wanted. □

The following two examples are easily verified to define a formal group.

**Example IV.2.4.** The formal additive group, denoted by $\widehat{\mathbb{G}}_a$, is defined by:

$$F(X,Y) = X + Y.$$

**Example IV.2.5.** The formal multiplicative group, denoted by $\widehat{\mathbb{G}}_m$, is defined by:

$$F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1.$$

As it is customary, after defining the mathematical objects, we give the morphisms between them.

**Definition IV.2.6.** *Let $(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ be formal groups defined over $R$. A homomorphism from $\mathcal{F}$ to $\mathcal{G}$ defined over $R$ is a power series $f \in R[[T]]$ (with no constant term) that satisfies*

$$f(F(X,Y)) = G(f(X), f(Y)).$$

*The formal groups $\mathcal{F}$ and $\mathcal{G}$ are isomorphic over $R$ if there are homomorphisms $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{F}$ defined over $R$ such that*

$$f(g(T)) = g(f(T)) = T.$$

**Proposition IV.2.7.** *Let $(\mathcal{F}, F)$ be a formal group and let $f : \mathcal{F} \to \mathcal{F}, f \in R[[T]]$ be a formal group homomorphism that has an inverse for composition $g \in R[[T]]$. Then $g : \mathcal{F} \to \mathcal{F}$ is a formal group homomorphism. Consequently $f$ is an automorphism of $\mathcal{F}$.*

*Proof.* Since $f(g(X)) = g(f(X)) = X$ and $f$ is a homomorphism, we have:

$$F(X,Y) = F(f \circ g(X), f \circ g(Y)) = f(F(g(X), g(Y))).$$

Thus

$$g(F(X,Y)) = g \circ f(F(g(X), g(Y))) = F(g(X), g(Y)).$$

□

**Proposition IV.2.8.** *The unique power series $i(T)$ such that $F(T, i(T)) = 0$ is a formal group homomorphism from $\mathcal{F}$ to $\mathcal{F}$.*

*Proof.* We have to prove that

$$i(F(X,Y)) = F(i(X), i(Y)).$$

It suffices to show that $H(X,Y) := F(F(X,Y), F(i(X), i(Y))) = 0$, since then

$$F(i(F(X,Y)), H(X,Y)) = i(F(X,Y))$$

but thanks to associativity we also have:

$$\begin{aligned} F(i(F(X,Y)), H(X,Y)) &= F(F(i(F(X,Y)), F(X,Y)), F(i(X), i(Y))) \\ &= F(0, F(i(X), i(Y))) = F(i(X), i(Y)) \end{aligned}$$

Indeed, we have

$$\begin{aligned}F(F(X,Y),F(i(X),i(Y))) &= F(F(F(Y,X),i(X)),i(Y)) = F(F(Y,F(X,i(X))),i(Y)) \\ &= F(F(Y,0),i(Y)) = F(Y,i(Y)) = 0\end{aligned}$$

as we wanted. □

**Definition IV.2.9.** ***(Multiplication by** $m$**)**. Let $(\mathcal{F}, F)$ be a formal group. We define inductively:*

$$[0](T) = 0, \quad [m+1](T) = F([m](T),T), \quad [m-1](T) = F([m](T),i(T)).$$

*for $m \in \mathbb{Z}$.*

**Proposition IV.2.10.** *The multiplication-by-m map $[m] : \mathcal{F} \to \mathcal{F}$ defined in (IV.2.9) is a homomorphism in the sense of Definition IV.2.6*

*Proof.* For $m = 0$ it is obvious:

$$[0]F(X,Y) = 0 = F(0,0) = F([0]X,[0]Y).$$

Now, suppose that it is true for $m \in \mathbb{Z}$, which means that:

$$[m]F(X,Y) = F([m]X,[m]Y).$$

Then, we are going to see that this is also true for $m+1$ and $m-1$. Using the the induction hypothesis and the properties of $F$ we have:

$$\begin{aligned}[m+1]F(X,Y) &= F([m]F(X,Y),F(X,Y)) = F(F([m]X,[m]Y),F(X,Y)) \\ &= F(F([m]X,[m]Y),F(Y,X)) = F([m]X,F([m]Y,F(Y,X))) \\ &= F([m]X,F(F([m]Y,Y),X)) = F([m]X,F([m+1]Y,X)) \\ &= F([m]X,F(X,[m+1]Y)) = F(F([m]X,X),[m+1]Y) \\ &= F([m+1]X,[m+1]Y).\end{aligned}$$

And also using that $i(T)$ is a formal group homomorphism we have:

$$\begin{aligned}[m-1]F(X,Y) &= F([m]F(X,Y),i(F(X,Y))) = F(F([m]X,[m]Y),F(i(X),i(Y))) \\ &= F(F(F([m]Y,[m]X),i(X)),i(Y)) = F(F([m]Y,F([m]X,i(X))),i(Y)) \\ &= F(F([m]Y,[m-1]X),i(Y)) = F(F([m-1]X,[m]Y),i(Y)) \\ &= F([m-1]X,F([m]Y,i(Y))) = F([m-1]X,[m-1]Y),\end{aligned}$$

which finishes the proof. Let us notice that commutativity has been essential. □

**Proposition IV.2.11.** *Let $\mathcal{F}$ be a formal group over a ring $R$ and let $m \in \mathbb{Z}$.*

*(a)* $[m](T) = mT + ($*higher order terms*$)$.

*(b) If $m \in R^\times$, then $[m] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.*

*Proof.* (a) We are going to prove this by induction on $m$. For $m = 0, [0](T) = 0$ and for $m = 1, [1](T) = F([0](T), T) = F(0, T) = T$, so the result holds. Now, suppose that the result holds for $m \in \mathbb{Z}$. Let us see first the upward induction:

$$[m + 1](T) = F([m](T), T) = [m](T) + T + \cdots = (m + 1)T + (\text{higher order terms}).$$

For the downward induction, we have:

$$[m-1](T) = F([m](T), i(T)) = [m](T)+i(T)+\cdots = mT-T+\cdots = (m-1)T+(\text{higher order terms}).$$

(b) From (a) and Lemma IV.1.6 it follows inmediately that $[m]$ has an inverse for composition. Then Proposition IV.2.7 guarantees that this inverse is a formal group homomorphism, hence $[m]$ is an isomorphism. □

### IV.2.1 Groups associated to formal groups

**Notation:** Throughout all this section, $R$ is a complete local ring, with maximal ideal $\mathcal{M}$ and residue field $k$. $\mathcal{F}$ will be a formal group over $R$ with formal group law $F(X, Y)$.

When we evaluate $F(X, Y)$ in elements of the maximal ideal $\mathcal{M}$, the power series converges and therefore $F$ gives $\mathcal{M}$ the structure of an abelian group.

**Definition IV.2.12.** *The group associated to $\mathcal{F}/R$, denoted by $\mathcal{F}(\mathcal{M})$, is the set $\mathcal{M}$ endowed with the group operations*

$$\begin{aligned} x \oplus_{\mathcal{F}} y &= F(x, y) \quad \textit{addition} \qquad \textit{for } x, y \in \mathcal{M}. \\ \ominus_{\mathcal{F}} x &= i(x) \quad \textit{inversion} \qquad \textit{for } x \in \mathcal{M}. \end{aligned}$$

Similarly, $\mathcal{F}(\mathcal{M}^n)$ is the set $\mathcal{M}^n$ with the above group operations. The fact that $R$ is complete implies that both $F(x, y)$ and $i(x)$ converge for all $x, y \in \mathcal{M}$. The properties of $F$ makes $\mathcal{F}(\mathcal{M})$ inmediately into a group.

A formal group homomorphism $f : (\mathcal{F}, F) \to (\mathcal{G}, G)$ induces a group morphism between the corresponding groups, in the obvious way:

$$f(x \oplus_{\mathcal{F}} y) = f(F(x, y)) = G(f(x), f(y)) = f(x) \oplus_{\mathcal{G}} f(y).$$

Therefore, if the formal group homomorphism is an isomorphism, so is the induced morphism on the associated groups.

**Example IV.2.13.** The additive group $\widehat{\mathbb{G}}_a(\mathcal{M})$ associated to the additive formal group given in Example IV.2.4, is just $\mathcal{M}^+$, i.e. $\mathcal{M}$ with its usual addition law.

The multiplicative group $\widehat{\mathbb{G}}_m(\mathcal{M})$, associated to the multiplicative formal group $G(X, Y) = (1 + X)(1 + Y) - 1$, given in Example IV.2.5, is isomorphic to the group of principal units: $1 + \mathcal{M}$ with multiplication as group law. To see this, let $f : \mathcal{M} \to 1 + \mathcal{M}, f(x) = 1 + x$. Then for $x, y \in \mathcal{M}$:

$$f(x \oplus_G y) = (1 + x)(1 + y) = f(x)f(y)$$

So $f$ is a group morphism between $\widehat{\mathbb{G}}_m(\mathcal{M})$ and $1+M$, with inverse $f^{-1}(y)=y-1$ and therefore $f$ is an isomorphism.

Let us notice the exact sequences:

$$0 \longrightarrow \widehat{\mathbb{G}}_a(\mathcal{M}) \longrightarrow R \longrightarrow k \longrightarrow 0$$
$$0 \longrightarrow \widehat{\mathbb{G}}_m(\mathcal{M}) \overset{z\mapsto 1+z}{\longrightarrow} R^\times \longrightarrow k^\times \longrightarrow 1.$$

They follow from the description of $\widehat{\mathbb{G}}_a(\mathcal{M})$ y $\widehat{\mathbb{G}}_m(\mathcal{M})$ given above and the fact that the kernel of the reduction modulo $\mathcal{M}$, $R^\times \to k^\times$ is the group of principal units $1+\mathcal{M}$.

**Proposition IV.2.14.** *Let $\mathcal{F}/R$ be a formal group defined over a complete local ring.*

*(a) For each $n \geq 1$, the map*
$$\frac{\mathcal{F}\left(\mathcal{M}^n\right)}{\mathcal{F}\left(\mathcal{M}^{n+1}\right)} \longrightarrow \frac{\mathcal{M}^n}{\mathcal{M}^{n+1}}$$
*induced by the identity map on sets is an isomorphism of groups.*

*(b) Let $p$ be the characteristic of the residue field $k$, where $p$ is allowed to equal 0. Then every element of finite order in $\mathcal{F}(\mathcal{M})$ has an order that is a power of $p$.*

*Proof.* (a) Since the underlying sets are the sames, it suffices to show that the identity map is a morphism of groups. For any $x, y \in \mathcal{M}^n$ we have:

$$x \oplus_{\mathcal{F}} y = F(x,y) = x + y + (\text{ higher-order terms }) \equiv x + y \pmod{\mathcal{M}^{2n}}$$

and the congruence also holds mod $\mathcal{M}^{n+1}$ since $\mathcal{M}^{2n} \subset \mathcal{M}^{n+1}$ for every $n \geq 1$.

(b) Let $x$ be a torsion element and $m \in \mathbb{N}$ its order. If we write $m = m' p^{v_p(m)}$, then $p \nmid m'$ and $0 = mx = m'(p^{v_p(m)}x)$, which tell us that it suffices to prove that there are no non-zero torsion elements of order prime to $p$. So let $m \in \mathbb{Z}$ such that $p \nmid m$ (for $p=0$ this means that $m$ is arbitrary) and suppose there exists $x \in \mathcal{M}$ such that $[m]x = 0$. But since $m$ is prime to $p$, $m \notin \mathcal{M}$ so that $m \in R^\times$, since $R$ is a local ring. Then, by Proposition IV.2.11, $[m] : \mathcal{F} \to \mathcal{F}$ is a formal group automorphism, thus it induces an automorfism in $\mathcal{F}(\mathcal{M})$, so $[m]$ has trivial kernel and therefore $x = 0$. □

## IV.3 The formal group of an elliptic curve

We are going to examine the group structure of an elliptic curve near the point at infinity. But before that, we will want to move it to the origin, that is, the affine* point $[0:0:1]$.

