Local Fields

Winter Term 2015

Université du Luxembourg

Sara Arias-de-Reyna
sara.ariasdereyna@uni.lu

Contents

Preface

These lecture notes correspond to the course *Local Fields* from the Master in Mathematics of the University of Luxembourg, taught in the Winter Term 2015. It consists of 14 lectures of 90 minutes each. This lecture belongs to the fourth semester of the Master, and it builds on the lectures *Commutative Algebra*, belonging to the first semester.

The aim of the lecture is to explain the basic theory of local fields, and apply this theory to obtain information about number fields. It is mainly based on Chapter II of [4]. Other fundamental sources we have used to prepare the lecture are [5], [3], [2].

Luxembourg, December 2015.
Sara Arias-de-Reyna,

1 p-adic numbers

The first example of local field that one naturally comes up with is the field of p-adic numbers. In this section we will introduce p-adic numbers as formal power series; later we will see how they arise as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value.

As a motivation to introduce p-adic numbers, consider the ring of integers, $\mathbb{Z}$, and the ring of polynomials in one variable with complex coefficients, $\mathbb{C}[z]$. Both are Euclidean domains, hence share many properties. Note, however, that the elements of $\mathbb{C}[z]$ can be considered as analytic functions, thus opening the way to complex analysis methods. In particular, one can study the behaviour of analytic functions locally at a point by considering their power series expansion. Let $\alpha \in \mathbb{C}$ be a point, and $f(z) \in \mathbb{C}[z]$. One can write the power series expansion of $f(z)$ around α as

$$f(z) = a_0 + a_1(z-\alpha) + a_2(z-\alpha)^2 + \cdots + a_n(z-\alpha)^n, \tag{1.1}$$

where n is the degree of $f(z)$ and $a_0, \ldots, a_n \in \mathbb{C}$. This power series development yields information about the behaviour of the function $f(z)$ at α; namely, $a_0 = 0$ if and only if f vanishes at α; more generally the order of vanishing of $f(z)$ at α is given as $\min\{i : a_i \neq 0\}$. Now, can we emulate this process if we replace $\mathbb{C}[z]$ by $\mathbb{Z}$?

Let us take a closer look at the way the element $f(z) \in \mathbb{C}[z]$ defines a function $f : \mathbb{C} \to \mathbb{C}$. Let $\alpha \in \mathbb{C}$. Then $f(\alpha)$ is evaluated by substituting z by α; in other words, we want to identify z and α. This can be interpreted as taking the class of $f(z)$ in the ring $\mathbb{C}[z]/(z-\alpha) \simeq \mathbb{C}[\alpha] = \mathbb{C}$.

Note now that the elements $z - \alpha$, for α running through the complex numbers, correspond precisely to the nonzero prime ideals of $\mathbb{C}[z]$. This insight allows us to jump from $\mathbb{C}[z]$ to $\mathbb{Z}$.

Namely, if we now consider an element $a \in \mathbb{Z}$, and fix a prime number $p > 0$, we can "evaluate" the element a at p by considering the class of a in $\mathbb{Z}/(p)$. We can say that the element $a \in \mathbb{Z}$ defines a function (which we still denote a)

$$a : \{p > 0 \text{ prime number}\} \to \bigcup_{\substack{p>0 \\ \text{prime number}}} \mathbb{Z}/(p).$$

This function maps a prime number $p > 0$ to the residue class of a modulo p. So far, this does not seem very useful...

But, let $p > 0$ be a prime number. What we certainly can do is to expand our $a \in \mathbb{Z}$ as a power series in p with coefficients in $\mathbb{Z}$ in analogy to (1.1), namely, to write

$$a = a_0 + a_1 p + \cdots + a_n p^n.$$

Of course there are many ways to write such an expansion! For instance, take $a = 12$, $p = 5$. Then $a = 2 + 2 \cdot 5 = 7 + 1 \cdot 5$.