Let us start with an elliptic curve given by a Weierstrass equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Now we dehomogenize by making $Y = 1$, instead of $Z = 1$ which is what we are used to. This just means that we have moved to the affine chart $Y = 1$ where the line at infinity is $Y = 0$, instead of $Z = 0$. Here, the equation of our elliptic curve is:

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Now we substitute $v = -x, w = -z$ and obtain:

$$-w + a_1vw + a_3w^2 = -v^3 - a_2v^2w - a_4vw^2 - a_6w^3.$$

Or equivalently:

$$w = a_1vw + a_3w^2 + v^3 + a_2v^2w + a_4vw^2 + a_6w^3.$$

After the composition of the change of charts and this last change of variables, the points of the form $[a : 1 : b]$ are sent to the point $(-a, -b)$ in the affine chart $Y = 1$. So, in particular, $\mathcal{O} = [0 : 1 : 0]$ is sent to $O = (0, 0)$. The rest of points of the curve, of the form $[x : y : 1]$, if they are on the new affine plane $Y = 1$, are sent to $\left[-\frac{x}{y} : 1 : -\frac{1}{y}\right]$ (since $y \neq 0$), or $\left(-\frac{x}{y}, -\frac{1}{y}\right)$ in our new system of coordinates.

We are going to rename $v = z$ for convenience, because $v$ will be our valuation later on. Summarizing, the new equation for our elliptic curve, with which we will be working this whole section, is:

$$w = a_1zw + a_3w^2 + z^3 + a_2z^2w + a_4zw^2 + a_6w^3 = f(z, w) \tag{IV.3}$$

and the change of coordinates that has transformed the original Weierstrass equation into this one is:

$$\left\{\begin{aligned} z &= -\frac{x}{y} \\ w &= -\frac{1}{y} \end{aligned}\right. \qquad \text{or} \qquad \left\{\begin{aligned} x &= \frac{z}{w} \\ y &= -\frac{1}{w} \end{aligned}\right. \tag{IV.4}$$

The equation (IV.3) allows us to substitute

$$w = f(z, w) = f(z, f(z, w)) = \dots$$

*By default, we choose $Z = 0$ as the line at infinite. Consequently, we inject the affine point $(x, y)$ into the projective plane as $[x : y : 1]$.

in order to write $w$ as a power series in $z$. More precisely, we want to prove that the sequence

$$w_{m+1}(z) = f(z, w_m(z)), \quad w_0(z) = 0 \tag{IV.5}$$

converges to an element $w(z) \in \mathbb{Z}[a_1, \dots, a_6][[z]]$, verifying $w(z) = f(z, w(z))$, which we will prove using Hensel's Lemma IV.1.5.

A single substitution show us that:

$$\begin{aligned}
w &= z^3 + \left(a_1 z + a_2 z^2\right) w + (a_3 + a_4 z) w^2 + a_6 w^3 \\
&= z^3 + \left(a_1 z + a_2 z^2\right) \left[z^3 + \left(a_1 z + a_2 z^2\right) w + (a_3 + a_4 z) w^2 + a_6 w^3\right] \\
&+ (a_3 + a_4 z) \left[z^3 + \left(a_1 z + a_2 z^2\right) w + (a_3 + a_4 z) w^2 + a_6 w^3\right]^2 \\
&+ a_6 \left[z^3 + \left(a_1 z + a_2 z^2\right) w + (a_3 + a_4 z) w^2 + a_6 w^3\right]^3 \\
&\vdots \\
&= z^3 + a_1 z^4 + \left(a_1^2 + a_2\right) z^5 + \left(a_1^3 + 2a_1 a_2 + a_3\right) z^6 \\
&+ \left(a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4\right) z^7 + \cdots \\
&= z^3 \left(1 + A_1 z + A_2 z^2 + \cdots\right)
\end{aligned}$$

where each $A_n \in \mathbb{Z}[a_1, \dots, a_6]$ is a polynomial in the coefficients of $E$. This is easy to notice when we regroup the coefficients, because for each monomial $z^k$, substitutions will eventually stop contributing to its coefficient.

**Proposition IV.3.1.** *The procedure described above converges to a power series*

$$w(z) = z^3 \left(1 + A_1 z + A_2 z^2 + \cdots\right) \in \mathbb{Z}[a_1, \dots, a_6][[z]]$$

*and $w(z)$ is the unique power series in $\mathbb{Z}[a_1, \dots, a_6][[z]]$ satisfying*

$$w(0) = 0 \qquad \textit{and} \qquad w(z) = f(z, w(z)).$$

*Proof.* We just have to use Hensel's lemma in its $I$-adic form (Lemma IV.1.5) in the ring $R = \mathbb{Z}[a_1, \dots, a_1][[z]]$ complete with respect to the ideal $I = (z)$. Let $F(w) = f(z, w) - w$, $a = 0$. Then

$$F(a) = f(z, 0) - 0 = z^3 \in I^3$$

$$F'(a) = \left.\frac{\partial f(z, w)}{\partial w}\right|_{w=0} - 1 = -1 + a_1 z + a_2 z^2 \in R^\times.$$

Moreover, $F'(a) \equiv -1 \pmod{I}$. So Hensel's lemma, with these data and $\alpha = -1$ tell us that there exists a unique $w(z) \in R$ such that $F(w(z)) = 0$ and $w(z) \in I^3$. This translates respectively into $w(z) = f(z, w(z))$ and

$$w(z) = z^3 \left(1 + A_1 z + A_2 z^2 + \cdots\right) \in \mathbb{Z}[a_1, \dots, a_6][[z]]; \qquad w(0) = 0.$$

And the sequence converging to $w(z)$ that the statement of Lemma IV.1.5 gives us is

$$w_{m+1}(z) = w_m(z) - F(w_m(z))/(-1) = f(z, w_m(z))$$

and this is the sequence we constructed in (IV.5) earlier, which proves our claims. □

Using Proposition IV.2.1, it is inmediate to compute the Laurent series for $x$ and $y$:

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2\left(1 + A_1 z + A_2 z^2 + \cdots\right)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - \left(a_4 + a_1 a_3\right) z^2 - \cdots$$
$$y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3\left(1 + A_1 z + A_2 z^2 + \cdots\right)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + \left(a_4 + a_1 a_3\right) z - \cdots$$

The pair $(x(z), y(z))$ provides a formal solution to the original Weierstrass equation:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

i.e., a solution over $K((z))$. In order to make sense of the point $(x(z), y(z))$ we must work over a field $K$ complete with respect to a discrete valuation, with valuation ring $R$ and maximal ideal $\mathcal{M}$. Then, if $a_1, \ldots, a_6 \in R$, $x(z)$ and $y(z)$ will converge for every $z \in \mathcal{M} \setminus \{0\}$ and this way we get a point $(x(z), y(z)) \in E(K)$. The map

$$\mathcal{M} \to E(K), \qquad z \mapsto (x(z), y(z)), 0 \mapsto \mathcal{O} \tag{IV.6}$$

is injective since it has a left inverse $(x, y) \mapsto -x/y$ (by IV.4).

What we are looking for is the formal power series giving formally the group law of $E$.

Recall that the change of coordinates we did at the beginning of this section leaves us in the $(z, w)$-plane, where a point $(z_0, w_0)$ is in $E$ if and only if $w_0 = f(z_0, w_0)$. (IV.3). What we want is the group law on this plane.

First, we compute the third point of intersection, $(z_3, w_3)$, of $E$ with the line through the two points of $E$ that we are adding. Then the addition of the two points is the inverse of $(z_3, w_3)$ but we ought to make all computations with power series.

Let $z_1, z_2$ be indeterminates and $w_i = w(z_i)$ for $i = 1, 2$, so that if $z_i \in \mathcal{M}$, then $(z_i, w_i)$ is a point of $E(K)$. The line connecting $(z_1, w_1)$ and $(z_2, w_2)$ has slope:

$$\lambda = \lambda\left(z_1, z_2\right) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}\left[a_1, \ldots, a_6\right]\left[\left[z_1, z_2\right]\right]$$

by (IV.3.1). We understand that $A_0 = 1$. Let's note that $\lambda(z_1, z_2)$ only has terms of degree 2 or greater since the division $\frac{z_2^n - z_1^n}{z_2 - z_1}$ is exact and results in a homogeneus polynomial of degree $n - 1$.

We let

$$\nu = \nu\left(z_1, z_2\right) = w_1 - \lambda z_1 \in \mathbb{Z}\left[a_1, \ldots, a_6\right]\left[\left[z_1, z_2\right]\right]$$

so the line we were looking for has equation: $w = \lambda z + \nu$. If we substitute this into the equation for $E$: $w = f(z, w)$ we get a cubic $g(z)$, and two of itse roots must be $z_1$ and $z_2$. The third root is the $z$-coordinate of the third point of intersection of the line $w = \lambda z + \nu$ with $E$. By actually making the substitution of the line into $E$, and equating the second-degree term of $g$ to $(-z_1 - z_2 - z_3)$, times the leading coefficient, we arrive at:

$$\begin{aligned} z_3 &= z_3\left(z_1, z_2\right) \\ &= -z_1 - z_2 + \frac{a_1 \lambda + a_3 \lambda^2 + a_2 y + 2 a_4 \lambda \nu + 3 a_6 \lambda^2 \nu}{1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3} \in \mathbb{Z}\left[a_1, \ldots, a_6\right]\left[\left[z_1, z_2\right]\right] \end{aligned}$$

since $1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$ is a unit in $\mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$.

We then let $w_3 = \lambda(z_1, z_2)\, z_3(z_1, z_2) + \nu(z_1, z_2)$. Since $(z_1, w_1), (z_1, w_1)$ and $(z_3, w_3)$ are collinear on $E$, they add to $O$ in the $(z, w)$-plane using the group law. Furthermore we have $w(z_3) = f(z_3, w(z_3))$ because $(z_3, w_3) \in E$ by construction, so we must have $w_3 = w(z_3)$, since $w(z_3)$ is the only power series verifying $w(z_3) = f(z_3, w(z_3))$ by Proposition IV.3.1.

So far we have

$$(z_3, w_3) = -\left((z_1, w_1) + (z_2, w_2)\right).$$

So we need the formula for the negative of a point in the $(z, w)$ plane. If suffices to have the formula $i(z)$ for the $z$-coordinate of the negative a point, since then $(z_1, w_1) + (z_2, w_2) = (i(z_3), w(i(z_3)))$.

In the $(x, y)$-plane, the inverse of $(x, y)$ is $(x, -y - a_1x - a_3)$. Using that $z = -x/y$ we find that the $z$-coordinate of the inverse in the $(z, w)$-plane is:

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} - a_1z^{-1} - \cdots}{-z^{-3} + 2a_1z^{-2} + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][[z]] \tag{IV.7}$$

The $w$-coordinate of the inverse $(z, -y - a_1x - a_3)$ is:

$$w' = -\frac{1}{y} = \frac{z^3}{-1 + 2a_1z + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][[z]].$$

Since $(i(z), w') \in E$, it verifies $w' = f(i(z), w')$ and, as before, $w(i(z))$ is the only power series with this property by Proposition IV.3.1, so we must have $w' = w(i(z))$.

We have arrived at the power series giving formally the $z$-coordinate of the sum of the points $(z_1, w_1), (z_2, w_2)$:

$$\begin{aligned} F(z_1, z_2) &= i(z_3(z_1, z_2)) \\ &= z_1 + z_2 - a_1z_1z_2 - a_2\left(z_1^2z_2 + z_1z_2^2\right) \\ &\quad + \left(2a_3z_1^3z_2 + (a_1a_2 - 3a_3)\, z_1^2z_2^2 + 2a_3z_1z_2^3\right) + \cdots \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]] \end{aligned}$$

Although it is very tedious, we can compute as many terms as we want since, as we did at the begining of this section, we can compute arbitrarily many of the polynomials $A_i \in \mathbb{Z}[a_1, \ldots, a_n]$ by making more subtutions of the equation $w = f(z, w)$ to itself. This allows us to compute also as many terms as we want of $\lambda$ and $\nu$ and therefore also of $z_3$. The same goes for $i(z)$ in (IV.7), so we can compute $F(z_1, z_2)$.

$F(z_1, z_2)$ is in fact a formal group since we have:

$$F(z_1, z_2) = z_1 + z_2 + \text{ higher-order terms}$$

and the conmmutativity and associativity of the group law inmediately imply:

$$F(z_1, z_2) = F(z_2, z_1)$$
$$F(z_1, F(z_2, z)) = F(F(z_1, z_2), z).$$

Furthermore, $i(z)$ is, as the notation suggest, the inverse for the formal group law:

$$F(z, i(z)) = z\text{-coordinate of the origin } (0{,}0) \ = 0.$$

**Definition IV.3.2.** *(Formal group of an elliptic curve). For an elliptic curve $E/R$, the power series $F(z_1, z_2)$ described above define a formal group (over $R$) called the formal group associated to $E$, denoted $\widehat{E}$.*

**Observation IV.3.3.** We have described $F(z_1, z_2)$ for $z_1 \neq z_2$ since we have used the expresion $\frac{z_2^n - z_1^n}{z_2 - z_1}$. But this expression also has a limit when $z_2 \to z_1$ so the expresion for $F(z_1, z_2)$ is always valid.

When $E$ is defined over a local ring $R$ complete with respect to the maximal ideal $\mathcal{M}$, then $F(z_1, z_2)$ is continuous in $\mathcal{M} \times \mathcal{M}$. Furthermore, in this case, the power series $x(z), y(z)$ give a well defined map

$$\mathcal{M} \longrightarrow E(K), \quad z \longrightarrow P_z = (x(z), y(z))$$

that is a group morphism between $\widehat{E}$ and $E(K)$ since by construction $P_{F(z,z')} = P_z + P_{z'}$ for $z \neq z'$ and we sorted out above what happens for $z = z'$.

# Chapter V

# The Néron-Ogg-Shafarevich Criterion

First, we fix the following notation for the entire chapter.

- $K$ will be a complete field with respect to a discrete normalized valuation $v$.
- $|\cdot|$ any of the (equivalent) nonarchimedean absolute values asociated to $v$.
- $R = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$ the valuation ring[†] of $K$
- $R^\times = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$ the group of units of $R$.
- $\mathcal{M} = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}$ the maximal ideal of $R$.
- $\pi$ a uniformizer of $R$, i.e. a generator of $\mathcal{M}$. Recall that every $x \in K^\times$ is of the form $x = u\pi^n$ with $n \in \mathbb{Z}, u \in R^\times$.
- $k = R/\mathcal{M}$ the residue field of $R$.

We further assume that $K$ and $k$ are always perfect.

In other words, in this chapter we are going to use the modern definition of *Local Field*: A perfect field $K$ complete with respect to a discrete valuation and with residue field $k$ also perfect. Nonetheless, we will reserve the term *Local Field* for the smaller class of fields that satisfies the classic definition, i.e. when $k$ is finite. Even though in practice almost all fields we use are local fields in the classical sense, we will need that the results in these chapters do not rely on the fact that $k$ is finite, because in the proof of the Criterion we will work with extensions of $K$ whose residue field is algebraically closed.

The concepts and tools developed in this chapter are all oriented to prove the Criterion of Néron-Ogg-Shafarevic, and can all be found in Silvermans's book [16], mainly in Chapter VII. **The notation and some results about elliptic curves that we will use in this chapter can be found in Appendix A.**

[†] I do not denote the valuation ring as $\mathcal{O}$ because here $\mathcal{O}$ is reserved for the point at infinity (zero element of the group) of our elliptic curves.

## V.1 Minimal Weierstrass Equations

Let $E/K$ be an elliptic curve with Weierstrass equation:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

At first the coefficients are only in $K$, but if we make the substitution $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ followed by multipliying the equation by $u^6$ we obtain a new Weierstrass equation:

$$E : y^2 + a_1uxy + a_3u^3y = x^3 + a_2u^2x^2 + a_4u^4x + a_6u^6$$

in which the original coefficients $a_i$ has been replaced by $u^ia_i$. Therefore, if we take $u = \pi^n$ for a sufficiently large $n \in \mathbb{N}$, by this method we obtain a Weierstrass equation whose coefficients are all in $R$, so we have $\Delta \in R$, i.e. $v(\Delta) \geq 0$. Now, since $v$ is discrete, among all Weiertrass equations with coefficients in $R$, we can choose one that minimizes the quantity $v(\Delta)$, so we have the following definition.

**Definition V.1.1.** *Let $E/K$ be an elliptic curve. A minimal Weierstrass equation (for $E$ at $v$) is a Weierstrass equation for $E/K$ that minimizes de value $v(\Delta)$ subject to the conditions that its coefficients are all in $R$.*

*The minimal value of $v(\Delta)$ under this conditions is called the minimal discriminant of $E$ at $v$.*

As proven above, we have:

**Proposition V.1.2.** *Every elliptic curve $E/K$ has a minimal Weierstrass equation.*

Following the notation established in (A.3), we have

**Proposition V.1.3.** *Let $E/K$ be an elliptic curve with a Weierstrass equation with coefficients in $R$. Then any of the following conditions are sufficient for the equation to be minimal.*

1. $v(\Delta) < 12$.
2. $v(c_4) < 4$.
3. $v(c_6) < 6$.

*Proof.* If $a_i \in R$ for all $i$, then obviously $\Delta, c_4, c_6 \in R$. By (A.3) we know that any change of variables that produces a new Weierstrass equation* has as new discriminat $\Delta' = u^{-12}\Delta$ and that also $c_4' = u^{-4}c_4, c_6' = u^{-6}c_6$, for some $u \in K$. So $v(\Delta), v(c_4)$ and $v(c_6)$ can only be changed by multiples of 12, 4 and 6 respectively, which added to the condition $v(\Delta), v(c_4), v(c_6) \geq 0$ gives us the result. □

If $\operatorname{char} k \neq 2, 3$, then we only need to look at $\Delta$ and $c_4$. More precisely:

*We will denote the quantities related to the new equation with a prime.

**Proposition V.1.4.** *Let $E/K$ be an elliptic curve with a Weierstrass equation with coefficients in $R$. If $\operatorname{char} k \neq 2, 3$, then the equation is minimal if and only if $v(\Delta) < 12$ or $v(c_4) < 4$. Furthermore, we can always find a minimal* ***reduced*** *Weierstrass form.*

Before the proof is worth noticing the following

**Observation V.1.5.** If $\operatorname{char}(k) \neq p$, then $\operatorname{char}(K) \neq p$.

This is true in a more general set up. Assume $R$ is a subring of $K$ with a maximal ideal $\mathfrak{m}$ and that $k = R/\mathfrak{m}$. If $\operatorname{char}(K) = p$, then $\underbrace{1_R + \cdots 1_R}_{p \text{ times}} = 0$. Reducing modulo $\mathfrak{m}$, we have $\underbrace{1_k + \cdots 1_k}_{p \text{ times}} = 0$, so that $\operatorname{char} k$ is positive and divides $p$, hence $\operatorname{char}(k) = p$.

*Proof.* (of Proposition V.1.4) The "*if*" part has already been proved above. Assume that we have a minimal equation $y^2 = x^3 + Ax + B$. Recall that $c_4 = -48A$ and $\Delta = -16(4A^3 + 27B^2)$. Assume that $v(\Delta) \geq 4$ and $v(c_4) \geq 12$. Then

$$4 \leq v(c_4) = v(48) + v(A) = v(A)$$
$$2v(B) = v(-B^2) = v(\Delta + 16 \cdot 4A^3) \geq \min\{v(\Delta), 3v(A)\} \geq 12$$

where we have used that $v(2^n 3^m) = nv(2) + mv(3) = 0$ for every $m, n \in \mathbb{Z}$, because $\operatorname{char}(k) \neq 2, 3$. In other words, we have $v(A) \geq 4$ and $v(B) \geq 6$. Then we make the change of coordinates:

$$x = \pi^2 x', \qquad y = \pi^3 y'$$

and we get a new reduced Weierstrass equation:

$$(y')^2 = (x')^3 + A'x + B', \qquad \text{where } A' = \pi^{-4}A, B' = \pi^{-6}B.$$

Now $v(A') = v(\pi^{-4}A) = -4 + v(A) \geq 0$ and $v(B') = v(\pi^{-6}B) = -6 + v(A) \geq 0$ which means that our new equation $(y')^2 = (x')^3 + A'x + B'$ has coefficients in $R$ and

$$0 \leq v(c_4') = v(c_4) - 4 < v(c_4)$$
$$0 \leq v(\Delta') = v(\Delta) - 12 < v(\Delta).$$

Which contradicts the fact that our original equation was minimal. Therefore we must have either $v(\Delta) < 12$ or $v(c_4) < 4$.

Finally, since $\operatorname{char}(k) \neq 2, 3$ implies that $\operatorname{char}(K) \neq 2, 3$, every elliptic curve $E$ has a reduced Weierstass equation $y^2 = x^3 + Ax + B$, not necessarily minimal. We can get the coefficients to lie in $R$ easily as we described at the beginning of the section. Then we can repeat the process described above, always obtaining a reduced Weierstrass equation over $R$, until either $v(\Delta) < 12$ or $v(c_4) < 4$ and then our equation would be minimal. This proves we can always get a minimal reduced Weiertrass equation. □

**Example V.1.6.** The Weierstrass equation

$$y^2 = x^3 + x$$

has discriminant $\Delta = -2^6$, so by (V.1.3) is minimal over $\mathbb{Q}_p$ for all primes $p$.

Now we characterize all the changes of variables that achieve and maintain the minimality of a Weierstrass equation. Note that if the coefficients $a_i$ of a Weierstrass equation for $E$ are in $R$, then every quantity in (A.3) is also is $R$, except maybe the $j$-invariant, since all of them are polynomial in the $a_i$. In particular this is true for minimal Weierstrass equations.

**Proposition V.1.7.** *(a) A minimal Weierstrass equation is unique up to change of variables*

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t \tag{V.1}$$

*with $u \in R^\times$ and $r, s, t \in R$.*

*(b) Conversely, if a change of coordinates (V.1) transforms a Weierstrass equation into a minimal one, then $u, r, s, t \in R$.*

*Proof.* (a) We know from (A.1.2) that any change of variables that transforms a Weierstrass equation into another is of the form (V.1) with $u, r, s, t \in K, u \neq 0$. If both our original Weierstrass equation and the new one are minimal, then $v(\Delta) = v(\Delta')$, and since $u^{12}\Delta' = \Delta$, we must have $v(u) = 0$, i.e., $u \in R^\times$. The transformation formulas for $b_6$ and $b_8$ are respectively

$$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$$
$$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4.$$

First, we notice that $v(4)$ and $v(3)$ cannot both be positive because otherwise $0 = v(1) = v(4-3) \geq \min\{v(3), v(4)\} > 0$, a contradiction.

Suppose first that $v(4) = 0$, then the above transformation formula for $b_6$ tells us that:

$$4r^3 = d_0 + d_1r + d_2r^2, \quad d_i \in R.$$

And taking valuations, while writing $n = v(r)$, we have:

$$3n = v(4r^3) = v(d_0 + d_1r + d_2r^2) \geq \min(v(d_0), v(d_1r), v(d_2r^2)) \geq \min(0, n, 2n).$$

If $n < 0$, then we have $3n \geq 2n$, i.e. $n \geq 0$, a contradiction. So we must have $v(r) = n \geq 0$.

In the other case, $v(3) = 0$, working with the transformation formula for $b_8$ we get exactly the same result. Therefore $r \in R$.

The transformation formula for $a_2$ is:

$$u^2a_2' = a_2 - sa_1 + 3r - s^2.$$

Which then translates again into

$$s^2 = d_0 + d_1s, \text{ for some } d_i \in R.$$

So $2v(s) = v(s^2) = v(d_0 + d_1s) \geq \min(0, v(s))$. This implies, as it did with $r$, that $v(s) \geq 0$.

The transformation formula for $a_6$ is:

$$u^6 a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1$$

And again we write it as:

$$t^2 = d_0 + d_1 t, \text{ for some } d_i \in R$$

So $2v(t) = v(t^2) = v(d_0 + d_1 t) \geq \min(0, v(t))$. This implies again that $v(t) \geq 0$.

We have proven that $r, s, t \in R$. It is worth noticing that the order in doing so has been important.

(b) Since the new equation is minimal, we must have $v(\Delta') \leq v(\Delta)$. But $u^{12}\Delta' = \Delta$ so it follows that $v(u) \geq 0$, i.e. $u \in R$. Now we can repeat the proof in (a) to obtain that $r, s, t \in R$, in that order. □

## V.2 Reduction Modulo $\pi$

We denote the natural projection map from $R$ to its residue field by a tilde:

$$R \to R/\mathcal{M}, \qquad t \mapsto \tilde{t} = t + \pi R.$$

Let $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(K)$. Then dividing by the coordinate with the greatest absolute value (in particular it is nonzero), we get coordinates for $P$ that are all in $R$ and at least one is in $R^\times$.

Then it makes sense to reduce them modulo $\pi$, which gives us a map:

$$\mathbb{P}^n(K) \to \mathbb{P}^n(k), \qquad P = [x_0 : \cdots : x_n] \mapsto \widetilde{P} = [\tilde{x}_0 : \cdots : \tilde{x}_n]$$

that is well defined, because we are dividing by a coordinate, which cancels out the scalar factor that relates two different representatives of $P$. To make the reduction of $P$, of course, we need to have all the coordinates of $P$ lying in $R$ and at least one of them in $R^\times$, but we have just seen that this is always possible.