Remark 1.1. *Let $p > 0$ be a prime number. Then any $a \in \mathbb{N}$ can be uniquely written as*

$$a = a_0 + a_1 p + \cdots + a_n p^n, \tag{1.2}$$

with $0 \leq a_i < p$ for all $i = 0, \ldots, n$. We call the equation (1.2) *the* p-adic expansion *of a.*

Indeed, we perform the following divisions

$$\begin{aligned} a &= pq_0 + a_0 \\ q_0 &= pq_1 + a_1 \\ &\cdots \\ q_{n-1} &= pq_n + a_n \\ q_n &= a_n, \end{aligned} \tag{1.3}$$

and then we write $a = a_0 + a_1 p + \cdots + a_n p^n$. The process terminates when $q_n < p$, so that when we divide it by p we get it back. This proves the existence of the expansion.

Assume now we have two different expansions

$$a = a_0 + a_1 p + \cdots + a_n p^n = b_0 + b_1 p + \cdots + b_m p^m$$

with $0 \leq a_i < p$ for all $i = 0, \ldots n$; $0 \leq b_j < p$ for all $j = 0, \ldots, m$. Let k be the first index such that $a_k \neq b_k$ (there must be one such index because the two expansions are different). Then, subtracting $a_0 + \cdots + a_{k-1} p^{k-1}$ from both sides, we get

$$p^k(a_k + \cdots + a_n p^{n-k}) = p^k(b_k + \cdots + b_m p^{m-k})$$

Dividing out p^k from both sides, we get that $a_k - b_k$ must be divisible by p. But $|a_k - b_k| < p$, hence $a_k = b_k$, contradicting the choice of k.

By the previous remark, we can expand any natural number as a finite sum of powers of p in an unique way. And this expansion yields information on a "locally at p"; namely $a_0 = 0$ if and only if $p|a$, and more generally the power of p dividing a is given by $\min\{i : a_i \neq 0\}$. But what about negative numbers? Obviously all numbers of the form $\sum_{i=0}^{n} a_i p^i$ with $0 \leq a_i < p$ are positive, so negative numbers cannot be represented in this way.

What happens if we try to apply Algorithm (1.3) to $-1 \in \mathbb{Z}$?

$$\begin{aligned} -1 &= p \cdot (-1) + (p-1) \\ -1 &= p \cdot (-1) + (p-1) \\ &\cdots \\ -1 &= p \cdot (-1) + (p-1) \\ &\cdots \end{aligned}$$

We get the same equation all the time, hence the process does not terminate! If we put these equations together, formally, we get $-1 = (p-1) + (p-1)p + (p-1)p^2 + \ldots$ While this expression has no meaning in $\mathbb{Z}$, it can be interpreted as a formal power series.

Definition 1.2. *Let $p > 0$ be a prime number. A p-*adic integer *will be a formal power series*

$$a_0 + a_1 p + a_2 p^2 + \cdots,$$

where $0 \leq a_i < p$ for all $i \in \mathbb{N}$. The set of all p-adic integers will be denoted by $\mathbb{Z}_p$.

Remark 1.3. *Note that, in the previous definition, we have defined a* set*. We still do not have an addition or a multiplication; the symbols "$+$" and "p^i" that appear in the formal power series expansions are just symbols, separating the different digits. In other words, if we write $A_p = \{0, 1, \dots, p-1\}$, we can identify the set of p-adic integers $\mathbb{Z}_p$ with the set $A_p \times A_p \times \cdots$ of infinite tuples of elements of A_p: an element $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ corresponds to the tuple $(a_0, a_1, \dots) \in A_p \times A_p \times \cdots$.*

As we have seen, we have a set-theoretic inclusion $\mathbb{N} \hookrightarrow \mathbb{Z}_p$, that to each natural number a associates the (finite) formal power series $\sum_{i=0}^{n} a_i p^i$ obtained in (1.3). Now we want to define an addition and a multiplication in $\mathbb{Z}_p$, extending the usual addition and multiplication in $\mathbb{N}$, in such a way that $\mathbb{Z}_p$ becomes a ring. Of course, we want our ring structure to emulate that of $\mathbb{Z}[[X]]$. But here the restriction that the coefficients be between 0 and $p-1$ gets in the way. Namely, if we have two power series $\sum_{i=0}^{\infty} a_i X^i, \sum_{i=0}^{\infty} b_i X^i$ and they happen to satisfy that $0 \leq a_i, b_i < p$ for all i, it does not follow that their sum in $\mathbb{Z}[[X]]$, say $\sum_{i=0}^{\infty} c_i X^i = \sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i$ satisfies that $0 \leq c_i < p$. We have to consider the usual process of "carrying-over" the digits.