We are interested in this map for $\mathbb{P}^2(K)$. More specifically, to its restriction to $E(K)$, which will also be denoted by a tilde.

Having chosen a minimal Weierstrass equation for $E/K$, we can reduce its coefficients modulo $\pi$, so we get a possibly singular curve over $k$:

$$\widetilde{E} : y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6.$$

The curve $E/k$ is called the *reduction of $E$ modulo $\pi$*. The fact that we started with a minimal Weierstrass equation for $E$ guarantees us (Proposition V.1.7) that this new equation is unique up to the standard changes of variables (A.1.2 (b)) over $k$.

Of course, if a point satisfies the minimal Weierstrass equation of $E$, taking the reduction modulo $\pi$ shows us that $\widetilde{P} \in \widetilde{E}(k)$. So the reduction modulo $\pi$ restricts to a map:

$$E(K) \to \widetilde{E}(k), \qquad P = [x_0 : x_1 : x_2] \mapsto \widetilde{P} = [\tilde{x}_0 : \tilde{x}_1 : \tilde{x}_2].$$

**Observation V.2.1.** If $E_1$ and $E_2$ are two elliptic curves and $\phi : E_1 \to E_2$ is a map verifying

1. $\phi(-P) = -\phi(P)$ for every $P \in E_1$.
2. $P_1 + P_2 + P_3 = \mathcal{O} \implies \phi(P_1) + \phi(P_2) + \phi(P_3) = \mathcal{O}$,

then $\phi$ is a group morphism. This is because under these assumptions:

$$\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$$

Even though $\widetilde{E}/k$ may be singular, $\widetilde{E}_{\mathrm{ns}}(k)$ is always a group (Proposition A.2.6). We define the following subsets of $E(K)$:

$$\begin{aligned} E_0(K) &= \left\{ P \in E(K) : \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(k) \right\} \\ E_1(K) &= \{ P \in E(K) : \widetilde{P} = \widetilde{\mathcal{O}} \} \end{aligned}$$

We say that $E_0(K)$ are the points with *nonsingular reduction* and $E_1(K)$ is the kernel of the reduction.

$E_1(K)$ is obviously a subgroup of $E(K)$. $E_0$ is also a subgroup, but this is not inmediate. In fact, it is part of the following:

**Proposition V.2.2.** *There is an exact sequence of abelian groups*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E}_{\mathrm{ns}}(k) \longrightarrow 0$$

*where the right-hand map is reduction modulo $\pi$ and the left-hand map is the inclusion.*

*Proof.* Since $E_1$ is the kernel of the reduction and is a subset of $E_0(K)$, there are three things to prove:

1. The reduction modulo $\pi$ map $E_0(K) \longrightarrow \widetilde{E}_{\mathrm{ns}}(k)$ is surjective.
2. $E_0(K)$ is a subgroup of $E(K)$
3. The reduction modulo $\pi$ map is a group morphism.

To prove the first, let

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

be a minimal equation for $E$. After reducing it modulo $\pi$ we get an equation $\tilde{f}(x, y)$ for $\widetilde{E}$. Let $\widetilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in \widetilde{E}_{\mathrm{ns}}(k)$. Since $\widetilde{P}$ is nonsingular, we must be in at least one of the following situations:

$$\frac{\partial \tilde{f}}{\partial x}(\widetilde{P}) \neq 0 \quad \text{or} \quad \frac{\partial \tilde{f}}{\partial y}(\widetilde{P}) \neq 0.$$

Assume we are in the first case. Let $y_0 \in R$ such that $\tilde{y}_0 = \tilde{\beta}$. Then the equation $f(x, y_0) = 0$, when reduced modulo $\pi$ has $\tilde{\alpha}$ as a single root since $(\partial \tilde{f}/\partial x)(\tilde{\alpha}, \tilde{y_0}) \neq 0$. Since $K$ is complete with respect a discrete valuation, Hensel's Lemma (I.2.12) tells us that we can lift this mod $\pi$ root $\tilde{\alpha}$ to a $x_0 \in R$ such that $\tilde{x}_0 = \tilde{\alpha}$ and $f(x_0, y_0) = 0$. This implies that $Q = (x_0, y_0) \in E(K)$ and $\widetilde{Q} = \widetilde{P}$, so $Q \in E_0(K)$. The case $\frac{\partial \tilde{f}}{\partial y}(\widetilde{P}) \neq 0$ is carried out in exactly the same way, lifting the root $\tilde{\beta}$ of the the reduction of $f(x_0, y)$ to some $y_0$ such that $f(x_0, y_0) = 0$.

To prove that $E_0(K)$ is a subgroup of $E(K)$, observe that both the group laws of $E(K)$ and $\widetilde{E}_{\mathrm{ns}}(k)$ are defined by taking intersections in $\mathbb{P}^2(K)$ and $\mathbb{P}^2(k)$ respectively. For any line of $\mathbb{P}^2(K)$ we can find an equation:

$$L : Ax + By + cZ = 0$$

with $A, B, C \in R$ and one of them in $R^\times$. Then it makes sense to take the reduction of its coefficients:

$$\widetilde{L} : \widetilde{A}x + \widetilde{B}y + \widetilde{C}z = 0.$$

If a point $P$ is in $L$ then obviously $\widetilde{P} \in \widetilde{L}$.

The reduction map obviously sends $\mathcal{O} \in E(K)$ to $\widetilde{E}_{\mathrm{ns}}(k)$. Let $P = (x, y) \in E_0(K)$. Then

$$\widetilde{(-P)} = (\tilde{x}, -\tilde{y} - \tilde{a_1}\tilde{x} - \tilde{a_3}) = -(\tilde{x}, \tilde{y}) = -\widetilde{P}.$$

Since $\widetilde{E}_{\mathrm{ns}}(k)$ is a group:

$$P \in E_0(K) \implies \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(k) \implies -\widetilde{P} = \widetilde{(-P)} \in \widetilde{E}_{\mathrm{ns}}(k) \implies -P \in E_0(K).$$

By Observation (V.2.1), it suffices to show that if three points are collinear (they add up to $\mathcal{O}$), their reductions are also collinear in $\widetilde{E}_{\mathrm{ns}}(K)$.

With all this in mind, let $P_1, P_2 \in E_0(K)$ and $P_3 \in E(K)$ such that $P_1 + P_2 + P_3 = \mathcal{O}$. So there is a line $L$ that intersects $E$ at $P_1, P_2, P_3$ with the appropriate multiplicities. (for example, if $P_1 = P_2 \neq P_3$, then $L$ intersects $E$ at $P_1$ with multiplicity 2 and at $P_3$ with multiplicity 1). If we prove that $\widetilde{L}$ intersects $\widetilde{E}$ at $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}$ with the corresponding multiplicities, i.e. $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = \widetilde{\mathcal{O}}$, it will follow that $\widetilde{P}_3 = -(\widetilde{P}_1 + \widetilde{P}_2) \in E_{\mathrm{ns}}(k)$, so $P_3 \in E_0(k)$. This would imply that the reduction modulo $\pi$ sends sums of points of $E_0(K)$ to the sum of the reduced points in $E_{\mathrm{ns}}(k)$. So $E_0$ a subgroup of $E(K)$ and the reduction map is a morphism.

It only remains to prove that $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = \widetilde{\mathcal{O}}$. There are many cases to consider, and we will show only the first one, since the rest are quite lenghty.

First, assume that $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3 = \widetilde{\mathcal{O}}$ are all distinct. Then

$$\widetilde{L} \cap \widetilde{E} = \left\{ \widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3 \right\}$$

are all distinct points and therefore $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = \widetilde{\mathcal{O}}$.

The case where two distinct points have the same reduction can be found in [16, Proposition 2.1, Ch. VII, pages 189,190], and the rest are similar to this last one ([16, Exercise 7.15, page 205]). □

**Proposition V.2.3.** *Let $E/K$ be given by a minimal Weierstrass equation, let $\widehat{E}/R$ be the formal group associated to $E$ as in IV.3.2, and let $w(z) \in R[x]$ be the power series from IV.3.1. Then the map*

$$\widehat{E}(\mathcal{M}) \longrightarrow E_1(K), \quad z \longmapsto \left( \frac{z}{w(z)}, -\frac{1}{w(z)} \right)$$

*is an isomorphism of groups. (We understand that $z = 0$ goes to $\mathcal{O} \in E_1(K)$).*

*Proof.* We have

$$w(z) = z^3(1 + \dots) \in R[[z]]$$

so $w(z)$ converges for every $z \in \mathcal{M}$ and $(x, y) = (z/w(z), -1/w(z)) \in E(K)$ (see IV.3.1).

Furthermore, the reduction of $[z/w(z) : -1/w(z) : 1] = [-z : 1 : -w(z)]$ is $[0 : 1 : 0] = \mathcal{O}$, which shows that $(z/w(z), -1/w(z)) \in E_1(K)$. Furthermore the map:

$$\widehat{E}(\mathcal{M}) \longrightarrow E_1(K), \quad z \longmapsto \left( \frac{z}{w(z)}, -\frac{1}{w(z)} \right) \tag{V.2}$$

is injective since it has left inverse $(x, y) \mapsto -x/y$. It is also a group morphism because the group law of $\widehat{E}(\mathcal{M})$ was computed using the group law of $E$ in the $(z, w)$ plane, and this map simply changes $E$ from the $(z, w)$-plane to the $(x, y)$-plane (See Observation IV.3.3). It remains to see that it is surjective.

Let $(x, y) \in E_1(K)$. A representative of $[x : y : 1]$, with homogeneous coordinates in $R$, must reduce to the point at infinity $\mathcal{O} = [0 : 1 : 0]$. Such a set of coordinates is obtained dividing by the coordinate of $[x : y : 1]$ with maximum absolute value. Therefore $y$ cannot be zero and we must have $\max\{|x|, |y|\} = |y| > 1$. So $[x : y : 1] = [x/y : 1 : 1/y]$ and $[x/y : 1 : 1/y]$ can be reduced directly to $\mathcal{O}$ modulo $\mathcal{M}$. In particular, $-x/y \in M$ and the map:

$$E_1(K) \longrightarrow \widehat{E}(\mathcal{M}), \quad (x, y) \longmapsto z = -\frac{x}{y} \tag{V.3}$$

is well defined. It is clearly injective since it has the previous map (V.2) as a left inverse.

We have proved that both morphisms (V.2) and (V.3) are isomorphisms since they are mutual inverses. □

## V.3 Good and Bad Reduction

Let $E/K$ be an elliptic curve. The reduction $\widetilde{E}$ can only be of three types, according to a basic general result on elliptic curves: nonsingular, singular with a node or singular with a cusp (Proposition A.1.5). In accordance, we define:

**Definition V.3.1.** *Let $E/K$ be an elliptic curve, and let $\widetilde{E}$ be the reduction modulo $\mathcal{M}$ of a minimal Weierstrass equation for $E$.*

1. *(a) $E$ has good (or stable) reduction if $\widetilde{E}$ is nonsingular.*
2. *(b) $E$ has multiplicative (or semistable) reduction if $\widetilde{E}$ has a node.*
3. *(c) $E$ has additive (or unstable) reduction if $\widetilde{E}$ has a cusp.*

*In cases (b) and (c) we say that $E$ has bad reduction. If $E$ has multiplicative reduction, then the reduction is said to be* split *if the slopes of the tangent lines at the node are in $k$, and otherwise it is said to be* nonsplit.

**Proposition V.3.2.** *Let $E/K$ be an elliptic curve given by a minimal Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Let $\Delta$ be the discriminant of this equation, and let $c_4$ be the usual expression involving $a_1, \ldots, a_6$ as described in (A.3).*

*(a) $E$ has good reduction if and only if $v(\Delta) = 0$, i.e., $\Delta \in R^\times$. In this case $\widetilde{E}/k$ is an elliptic curve.*

*(b) $E$ has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$ i.e., $\Delta \in \mathcal{M}$ and $c_4 \in R^\times$. In this case $\widetilde{E}_{ns}$ is the multiplicative group,*

$$\widetilde{E}_{\text{ns}}(\overline{k}) \cong \overline{k}^\times.$$

*(c) $E$ has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$ i.e., $\Delta, c_4 \in \mathcal{M}$. In this case $\widetilde{E}_{ns}$ is the additive group*

$$\widetilde{E}_{\text{ns}}(\overline{k}) \cong \overline{k}^+.$$

*Proof.* Its a direct consequence of Definition V.3.1 and Proposition A.2.6. Notice that for every $x \in R$

$$v(x) > 0 \iff \tilde{x} = 0.$$

□

**Observation V.3.3.** The reduction type of $E$ over $K$ does not depend on the minimal Weierstrass equation of $E$, since any two such equations are related by a change of coordinates of the form:

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t$$

with $u \in R^\times$. And since $\Delta = u^{12}\Delta'$ and $c_4 = u^4c_4'$, we have $v(\Delta) = v(\Delta')$ and $v(c_4) = v(c_4')$, so both minimal equations give the same type of reduction for $E$.