Definition 1.4. *Consider the maps*

$$\begin{aligned} P_1 : \mathbb{Z}_p &\to \mathbb{Z}[[X]] \\ \sum_{i=0}^{\infty} a_i p^i &\mapsto \sum_{i=0}^{\infty} a_i X^i, \end{aligned}$$

and

$$\begin{aligned} P_2 : \mathbb{Z}[[X]] &\to \mathbb{Z}_p \\ \sum_{i=0}^{\infty} a_i X^i &\mapsto \sum_{i=0}^{\infty} b_i p^i, \end{aligned}$$

where the digits b_i are obtained recursively as follows:

- *$i = 0$: write $a_0 = q_0 p + b_0$, with $0 \leq b_0 < p$.*
- *$i = 1$: write $a_1 + q_0 = q_1 p + b_1$ with $0 \leq b_1 < p$.*
- *$i = 2$: write $a_2 + q_1 = q_2 p + b_2$ with $0 \leq b_2 < p$.*
- $\cdots$

Remark 1.5. 1. *What the map P_2 is doing is to "redistribute" the sum, so that all digits lie between 0 and $p-1$. In particular, with the notations above, it holds that*

$$\sum_{i=0}^{n} a_i p^i \equiv \sum_{i=0}^{n} b_i p^i \pmod{p^{n+1}} \text{ for all } n \in \mathbb{N}.$$

2. *Let $a = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[[X]]$. Note that the image $P_2(a)$ is uniquely characterised as the element $b = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$, where the sequence $(b_i)_i$ satisfies the following two properties:*
   - *For all i, $b_i \in \{0, \dots, p-1\}$.*
   - *For all $n \in \mathbb{N}$, $\sum_{i=0}^{n} a_i p^i \equiv \sum_{i=0}^{n} b_i p^i \pmod{p^{n+1}}$.*

3. Note that $P_2 \circ P_1$ is the identity in $\mathbb{Z}_p$, whereas $P_1 \circ P_2$ is not the identity on $\mathbb{Z}[[X]]$.

Now we can define the addition and multiplication in $\mathbb{Z}_p$ from those in $\mathbb{Z}[[X]]$, in the following way.

Definition 1.6. *We define the maps*

$$\begin{aligned} + : \mathbb{Z}_p \times \mathbb{Z}_p &\to \mathbb{Z}_p \\ (a, b) &\mapsto P_2(P_1(a) + P_1(b)). \\ \cdot : \mathbb{Z}_p \times \mathbb{Z}_p &\to \mathbb{Z}_p \\ (a, b) &\mapsto P_2(P_1(a) \cdot P_1(b)). \end{aligned}$$

Proposition 1.7. *With the applications defined above, $\mathbb{Z}_p$ is a ring.*

One can of course prove this proposition by hand, but it becomes tedious. Instead, what we will do is to identify $\mathbb{Z}_p$ with a certain inverse limit, and check that the addition and multiplication induced on $\mathbb{Z}_p$ via this identification coincide with those defined above. The proof of Proposition 1.7 will be given in Remark 1.16.

Remark 1.8. *Let $a = \sum_{i=0}^{\infty} a_i p^i$. For each $n \in \mathbb{N}$, let us take the partial sum $\sum_{i=0}^{n} a_i p^i \in \mathbb{Z}$. We can consider this partial sum as the "value of a up to multiples of p^{n+1}". Note that the element a is uniquely determined by the infinite sequence of all partial sums $(\sum_{i=0}^{n} a_i p^i)_{n=0}^{\infty}$.*

Since each partial sum $\sum_{i=0}^{n} a_i p^i$ provides information modulo p^{n+1}, instead of considering it as an element of $\mathbb{Z}$ we might as well consider its projection modulo the ideal (p^{n+1}), thus obtaining an element of $\mathbb{Z}/p^{n+1}\mathbb{Z}$. In this way we can attach for each $a \in \mathbb{Z}_p$ an infinite sequence

$$(A_n \pmod{p^{n+1}})_n \in \prod_{n=0}^{\infty} \mathbb{Z}/p^{n+1}\mathbb{Z}.$$

However, this map from $\mathbb{Z}_p$ to $\prod_{n=0}^{\infty} \mathbb{Z}/p^{n+1}\mathbb{Z}$ is not surjective. Take for instance $p = 5$, and the sequence

$$(3 \pmod 5, 7 \pmod{5^2}, 7 \pmod{5^3}, \dots) \in \prod_{n=0}^{\infty} \mathbb{Z}/5^{n+1}\mathbb{Z}.$$

If there is an $a = \sum_{i=0}^{\infty} a_i 5^i \in \mathbb{Z}_5$ corresponding to that sequence, we would have that

$$\begin{aligned} 3 &\equiv a_0 \pmod 5 \\ 7 &\equiv a_0 + 5a_1 \pmod{5^2} \end{aligned}$$

But then $a_0 = 3$, and therefore $3 + 5a_1 \equiv 7 \pmod{25}$, which is not possible since $3 \not\equiv 7 \pmod 5$.

To sum up, there must be some compatibility: If the sequence $(A_n \pmod{p^{n+1}})_n$ comes from an element of $\mathbb{Z}_p$, we must have that, for all $n \in \mathbb{N}$,

$$A_{n+1} \equiv A_n \pmod{p^{n+1}}. \tag{1.4}$$

This leads us to the notion of inverse limit.

Remark 1.9.
- *Let $(R_n)_{n=0}^{\infty}$ be a family of rings. Recall that the product $\prod_{n=0}^{\infty} R_n$ is a ring with the sum and the multiplication defined component-wise, that is to say,*

$$(A_n)_n + (B_n)_n = (A_n + B_n)_n$$
$$(A_n)_n \cdot (B_n)_n = (A_n \cdot B_n)_n$$

Moreover, the neutral element for the addition is $(0_{R_0}, 0_{R_1}, \dots)$ (where 0_{R_i} denotes the neutral element for the addition in R_i) and the neutral element for the multiplication is $(1_{R_0}, 1_{R_1}, \dots)$ (where 1_{R_i} denotes the neutral element for the multiplication in R_i).

- *Let $f : R \to R'$ be a map. We say that f is a* morphism of rings *if $f(1_R) = 1_{R'}$ and, for all $a, b \in R$, $f(a+b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$.*

Definition 1.10. *Let $(R_n)_{n=0}^{\infty}$ be a family of rings, and assume we have a family of surjective ring homomorphisms $(f_n : R_n \to R_{n-1})_{n=1}^{\infty}$. We define the* inverse limit *of $(R_n)_{n=0}^{\infty}$ with respect to the morphisms $(f_n)_{n=1}^{\infty}$, denoted $\varprojlim_n R_n$, as*

$$\varprojlim_n R_n := \{(A_n)_n \in \prod_{n=0}^{\infty} R_n : f_n(A_n) = A_{n-1} \text{ for all } n = 1, \dots\}.$$

The elements of $\varprojlim_n R_n$ are called coherent sequences.

Lemma 1.11. *The set $\varprojlim_n R_n$, endowed with the addition and multiplication inherited from the product ring $\prod_{n=0}^{\infty} R_n$, is a subring.*

Proof. One just has to check that the inverse limit is closed under addition and multiplication, and the neutral element for the multiplication $(1, 1, \dots)$ belong to the inverse limit, and that the set is closed by taking additive inverses. □

Example 1.12. *Let $p > 0$ be a prime number. For each $n \in \mathbb{N}$, let $R_n = \mathbb{Z}/p^{n+1}\mathbb{Z}$. Now we define some morphisms connecting these rings: for each $n \geq 1$, let*

$$f_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$
$$x \pmod{p^{n+1}} \mapsto x \pmod{p^n}$$

Note that the maps f_n are well defined and surjective. We can thus consider the inverse limit of the family $(R_n)_{n=0}^{\infty}$ with respect to the morphisms $\{f_n : R_n \to R_{n-1}\}$; we will denote it by

$$\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}.$$

Next, we will identify the p-adic integers with the projective limit $\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$. We start with the following lemma:

Lemma 1.13. *Let $(A_n \pmod{p^{n+1}})_n \in \varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$. Then there exists a unique sequence $(a_i)_i$ such that the following two properties hold:*

- *For all i, $a_i \in \{0, \dots, p-1\}$.*

- *For all* n, $A_n \equiv \sum_{i=1}^{n} a_i p^i \pmod{p^{n+1}}$.