**Example V.3.4.** Let $p \geq 5$ be a prime. We define the following elliptic curves over $\mathbb{Q}_p$:

$$E_1 : y^2 = x^3 + px^2 + 1; \quad E_2 = y^2 = x^3 + x^2 + p; \quad E_3 : y^2 = x^3 + p.$$

with respective discriminants:

$$\Delta_1 = -2^6p^3 - 3^3; \quad \Delta_2 = -2^6p - 3^3p^2; \quad \Delta_3 = -2^43^3p^2.$$

Reducing modulo $p$, we se that $E_1$ has good reduction over $\mathbb{Q}_p$, and $E_2, E_3$ have bad reduction. In fact, $\widetilde{c_4(E_2)} \neq 0$ and $\widetilde{c_4(E_3)} = 0$. Therefore, $E_2$ has multiplicative (split*) reduction, and $E_3$ has additive reduction.

Much more can be said about the types of reduction and how they change when the ground field is extended. See for example [16, Ch.7, §5]. The only result we are going to use in the proof of the criterion of Néron-Ogg-Shafarevich is:

**Proposition V.3.5.** *Let $E/K$ be an elliptic curve and $K'/K$ be an unramified extension. Then the reduction type of $E$ over $K$ (good,multiplicative or additive) is the same as the reduction type of $E$ over $K'$.*

*Proof.* We set the notation $R'$ for the valuation ring of $K'$ and $v'$ for the valuation on $K'$ extending $v$.

For arbitrary characteristic, this result follows from Tate's algorithm, which can be found in [14, Ch. IV, §9]. We prove the result in the cases where $\text{char}(k) \geq 5$, so that by Proposition V.1.4, $E$ has a minimal Weierstrass equation over $K$ of the form:

$$E : y^2 = x^3 + Ax + B$$

Being an extension of $K$, $\text{char}(K') \geq 5$, so we can find minimal Weierstrass equations for $E$ over $K'$ that are reduced. Let

$$x = \left(u'\right)^2 x', \quad y = \left(u'\right)^3 y'$$

be a change of coordinates that produces a reduced minimal Weierstrass equation over $K'$. The change of coordinates must be of this kind since these are the only change of coordinates that preserve the reduced Weierstrass form (see Appendix A, §1).

Since $K'/K$ is unramified we can find an $u \in K$ with the same valuation as $u'$, so that $u/u' \in {R'}^{\times}$. And we can replace $u'$ with $u$ in the change of variables that we used to get a minimal Weierstrass equation over $K'$:

$$x = u^2x', \quad y = u^3y'.$$

But this new equation has coefficients in $R$, so by the minimality of the original equation over $K$, we must have $v(u) = 0$. Therefore, the original equation was also minimal over $K'$. Since $v'$ extends $v$, we have $v(\Delta) = v'(\Delta)$ and $v(c_4) = v'(c_4)$, so it follows that the reduction type of $E$ over $K$ is the same as the reduction type of $E$ over $K'$. □

*The formulas for the slopes of the tangent lines at the singular point can be found in Appendix A. They involve a square root of a quantity of $k = \mathbb{F}_p$. If this square root exists in $\mathbb{F}_p$, then the multiplicative reduction is split, and if it isn't in $\mathbb{F}_p$, the reduction is nonsplit.

## V.4 The Tate Module

**Definition V.4.1.** *Let $E/K$ be an elliptic curve*. The $m$-torsion points of $E$, denoted $E[m]$, are the points whose order divides $m$, i.e.*

$$E[m] = \{P \in E : [m]P = 0\} = \ker([m]).$$

**Proposition V.4.2.** *Let $E/K$ be an elliptic curve. For every $m \in \mathbb{Z}$ relatively prime with* $\mathrm{char}(K)$ *we have an isomorphism of abelian groups:*

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

*Proof.* [16, Ch. 3, Corollary 6.4, page 86]. □

In particular, every $E[m]$ is finite. The above isomorphism does not holds over $K$ in general, only over the algebraically closed field $\overline{K}$. In other words, the inclusion $E(K)[m] \subset E[m]$ is strict in general.

There is a little more structure in $E[m]$, since every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$ thanks to Observation A.2.4:

$$[m]\left(P^\sigma\right) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}.$$

We thus obtain a representation

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

where the latter isomorphism involves choosing a basis for $E[m]$.

If order to get a characteristic 0 representation, we recreate the construction of the $\ell$-adics as the inverse limit of the finite groups $\mathbb{Z}/\ell^n\mathbb{Z}$, but with $E[\ell^n]$. So we define:

**Definition V.4.3.** *Let $E/K$ be an elliptic curve and $\ell \in \mathbb{Z}$ a prime number. The $\ell$-adic Tate module of $E$ is the group*

$$T_\ell(E) = \varprojlim E[\ell^n],$$

*the inverse limit being taken with respect to the natural maps*

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$ module, we see that the Tate module has a natural structure as a $\mathbb{Z}_\ell$ module.

Since $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$ for every $m \in \mathbb{Z}$, $\mathrm{Gal}(\overline{K}/K)$ **also acts on $T_\ell(E)$, componentwise.** This action is well defined due to the action of $\mathrm{Gal}(\overline{K}/K)$ commuting with the multiplication-by-$\ell$ map.

*Recall that if $E$ is defined over $K$, we understand that $E = E(\overline{K})$, i.e., a generic point $P \in E$ has coordinates in $\overline{K}$.

## V.5 Points of Finite Order

The points of finite order or *torsion points* of $E$ are:

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m]$$

and if $E$ is defined over $K$, we are usually interested in the corresponding subgroup: $E_{tors}(K) = E_{tors} \cap E(K)$. If $K$ is a number field, $E_{tors}(K)$ is always a finite group because the Mordell-Weil theorem tell us that $E(K)$ is a finitely generated (abelian) group, and $E_{tors}(K)$ is just its torsion subgroup, so it is finite.

In this section we analyze $E_{tors}(K)$, mainly by means of the next proposition, which will be a crucial tool in the proof of the Néron-Ogg-Shafarevich Criterion.

**Proposition V.5.1.** *Let $E/K$ be an elliptic curve and let $m \geq 1$ be an integer relatively prime to char($k$).*

*(a) The subgroup $E_1(K)$ has no nontrivial points of order $m$.*

*(b) Assume further that the reduced curve $\widetilde{E}/k$ is nonsingular. Then the reduction map*

$$E(K)[m] \longrightarrow \widetilde{E}(k)$$

*is injective, where $E(K)[m]$ denotes the set of points of order $m$ in $E(K)$.*

*Proof.* From Proposition V.2.3 we know that $E_1(K) \cong \widehat{E}(\mathcal{M})$. Our general result on formal groups IV.2.14 tell us that $\widehat{E}(\mathcal{M})$ has no nontrivial points of order $m$, so neither does $E_1(\mathcal{M})$. This proves (a).

Proposition V.2.2 gives us an exact sequence:

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E}_{\mathrm{ns}}(k) \longrightarrow 0.$$

If we assume that $\widetilde{E}$ is nonsingular, then $E_0(K) = E(K)$ and $\widetilde{E}_{\mathrm{ns}}(k) = \widetilde{E}(k)$. Since there is no nontrivial $m$-torsion of $E(K)$ in the kernel of the reduction map (i.e. in $E_1(K)$), the $m$-torsion of $E(K)$ injects into $\widetilde{E}(k)$, which proves (b). □

There is a stronger version for this result only valid when the curve is defined over $\mathbb{Q}$. If we have an elliptic curve

$$E : y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{Q}$$

Let $D$ be the least common denominator of $a, b$ and $c$. If we multiply the equation for $E$ by $D^6$ and make the change of coordinates

$$(D^2x, D^3, y) \mapsto (x, y)$$

we get an equation with integers coefficients $E' : y^2 = f(x)$, and of course:

$$(x, y) \in E(\mathbb{Q}) \Longleftrightarrow \left(D^2x, D^3y\right) \in E'(\mathbb{Q})$$

So that this change of coordinates is an isomorphism of algebraic varieties than preserve the rational points.

Now that we have and equation with integer coefficients, we can reduce modulo $p$ the coefficients (reduction modulo $p$ is again denoted with a tilde). If this reduced curve, $\widetilde{E}$, is nonsingular we say that $E$ has *good reduction* at $p$. We would need to know that under these conditions the points of $E(\mathbb{Q})_{\text{tors}}$ have integer coordinates, a result know as Nagell-Lutz Theorem. We only state the part that we are interested in.

**Theorem V.5.2.** *(Nagell-Lutz Theorem) Let*

$$y^2 = x^3 + ax^2 + bx + c$$

*be an elliptic curve with integer coefficients. If $P = (x, y)$ is a rational point of finite order, then $x, y \in \mathbb{Z}$.*

*Proof.* [15, Theorem 2.5, page 56] □

The result we mentioned before is as follows.

**Proposition V.5.3.** *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax^2 + bx + c = f(x)$, where $a, b, c \in \mathbb{Z}$, such that $E$ has good reduction at the prime $p \in \mathbb{Z}$. Then the map:*

$$\phi : E(\mathbb{Q})_{tors} \to \widetilde{E}(\mathbb{F}_p), \quad \mathcal{O} \mapsto \widetilde{\mathcal{O}}, \quad (x, y) \mapsto (\tilde{x}, \tilde{y})$$

*is an injective group morphism. Therefore, $E(\mathbb{Q})_{tors}$ is isomorphic to a subgroup of $\widetilde{E}(\mathbb{F}_p)$.*

Before seeing the proof, is worth noticing that this Proposition tell us that $|E(\mathbb{Q})_{\text{tors}}|$ divides $\left|\widetilde{E}(\mathbb{F}_p)\right|$ for every prime at which $E$ has good reduction. Therefore, it provides another proof for the finiteness of $E_{tors}(K)$, though only when $K = \mathbb{Q}$.

*Proof.* First of all, $\phi$ is well defined thanks to Theorem V.5.2. Next we show that $\phi$ is a morphism. We have

$$\phi(-P) = \phi(x, -y) = (\tilde{x}, -\tilde{y}) = -\phi(P)$$

Therefore, in order to prove $\phi(P + Q) = \phi(P) + \phi(Q)$, it suffices to show that if $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3) \in E(\mathbb{Q})_{\text{tors}}$ are collinear (add to $\mathcal{O}$) then

$$\phi(P) + \phi(Q) + \phi(R) = \widetilde{P} + \widetilde{Q} + \widetilde{R} = \widetilde{\mathcal{O}}.$$

This equation obviously holds if $P, Q$ or $R$ are $\mathcal{O}$ using that $\phi(-P) = -\phi(P)$. So we can assume that $P, Q, R \neq \mathcal{O}$, and since they are collinear affine points, we have:

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) \tag{V.4}$$

where $\lambda, \nu \in \mathbb{Q}$ and $y = \lambda x + \nu$ is the line that passes through the three points. Since $a, b, c, x_1, x_2, x_3$ are integers, $\lambda$ and $\nu$ must also be integers, so we can reduce (V.4) modulo $p$. This implies that $\widetilde{P}, \widetilde{Q}$ y $\widetilde{R}$ are collinear and therefore add up to $\widetilde{\mathcal{O}}$. This proves that $\phi$ is a morphism[*].

Because of how $\phi$ is defined we have $\ker(\phi) = \mathcal{O}$, so $\phi$ is injective. □

Next we show several illustrative examples of applications of this propositions. We first notice that: $E(\mathbb{Q}) \subset E(\mathbb{Q}_p)$ for every prime $p$.

Also, it is worth having in mind how to compute $E[2]$. In general, the condition $P = -P$ gives us a cubic polynomial in $x$, whose roots are the $x$-coordinates of the 3 affine points of $E[2]$. But when the curve has equation $E : y^2 = x^3 + ax^2 + bx + c = f(x)$, it is even easier. In this case

$$E[2] = \{\mathcal{O}, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}$$

where $\alpha_i, i = 1, 2, 3$ are the roots[†] of $f(x)$.

**Observation V.5.4.** If $E(K)[p] = \{\mathcal{O}\}$ for every prime $p$, then $E(K)[m] = \{\mathcal{O}\}$ for every $m \in \mathbb{Z}$ and therefore $E(K)_{tors} = \{\mathcal{O}\}$.

To see this write $m = pm'$ for a prime divisor $p$ of $m$. Then $p(m'P) = mP = \mathcal{O}$ implies $m'P = \mathcal{O}$, since $E(K)[p] = \{\mathcal{O}\}$. We can apply this reassoning to $m' = m/p$ and repeat it until there is only a prime factor remaining, which will imply that $P = \mathcal{O}$.

**Example 1.** Let $E/\mathbb{Q}$ be the elliptic curve

$$E : y^2 + y = x^3 - x + 1.$$

Its discriminant is $\Delta = -611$, so $\widetilde{E}$ is nonsingular modulo 2. It is immediate to see that $\widetilde{E}(\mathbb{F}_2) = \{\mathcal{O}\}$. Then Proposition V.5.1 tell us that for every prime number $p \neq 2$

$$E(\mathbb{Q}_2)[p] \hookrightarrow \widetilde{E}(\mathbb{F}_2) = \{\mathcal{O}\}.$$

So $E(\mathbb{Q})[p] \hookrightarrow E(\mathbb{Q}_2)[p] = \{\mathcal{O}\}$. But since it is easily checked that $E(\mathbb{Q})[2] = \{\mathcal{O}\}$, we have $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$.

We are going to solve the following example first with Proposition V.5.1 and next with Proposition V.5.3.

**Example 2.** (Using Proposition V.5.1) Let $E/\mathbb{Q}$ be the elliptic curve

$$E : y^2 = x^3 + x.$$

[*] We had already proven that the reduction map on $E(\mathbb{Q}_p)$ was a group morphism, so restricted to the subgroup $E(\mathbb{Q})_{\text{tors}}$ it is also a group morphism. But I have chosen to include this proof because is simpler, though only valid for $K = \mathbb{Q}$.

[†] The roots $\alpha_i$ are necessarily different since if $E$ is of the form $E : y^2 = x^3 + ax^2 + bx + c = f(x)$, then $E$ is non-singular if and only $f$ the 3 roots of $f(x)$ are simple.

Its discriminant is $\Delta = -64$, thus $E$ has good reduction modulo $p$ for every prime $p \neq 2$. The reduction modulo $p$ of $E$ will be denoted $\widetilde{E}_p$. We compute:

$$\begin{aligned} \widetilde{E}_3\left(\mathbb{F}_3\right) &= \{\mathcal{O}, (0,0), (2,1), (2,2)\} \cong \mathbb{Z}/4\mathbb{Z} \\ \widetilde{E}_5\left(\mathbb{F}_5\right) &= \{\mathcal{O}, (0,0), (2,0), (3,0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2. \end{aligned} \tag{V.5}$$

Using Proposition V.5.1, we have:

$$E(\mathbb{Q})[m] \subset E(\mathbb{Q}_3)[m] \hookrightarrow \widetilde{E}_3\left(\mathbb{F}_3\right) \cong \mathbb{Z}/4\mathbb{Z} \text{ for every integer } m \text{ coprime with 3.}$$

$$E(\mathbb{Q})[m] \subset E(\mathbb{Q}_5)[m] \hookrightarrow \widetilde{E}_5\left(\mathbb{F}_5\right) \cong (\mathbb{Z}/2\mathbb{Z})^2 \text{ for every integer } m \text{ coprime with 5.}$$

So for every integer $m$ coprime with 3 and 5, $E(\mathbb{Q})[m]$ inyects into both $\widetilde{E}_3\left(\mathbb{F}_3\right)$ and $\widetilde{E}_5\left(\mathbb{F}_5\right)$ so the only nontrivial $m$-torsion point must be a 2-torsion point that reduces to $(0,0)$. Since $(0,0)$ is effectively a point of order 2, this is the only nontrivial rational $m$-torsion point for $m$ relatively prime to 3 and 5.

Furthermore $E(\mathbb{Q})[3]$ is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$ where every nontrivial element has order 3, so $E(\mathbb{Q})[3] = \{\mathcal{O}\}$. $E(\mathbb{Q})[5]$ is a subgroup of $\mathbb{Z}/4\mathbb{Z}$ where every nontrivial element has order 5, so $E(\mathbb{Q})[5] = \{\mathcal{O}\}$. Therefore, there is no $m$-torsion if 3 or 5 divides $m$.

We have proven that $E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0)\}$.

**Example 2.** (Using Proposition V.5.3) As before the elliptic curve over $\mathbb{Q}$:

$$E : y^2 = x^3 + x$$

has good reduction modulo 2 and we have (V.5). Proposition V.5.3 tell us that $E(\mathbb{Q})_{tors}$ injects in both $\widetilde{E}_3\left(\mathbb{F}_3\right)$ and $\widetilde{E}_5\left(\mathbb{F}_5\right)$. As a consequence, $E(\mathbb{Q})_{tors}$ has $\mathcal{O}$ and a point $P$ of order 2 that reduces to $(0,0)$ as its two only possible points. The only rational root of $x^3 + x$ is 0. Therefore $E(\mathbb{Q})[2] = \{\mathcal{O}, (0,0)\}$, and hence

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0)\}.$$

**Example 3.** Let $E : y^2 = x^3 - x = x(x+1)(x-1)$.

We easily get $E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} = E(\mathbb{Q})[2]$, so $|E(\mathbb{Q})_{tors}| \geq 4$. In order to get an upper bound, we use Proposition V.5.3. Since $\Delta = 64$, $E$ has good reduction modulo $p = 3$. Making the reduction we get the curve $\widetilde{E} : y^2 = x^3 - x$ over $\mathbb{F}_3$. For every $x \in \mathbb{F}_3$ we have $x^3 - x = 0$, so that

$$\widetilde{E}\left(\mathbb{F}_3\right) = \{\widetilde{\mathcal{O}}, (0,0), (1,0), (2,0)\}.$$

(We see that this is just $E[2]$ reduced modulo 3). Therefore, $\left|\widetilde{E}\left(\mathbb{F}_3\right)\right| = 4$, which means that $|E(\mathbb{Q})_{tors}|$ divides 4. This implies $|E(\mathbb{Q})_{tors}| = 4$ and therefore

$$E(\mathbb{Q})_{tors} = E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

## V.6 The Action of the Inertia Group

Recall that the inertia subgroup $I_v$ of $\overline{K}/K$ is the set of elements of $\mathrm{Gal}(\overline{K}/K)$ that act trivially on the residue field $\overline{k}$, and that we had $I_v = \mathrm{Gal}(\overline{K}/K^{nr})$ (see the end of section III.3). Also recall the short exact sequence

$$1 \longrightarrow \mathrm{Gal}\left(\overline{K}/K^{\mathrm{nr}}\right) \longrightarrow \mathrm{Gal}\left(\overline{K}/K\right) \longrightarrow \mathrm{Gal}\left(\overline{k}/k\right) \longrightarrow 1$$

and that $\mathrm{Gal}\left(K^{\mathrm{nr}}/K\right) \cong \mathrm{Gal}\left(\overline{k}/k\right)$.

**Definition V.6.1.** *Suposse that* $\mathrm{Gal}\left(\overline{K}/K\right)$ *acts on a set* $\Sigma$. *We say that* $\Sigma$ *is unramified at* $v$ *if the action of* $I_v$ *on* $\Sigma$ *is trivial.*

From Section V.4 we know that $\mathrm{Gal}\left(\overline{K}/K\right)$ acts on $E[m]$ and $T_\ell(E)$

**Proposition V.6.2.** *Let* $E/K$ *be an elliptic curve with good reduction.*

*(a) Let* $m \geq 1$ *be an integer that is relatively prime to char(k), i.e., satisfying* $v(m) = 0$. *Then* $E[m]$ *is unramified at* $v$.

*(b) Let* $\ell$ *be a prime with* $\ell \neq \mathrm{char}(k)$. *Then* $T_\ell(E)$ *is unramified at* $v$.

*Proof.* Since $E[m]$ is finite, there exists a finite extension $K'/K$ such that $E[m] \subset E(K')$ (for example, $K(E[m])$). Let $v'$ be the valuation extending $v$ to $K'$. The notation $R', \mathcal{M}', k'$ is self explanatory.

The fact that $E$ has nonsingular reduction means that if we take a minimal Weierstrass equation for $E$ at $v$, the discriminant satisfies $v(\Delta) = 0 = v'(\Delta)$. Therefore, our Weierstrass equation is also minimal over $K'$ and the reduced curve $\widetilde{E}/k'$ is nonsingular. Then, Proposition V.5.1 (b) tells us that the reduction map:

$$E(K')[m] = E[m] \longrightarrow \widetilde{E}(k')$$

is injective.

Let $\sigma \in I_v$ and $P \in E[m]$. We have to prove that $P^\sigma = P$. What we know is that $\widetilde{P}^\sigma = \widetilde{P}$ because $\sigma$ acts trivially on $E(\overline{k}) \supset E(k')$, and since reduction is a homomorphism, we have:

$$\widetilde{P^\sigma - P} = \widetilde{P}^\sigma - \widetilde{P} = \widetilde{O}$$

Since $P^\sigma - P \in E[m]$, it must be $P^\sigma - P = \mathcal{O}$ by the above-mentioned injection.

(b) It is a direct consequence of (a) and the fact that the action of $\mathrm{Gal}\left(\overline{K}/K^{\mathrm{nr}}\right)$ on $T_\ell(E)$ is componentwise. □

This result is an important part of the Néron-Ogg-Shafarevich Criterion.

## V.7 The Proof of the Criterion

To prove the criterion, we need a previous result: the finiteness of the group $E(K)/E_0(K)$. As mentioned at the begining of the chapter, $K$ is any field complete with respect a discrete valuation, with residue field not necessarily finite, since we are going to need to apply this result to the extension $\widehat{K^{nr}}/K$ where $\widehat{K^{nr}}$ is the completion of maximal unramified extension of $K$. The result follows from the existence of the Néron model ([14], Ch. IV, §§5,6), which is a group scheme over $\mathrm{Spec}(R)$ with generic fiber $E/K$. The proof of the existence of this model is beyond the scope of this text. Nonetheless, we state our result exactly as we need it and give the proper reference.

**Lemma V.7.1.** *(Kodaira-Néron) Let $K$ be a complete discretely valued field. Then the group $E(K)/E_0(K)$ is finite.*

*Proof.* [14, Ch. IV, Corollary 9.2 (d), pag 362]. □

Now we can state and prove the Criterion.

**Theorem V.7.2.** *(Néron-Ogg-Shafarevich Criterion) Let $E$ be an elliptic curve over a complete, discretely valued field $K$. Let $p = \mathrm{char}(k)$. Then the following statements are equivalent:*

*(a) $E$ has good reduction.*

*(b) $E[m]$ is unramified at $v$ for all integers $m \geq 1$ that are relatively prime to $p$.*

*(c) The Tate module $T_\ell(E)$ is unramified for some (all) primes $\ell \neq p$.*

*(d) $E[m]$ is unramified at $v$ for infinitely many integers $m \geq 1$ that are relatively prime to $p$.*

*Proof.* We have already proven the implication $(a) \implies (b)$ in Proposition V.6.2 (a). Due to the action of $I_v$ on $T_\ell(E)$ being componentwise (i.e. $T_\ell(E)$ is unramified at $v$ if and only if $E[\ell^n]$ is unramified at $v$ for all $n \geq 1$), the implications $(b) \implies (c) \implies (d)$ are obvious. In $(b) \implies (c)$, $(c)$ should read "... for all primes $\ell \neq p$". In $(c) \implies (d)$ it suffices that $(c)$ reads "... for a prime $\ell \neq p$". It remains to prove that $(d) \implies (a)$.

Let $\widehat{K}^{nr}$ be the completion with respect to $v$ of the maximal unramified extension, $K^{nr}$, of $K$. Assume (d), then we can find $m \in \mathbb{Z}$ verifying:

(I) $m$ is relatively prime to $p$.

(II) $m > \#E(\widehat{K}^{nr})/E_0(\widehat{K}^{nr})$.

(III) $E[m]$ is unramified at $v$.