Proof. We start showing the uniqueness of the sequence $(a_i)_i$. Assume that there exists another sequence $(b_i)_i$ satisfying the two properties of the statement. Then by the characterisation of the map P_2 given in Remark 1.5, it holds that $\sum_{i=0}^{\infty} a_i p^i = P_2(\sum_{i=0}^{\infty} a_i X^i) = \sum_{i=0}^{\infty} b_i p^i$, so the two sequences $(a_i)_i$ and $(b_i)_i$ coincide.

Now we prove the existence of the sequence $(a_i)_i$, by giving a recursive definition:

- $n = 0$: Let a_0 be the only integer in $\{0, \dots, p-1\}$ satisfying that $a_0 \equiv A_0 \pmod{p}$.
- $n = 1$: Since $A_1 \equiv A_0 \pmod{p}$, we have that $p | A_1 - a_0$. Set

$$b_1 = \frac{A_1 - a_0}{p} \in \mathbb{Z}.$$

  Let a_1 be the only integer in $\{0, \dots, p-1\}$ satisfying that $a_1 \equiv b_1 \pmod{p}$. Note that $a_0 + pa_1 \equiv A_1 \pmod{p^2}$.

- $n = 2$: Since $A_2 \equiv A_1 \pmod{p^2}$, we have that $p^2 | A_2 - (a_0 + pa_1)$. Set

$$b_2 = \frac{A_2 - (a_0 + a_1 p)}{p^2} \in \mathbb{Z}.$$

  Let a_2 be the only integer in $\{0, \dots, p-1\}$ satisfying that $a_2 \equiv b_2 \pmod{p}$. Note that $a_0 + a_1 p + a_2 p^2 \equiv A_2 \pmod{p^3}$.

- $\dots$.
- $n - 1 \to n$: By construction, we have that $a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \equiv A_{n-1} \pmod{p^n}$. Since $A_n \equiv A_{n-1} \pmod{p^n}$, we have that $p^n | A_n - (a_0 + pa_1 + \cdots + a_{n-1} p^{n-1})$. Set

$$b_n = \frac{A_n - (a_0 + pa_1 + \cdots + a_{n-1} p^{n-1})}{p^n} \in \mathbb{Z}.$$

  Let a_n be the only integer in $\{0, \dots, p-1\}$ satisfying that $a_n \equiv b_n \pmod{p}$. Note that $a_0 + a_1 p + \cdots + a_n p^n \equiv A_n \pmod{p^{n+1}}$.

□

Proposition 1.14. *The map*

$$\Phi : \mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$$
$$\sum_{i=0}^{\infty} a_i p^i \mapsto (\sum_{i=0}^{n} a_i p^i \pmod{p^{n+1}})_n$$

is bijective.

Proof. First of all, note that the image of Φ lies in $\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$ because the sequences $(\sum_{i=0}^{n} a_i p^i \pmod{p^{n+1}})_n$ are coherent (cf. Equation (1.4)).

Consider the map

$$\Psi : \varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}_p$$

$$(A_n \pmod{p^{n+1}}) \mapsto \sum_{i=0}^{\infty} a_i p^i,$$

where the sequence $(a_i)_i$ is given by Lemma 1.13. Let us check that Ψ and Φ are inverses of each other:

- $\Psi \circ \Phi = \mathrm{id}_{\mathbb{Z}_p}$: Take any $a = \sum_{i=0}^{\infty} a_i p^i$. We have that $\Phi(a) = (A_n \pmod{p^{n+1}})_n$, where $A_n = \sum_{i=0}^{n} a_i p^i$. The sequence $(a_i)_i$ satisfies (trivially) the two conditions in Lemma 1.13, so we get that $\Psi(A_n \pmod{p^{n+1}}) = \sum_{i=0}^{\infty} a_i p^i = a$.
- $\Phi \circ \Psi = \mathrm{id}_{\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}}$: Take any element $(A_n \pmod{p^{n+1}})_n \in \varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$, and let $a = \sum_{i=0}^{\infty} a_i p^i = \Psi((A_n \pmod{p^{n+1}})_n)$. Note that, by the definition of Ψ, for each $n \in \mathbb{N}$, we have that $A_n \equiv a_0 + a_1 p + \cdots + a_n p^n \pmod{p^{n+1}}$. Therefore, when we take $\Phi(a)$, we obtain the sequence $(\sum_{i=0}^{n} a_i p^i \pmod{p^{n+1}})_n = (A_n \pmod{p^{n+1}})_n$.