Let us recall that $E(\widehat{K}^{nr})/E_0(\widehat{K}^{nr})$ is a finite group thanks to the result of Kodaira-Néron (Lemma V.7.1), so all three properties of $m$ are guaranteed to coexist thanks to (d). Then we have the following short exact sequences:

$$\begin{array}{l} 0 \longrightarrow E_0\left(\widehat{K}^{\mathrm{nr}}\right) \longrightarrow E\left(\widehat{K}^{\mathrm{nr}}\right) \longrightarrow E\left(\widehat{K}^{\mathrm{nr}}\right)/E_0\left(\widehat{K}^{\mathrm{nr}}\right) \longrightarrow 0 \\ 0 \longrightarrow E_1\left(\widehat{K}^{\mathrm{nr}}\right) \longrightarrow E_0\left(\widehat{K}^{\mathrm{nr}}\right) \longrightarrow \qquad \widetilde{E}_{\mathrm{ns}}(\overline{k}) \qquad \longrightarrow 0. \end{array}$$

The first one is clear and the second one is from Proposition V.2.2, because the residue field of $\widehat{K}^{nr}$ is $\overline{k}$ (by Proposition I.2.7 the residue class field of $\widehat{K}^{nr}$ is the same as the one of $K^{nr}$, which is $k_s$, the separable closure of $k$. But since $k$ is perfect, we have $k_s = \overline{k}$).

$I_v$ acts trivially on $E[m]$, so for every $P = (x, y) \in E[m]$ and $\sigma \in I_v$, we have $\sigma(P) = P$. That is to say $P \in E[\overline{K}^{I_v}]$. And because $K^{nr} \subset \widehat{K}^{nr}$ is the fixed field of $I_v$, what we have said is tantamount to $E[m] \subset E(\widehat{K}^{nr})$. So $E(\widehat{K}^{nr})$ has a subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$. But from (II) we have that $\#E(\widehat{K}^{nr})/E_0(\widehat{K}^{nr}) < m$. Let us see that this implies that there exists a prime $\ell$ dividing $m$ such that $E_0(\widehat{K}^{nr})$ has a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. Let

$$\varphi : E[m] \longrightarrow E\left(\widehat{K}^{\mathrm{nr}}\right)/E_0\left(\widehat{K}^{\mathrm{nr}}\right)$$

be the quotient map restricted to $E[m]$ with kernel $E_0\left(\widehat{K}^{\mathrm{nr}}\right) \cap E[m]$. Since $E[m]/\ker\varphi$ is a subgroup of $E\left(\widehat{K}^{\mathrm{nr}}\right)/E_0\left(\widehat{K}^{\mathrm{nr}}\right)$, we must have

$$\#(E[m]/\ker\varphi) \leq \#\left(E\left(\widehat{K}^{\mathrm{nr}}\right)/E_0\left(\widehat{K}^{\mathrm{nr}}\right)\right) < m$$

If $E[m] = \mathbb{Z}_{P_1} \times \mathbb{Z}_{P_2}$ for $P_1, P_2$ points of exact order $m$, let $a, b \in \mathbb{Z}$ be divisors of $m$ so that $\ker\varphi \cong \mathbb{Z}_{aP_1} \times \mathbb{Z}_{bP_2} \subset E_0\left(\widehat{K}^{\mathrm{nr}}\right)$ (all subgroups of $E[m]$ are of this form). Now, if $a$ and $b$ are relatively prime, then $ab|m$. So

$$m \leq \frac{m}{ab}m = \#(E[m]/\ker\varphi) < m$$

which is a contradiction. So there exists a common prime divisor, $\ell$, of $a$ and $b$, and therefore $E_0\left(\widehat{K}^{\mathrm{nr}}\right)$ contains a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$.

Since $E_1\left(\widehat{K}^{\mathrm{nr}}\right)$ contains no nontrivial $\ell$-torsion (Proposition V.5.1 (a)), by the second exact sequence this means that $\widetilde{E}_{\mathrm{ns}}(\overline{k})$ contains a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$.

Now suppose that $E$ has bad reduction over $\widehat{K}^{nr}$. There are two cases to consider.

First suppose that the reduction is multiplicative, then by Proposition V.3.2, $\widetilde{E}_{\mathrm{ns}}(\overline{k}) \cong \overline{k}^{\times}$ as multiplicative groups, so the $\ell$-torsion is $\mu_\ell = \left\{x \in \overline{k}^{\times} \mid x^\ell = 1\right\} \cong \mathbb{Z}/\ell\mathbb{Z}$ ($\ell$-roots of unity), a contradiction because the $\ell$-torsion of $\widetilde{E}_{\mathrm{ns}}(\overline{k})$ should at least contain a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$.

If the reduction over $\widehat{K}^{nr}$ is additive then we have $\widetilde{E}_{\mathrm{ns}}(\overline{k}) \cong \overline{k}^{+}$ as additive groups, so $\widetilde{E}_{\mathrm{ns}}(\overline{k})$ cannot have $\ell$-torsion because $\ell$ is relatively prime to $\operatorname{char} k$.

Having discarded all types of bad reduction that $E$ could have, it follows that $E$ has good reduction over $\widehat{K}^{nr}$. Finally, since $\widehat{K}^{nr}/K$ is unramified*, we conclude, by Proposition V.3.5 that $E$ has good reduction over $K$.

$\square$

*$\widehat{K}^{nr}|K^{nr}$ may not be an algebraic extension, but its ramification index is clearly 1, which is the only thing we used to prove Proposition V.3.5. To see this note that, being the completion of $K^{nr}$, $\widehat{K}^{nr}$ has the same value group as $K^{nr}$, and of course $K^{nr}|K$ is unramified, so that their composite $\widehat{K}^{nr}|K$ has ramification index equal to 1.

# Appendix A

# Basic facts about Elliptic Curves

This appendix is basically a compilation of useful facts about elliptic curves that have been used throughout this text. They have been mostly taken from [16, Ch. III].

We begin by defining our main object of study:

**Definition A.0.1.** *An elliptic curve is a nonsingular curve of genus one together with a point $\mathcal{O} \in E$.*

We say that $E$ is *defined over* $K$, written $E/K$, if $E$ is defined over $K$ as an algebraic curve and $\mathcal{O} \in E(K)$. Recall that an algebraic variety, $V$, is defined over $K$ if its polynomial ideal $\mathcal{I}(V)$ can be generated by polynomials with coefficients in $K$. For an elliptic curve, this will mean that the coefficients of its equation are in $K$ even though the points of the curve are understood to be in $E(\overline{K})$.

## A.1 Weierstrass equations

**Definition A.1.1.** *A Weierstrass equation (over K) is an equation of the form:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*where $a_i \in K$ for all $i$.*

The curve defined by this equation is, of course, the set of points $[X : Y : Z] \in \mathbb{P}^2(\overline{K})$ that satisfy the homogeneous version of the previous equation:

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

As we can see, these curves have a single point in the line at infinity $Z = 0$, namely $\mathcal{O} = [0 : 1 : 0]$, which is never singular since $\frac{\partial F}{\partial Z}(\mathcal{O}) \neq 0$.

As the next proposition tell us, every elliptic curve can be thought of as a nonsingular, plane projective curve given by a Weierstrass equation.

**Proposition A.1.2.** *Let $E$ be an elliptic curve defined over $K$.*

*(a) There exist functions $x, y \in K(E)$ such that the map*

$$\phi : E \longrightarrow \mathbb{P}^2, \quad \phi = [x : y : 1]$$

*gives an isomorphism of $E/K$ onto a curve given by a Weierstrass equation*

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

*with coefficients $a_1, \dots, a_6 \in K$ and satisfying $\phi(O) = [0 : 1 : 0]$. The functions $x$ and $y$ are called Weierstrass coordinates for the elliptic curve $E$.*

*(b) Any two Weierstrass equations for $E$ as in (a) are related by a linear change of variables of the form*

$$X = u^2X' + r, \quad Y = u^3Y' + su^2X' + t$$

*with $u \in K^\times$ and $r, s, t \in K$.*

*(c) Conversely, every smooth cubic curve $C$ given by a Weierstrass equation as in (a) is an elliptic curve defined over $K$ with base point $\mathcal{O} = [0 : 1 : 0]$.*

*Proof.* [16, Ch. III, Proposition 3.1, pag 59] □

In the last proposition, (b) also tells us the form of every change of coordinates that preserves the Weierstrass form.

Sometimes, elliptic curves are defined as non-singular cubics, i.e., non-singular curves given by a cubic polynomial. It turns out that we can transform any cubic homogeneous polynomial $f(X, Y, Z) \in \mathbb{P}^2(K)$ into a Weierstrass equation over $K$ by means of projective transformations, which turn out to be rational functions over $K$. So the previous proposition tells us that the two definitions coincide. I covered this approach in [11].

Let $E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ be an elliptic curve. As showed before, $\mathcal{O}$ is non-singular. All the remaining points are affine. One such point $P = (x_0, y_0)$ is singular if:

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

In order to compute the tangent lines* of $E$ at $P$, we need to factor into linear equations the second-order term in the Taylor expansion of $f$ around $P$. We have:

$$\begin{array}{l} \frac{\partial f}{\partial x} = a_1y - 3x^2 - 2a_2x - a_4, \quad \frac{\partial f}{\partial y} = 2y + a_1x + a_3 \\ \frac{\partial^2 f}{\partial x^2} = -6x - 2a_2, \quad \frac{\partial^2 f}{\partial y^2} = 2, \quad \frac{\partial^2 f}{\partial x \partial y} = a_1 = \frac{\partial^2 f}{\partial y \partial x}. \end{array}$$

*For an algebraic curve $C$ given by the equation $f(x, y) = 0$, at a singular point $P$, even though you cannot define *the tangent line* by the usual formula due to $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$, what happens is that there are more than one tangent (or one with multiplicity greater than one). For a point $P = (x_0, y_0) \in C$, these tangents are defined as the factors in the linear-factor decomposition of the smallest nonzero homogeneus component of the Taylor expansion of $f$ around $P$. To see this in more detail we refer the reader to [7, Ch. 3,§1]

And the only non-zero derivative of order 3 is $\frac{\partial^3 f}{\partial x^3} = -6$. Thus, the Taylor series expasion of $f(x, y)$ around $P$ is

$$\begin{aligned} f(x,y) =& f(x,y) - f\left(x_0, y_0\right) \\ =& \frac{1}{2!}\left(\frac{\partial^2 f}{\partial x^2}(P)\left(x-x_0\right)^2 + 2\frac{\partial^2 f}{\partial x \partial y}(P)\left(x-x_0\right)\left(y-y_0\right) + \frac{\partial^2 f}{\partial y^2}(P)\left(y-y_0\right)^2\right) \\ &+ \frac{1}{3!}\frac{\partial^3 f}{\partial x^3}\left(x-x_0\right)^3 \\ =& \left(-3x_0 - a_2\right)\left(x-x_0\right)^2 + a_1\left(x-x_0\right)\left(y-y_0\right) + \left(y-y_0\right)^2 - \left(x-x_0\right)^3 \\ =& \left(\left(y-y_0\right) - \alpha\left(x-x_0\right)\right)\left(\left(y-y_0\right) - \beta\left(x-x_0\right)\right) - \left(x-x_0\right)^3 \end{aligned}$$

where

$$\alpha = \frac{a_1 + \sqrt{a_1^2 + 4\left(3x_0 + a_2\right)}}{2}, \beta = \frac{a_1 - \sqrt{a_1^2 + 4\left(3x_0 + a_2\right)}}{2} \tag{A.1}$$

are the roots of $\left(-3x_0 - a_2\right) + a_1 Y + Y^2 \in K[Y]$, where we have fixed one of the square roots of $a_1^2 + 4\left(3x_0 + a_2\right)$. We notice that $\alpha$ and $\beta$ are conjugates over $K$.

**Definition A.1.3.** *With notation as above, the singular point $P$ is a* ***node*** *if $\alpha \neq \beta$. In this case, the lines*

$$y - y_0 = \alpha\left(x - x_0\right) \qquad \text{and} \qquad y - y_0 = \beta\left(x - x_0\right)$$

*are the tangent lines at $P$. Conversely, if $\alpha = \beta$, then we say that $P$ is a* ***cusp****, in which case the tangent line at $P$ is given by*

$$y - y_0 = \alpha\left(x - x_0\right).$$

Suppose we have a Weierstrass equation as in (A.1.1). If $\operatorname{char}(\overline{K}) \neq 2$ then we can complete the square, and the substitution

$$y \to \frac{1}{2}\left(y - a_1 x - a_3\right)$$

gives an equation of the form:

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1 a_3, \quad b_6 = a_3^2 + 4a_6. \tag{A.2}$$

Associated to our Weierstrass equation we also define the quantities:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24 b_4 \\ c_6 &= -b_2^3 + 36 b_2 b_4 - 216 b_6 \\ \Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6 \\ j &= c_4^3 / \Delta. \end{aligned} \tag{A.3}$$

That verify the following relations:

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2.$$

Furthermore, if $\operatorname{char}(\overline{K}) \neq 2, 3$ then the substitution:

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

removes the $x^2$ term from (A.2), yielding the equation:

$$E : y^2 = x^3 - 27c_4x - 54c_6. \tag{A.4}$$

The only changes of variables that preserve the Weierstrass form (A.1.2 (b)) also change the quantities (A.3) associated to them. How they change them is collected in the following table ([16, Ch. III, pag 45]). The quantities for the equation obtained after such a change are denoted with a prime.

$$\begin{array}{rl}
ua_1' &= a_1 + 2s \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^3a_3' &= a_3 + ra_1 + 2t \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\
\hline
u^2b_2' &= b_2 + 12r \\
u^4b_4' &= b_4 + rb_2 + 6r^2 \\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\
\hline
u^4c_4' &= c_4 \\
u^6c_6' &= c_6 \\
u^{12}\Delta' &= \Delta \\
j' &= j
\end{array} \tag{A.5}$$

**Definition A.1.4.** *The quantity $\Delta$ is the discriminant of the Weiertrass equation and $j$ is called the $j$-invariant of the elliptic curve.*

The reason for their names can be found in the following proposition:

**Proposition A.1.5.** *(a) The curve given by a Weierstrass equation satisfies:*

*(i) It is nonsingular if and only if $\Delta \neq 0$.*

*(ii) It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.*

*(iii) It has a cusp if and only if $\Delta = c_4 = 0$.*

*In cases (ii) and (iii), there is only one singular point.*

*(b) Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same $j$-invariant.*

*(c) Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose $j$-invariant is equal to $j_0$.*

*Proof.* [16, Ch. III, Proposition 1.4] □

Let us recall that if $\operatorname{char}(\overline{K}) \neq 2, 3$, every elliptic curve over $K$ has an equation of the form:

$$y^2 = x^3 + Ax + B, \qquad A, B \in K.$$

Which is called a *reduced Weierstrass form.* For this kind of equation, the discriminant and $j$-invariant are as follow:

$$\Delta = -16\left(4A^3 + 27B^2\right) \quad \text{and} \quad j = -1728\frac{(4A)^3}{\Delta}.$$

The only change of coordinates that preserve the reduced Weierstrass form are easily checked to be:

$$x = u^2 x' \quad \text{and} \quad y = u^3 y' \quad \text{for some } u \in \overline{K}^{\times}.$$

## A.2 The Group Law on an Elliptic Curve

Let $E$ be an elliptic curve given by a Weierstrass equation. Since $E$ is a cubic, by Bezout's Theorem, every line in $\mathbb{P}^2(\overline{K})$ intersects $E$ at exactly 3 points (counting multiplicities). So, given two points $P, Q \in E$, the line that passes through them (which is the tangent line at $P$ if $P = Q$), must intersect the curve in a third point, that we will call $P * Q$. Notice that the point $\mathcal{O}$ is of order 3 for $E$: The third point of intersection of the tangent line of $E$ at $\mathcal{O}$ is again $\mathcal{O}$. With this in mind, a group law can be defined in $E$, as follows.

**Definition A.2.1.** *Let $P, Q \in E$, let $L$ be the line through $P$ and $Q$ (if $P = Q$, let $L$ be the tangent line to $E$ at $P$), and let $R$ be the third point of intersection of $L$ with $E$. Let $L'$ be the line through $R$ and $\mathcal{O}$. Then $L'$ intersects $E$ at $R$, $\mathcal{O}$, and a third point. We denote that third point by $P + Q$*

Or more concisely:

$$P + Q = (P * Q) * \mathcal{O}. \tag{A.6}$$

One can easily verify that this composition law makes $E$ into an abelian group with $\mathcal{O}$ as the zero element, except for the associativity. To check associativity is better to use the explicit formulas for the group law that I am going to give later, although it is still a long and tedious case by case consideration. Furthermore, it worth noticing that if a line $L$ intersects $E$ at the (not necessarily distinct) points $P, Q, R$, then $P + Q + R = \mathcal{O}$. It follows that the negative of a point is $P * \mathcal{O}$, i.e. the third point of intersection of the line through $P$ and $\mathcal{O}$, because

$$\mathcal{O} = P + (P * \mathcal{O}) + \mathcal{O} = P + (P * \mathcal{O})$$

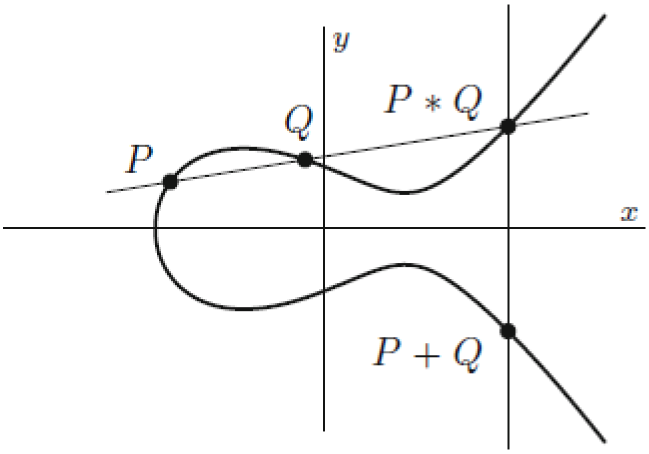

Figure A.1: Addition of distinct points

so $-P = P * \mathcal{O}$.

Over a field $K$ of characteristic different from 2 or 3, every elliptic curve has a Weierstrass equation of the form

$$y^2 = x^3 + Ax + B \tag{A.7}$$

and in this case the group law is shown in Figure. A.1 Adding or substracting a point $P$ to itself $m \in \mathbb{N}$ times will be denoted as $[m]P$ or $[-m]$ respectively. For example $[2]P = P + P$, $[-3]P = -P - P - P$.

By working with the equation of a line that passes through two points of $E$ and the equation for $E$ we get explicit formulas for the group law:

**Proposition A.2.2.** *Let $E$ be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*(a) Let $P = (x, y) \in E$. Then*

$$-P = (x, -y - a_1x - a_3).$$

*Next let*

$$P_1 + P_2 = P_3 \quad \text{with} \quad P_i = (x_i, y_i) \in E \quad \text{for } i = 1, 2, 3.$$

*(b) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then*

$$P_1 + P_2 = \mathcal{O}.$$

*Otherwise, the coordinates of $P_1 + P_2$ are*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

*where $\lambda$ and $\nu$ are:*

| | $\lambda$ | $\nu$ |
|---|---|---|
| $x_1 \neq x_2$ | $\dfrac{y_2 - y_1}{x_2 - x_1}$ | $\dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$ |
| $x_1 = x_2$ | $\dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$ | $\dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$ |

*With this notation, $y = \lambda x + \nu$ is the line through $P_1$ and $P_2$, or tangent to $E$ at $P_1$ if $P_1 = P_2$.*

*Proof.* [16, pages 53,54] □

We see that for a reduced Weierstrass form: $y^2 = x^3 + Ax + B$, the inverse of the point $(x, y)$ is $(x, -y)$.

**Definition A.2.3.** *(Multiplication-by-m map) The multiplication by $m$ map on an eliptic curve is just the map $[m] : E \to E, P \mapsto [m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}$.*

**Observation A.2.4.** We can compose the addition formula with itself $m$ times to get an explicit formula for multiplication-by-$m$ map. It is very impractical to do so, and gets messy very fast, but we do not need the actual formula. What is important is to notice that for an elliptic curve defined over $K$ and a point $P = (x, y) \in E$, the coordinates of $[m]P$ are in $K(x, y)$ since the ones of $P + P$ are $K(x, y)$ by the formulas we just gave. Which is to say that $[m]$ is, component-wise, a rational function on $x, y$ with coefficients in $K$.

**Therefore, $[m]$ commutes with the action[*] of $\mathrm{Gal}(\overline{K}/K)$ for every $m \in \mathbb{Z}$.**

Finally, we show how is the group structure of the nonsingular points of a singular curve given by a Weierstrass equation

**Definition A.2.5.** *Let $E$ be a (possibly singular) curve given by a Weierstrass equation over $K$. We define $E_{ns}(\overline{K})$ as the subset of nonsingular points of $E$.*

*Similarly, $E_{ns}(K) = E_{ns}(\overline{K}) \cap E(K)$ is the set of non singular points of $E(K)$*

Let us recall (Proposition A.1.5) that if $E$ is singular, it has a unique singular point.

**Proposition A.2.6.** *Let $E$ be a curve given by a Weierstrass equation over $K$ with $\Delta = 0$, so $E$ has a singular point $S$. Then the group law (Definition A.2.1) makes $E_{ns}(\overline{K})$ into an abelian group.*

*(a) Suppose that $c_4 \neq 0$, so $E$ has a node, and let*

$$y = \alpha_1 x + \beta_1 \quad \textit{and} \quad y = \alpha_2 x + \beta_2$$

[*] Recall that the action of $\mathrm{Gal}(\overline{K}/K)$ in the points of $E$ is coordinate-wise.

*be the distinct tangent lines to $E$ at $S$. Then the map*

$$E_{\mathrm{ns}}(\overline{K}) \longrightarrow \overline{K}^{\times}, \quad (x,y) \longmapsto \frac{y-\alpha_1 x-\beta_1}{y-\alpha_2 x-\beta_2}$$

*is an isomorphism of abelian groups.*

*(b) Suppose that $c_4 = 0$, so $E$ has a cusp, and let*

$$y = \alpha x + \beta$$

*be the tangent line to $E$ at $S$. Then the map*

$$E_{\mathrm{ns}} \longrightarrow \overline{K}^{+}, \quad (x,y) \longmapsto \frac{x-x(S)}{y-\alpha x-\beta}$$

*is an isomorphism of abelian groups.*

*Proof.* [16, Ch. III, Proposition 2.5]. □

In the previous proposition, $\overline{K}^{+}$ stands for the additive group $(K,+)$.

# Bibliography

[1] Arias-de-Reyna, Sara. *Course notes on local Fields*, University of Luxembourg, winter term of 2015.
`http://hdl.handle.net/10993/13303`

[2] Atiyah, Michael & Macdonald, Ian G. *Introduction To Commutative Algebra.* Westview Press (1994).

[3] Bilu, Yuri. *p-adic Numbers and Diophantine Equations.* Université de Bordeaux, Fall semester 2013. Avalaible at
`https://www.math.u-bordeaux.fr/~abesheno/bilu.pdf`

[4] Bourbaki, Nicolas. *Espaces Vectoriels Topologiques, Chapitres 1 à 5.* Éléments de Mathemátique. Réimpression inchangée de l'édition originale de 1981. Springer, (2007).

[5] Engler, Antonio & Prestel, Alexander. *Valued Fields.* Springer Monographs in Mathematics. Springer, (2005).

[6] Fröhlich, Albrecht . *Formal Groups.* First edition. Lectures notes on mathematics, No 74. Springer-Verlag Berlin, (1968).

[7] Fulton, William. *Algebraic curves. An Introduction to Algebraic Geometry.* (2008)

[8] Hungerford, Thomas W. *Algebra.* Springer. Third edition. (2003)

[9] Milne, J. S. *Algebraic Number Theory.* Avalaible at `www.jmilne.org/math/`. First published in 1996.

[10] Myrto Mavraki, Niki. *Notes about formal groups.*
`http://www.math.ubc.ca/~reichst/FormalGroups.pdf`

[11] Navas Orozco, Jesús. *Curvas elípticas y el Teorema de Mordell.* Final project to obtain the Mathematics Degree Title. Avalaible at:
`https://drive.google.com/file/d/15UZm2gUQYYcGXSY-mjTJdJkY3QIAI58C/view?usp=sharing`

[12] Neukirch, Jürgen. *Algebraic Number Theory*, (1992). Translated from the German by Norbert Schappacher. Springer.

[13] Rotman, Joseph J. *Advanced modern Algebra, part 2.* Third edition. Americal Mathematical Society (2017).

[14] Silverman, Joseph H. *Advances Topics on the Arithmetic of Elliptic Curves.* Springer-Verlag (1994).

[15] Silverman, Joseph H., John T. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer. 2nd Edition. (2015).

[16] Silverman, Joseph H. *The Arithmetic of Elliptic Curves.* Second edition (2009). Corrected second printing (2016).