□

Lemma 1.15. *The addition and multiplication induced by the identification $\Phi : \mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$ coincide with those in Definition 1.6.*

Proof. We will only consider the addition map, since the multiplication map is analogous. To prove that the addition induced on $\mathbb{Z}_p$ by that of $\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$ coincides with the one of Definition 1.6, we have to prove that the following diagram commutes

$$\begin{array}{ccc} \mathbb{Z}_p \times \mathbb{Z}_p & \xrightarrow{\quad + \quad} & \mathbb{Z}_p \\ \downarrow{\scriptstyle \Phi\times\Phi} & & \downarrow{\scriptstyle \Phi} \\ \left(\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}\right) \times \left(\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}\right) & \xrightarrow{+} & \left(\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}\right) \end{array}$$

Let us consider two elements $a = \sum_{i=0}^{\infty} a_i p^i, b = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$. Then if we apply $\Phi \times \Phi$, followed by $+$, we obtain

$$\Phi(a) + \Phi(b) = (\sum_{i=0}^{n} a_i p^i \pmod{p^{n+1}})_n + \sum_{i=0}^{n} b_i p^i \pmod{p^{n+1}})_n$$

$$= (\sum_{i=0}^{n} (a_i + b_i) p^i \pmod{p^{n+1}})_n$$

On the other hand, if we first apply $+$ and then Φ, we obtain

$$\Phi(a+b) = \Phi(P_2(P_1(\sum_{i=0}^{\infty} a_i p^i) + P_1(\sum_{i=0}^{\infty} b_i p^i))) \\ = \Phi(P_2(\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i)) = \Phi \circ P_2(\sum_{i=0}^{\infty}(a_i+b_i)X^i).$$

Recall that P_2 consists in substituting X by p, and then rearranging the sum so that the coefficients belong to $\{1, \dots, p-1\}$. Denote

$$\sum_{i=0}^{\infty} c_i p^i = P_2(\sum_{i=0}^{\infty}(a_i+b_i)X^i).$$

Then by Remark 1.5 we have that $\sum_{i=0}^{n} c_i p^i \equiv \sum_{i=0}^{n}(a_i+b_i)p^i \pmod{p^{n+1}}$. Hence

$$\Phi(a+b) = \Phi(\sum_{i=0}^{\infty} c_i p^i) = (\sum_{i=0}^{n} c_i p^i \pmod{p^{n+1}})_n \\ = (\sum_{i=0}^{n}(a_i+b_i)p^i \pmod{p^{n+1}})_n = \Phi(a) + \Phi(b).$$

This proves the assertion. □

Remark 1.16. *1. Since $\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$ is a ring, we obtain a proof of Proposition 1.7 as a corollary of Lemma 1.15 (See Exercise sheet 2).*

2. *From now on, we will identify $\mathbb{Z}_p$ and $\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$, and consider the elements of $\mathbb{Z}_p$ either as infinite formal power series in p^n, or as coherent sequences in $\prod_{i=1}^{\infty} \mathbb{Z}/p^{n+1}\mathbb{Z}$, at our convenience.*

3. *There is a natural injective map*

$$\mathbb{Z} \to \varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z} \\ a \mapsto (a \pmod{p^{n+1}})_n.$$

When restricted to the natural numbers, this inclusion coincides, via the identification of $\mathbb{Z}_p$ with $\varprojlim_n \mathbb{Z}/p^{n+1}\mathbb{Z}$, with the inclusion $\mathbb{N} \hookrightarrow \mathbb{Z}_p$ that to each natural number attaches its p-adic expansion (see Remark 1.1).

4. *Under the natural embedding $\mathbb{N} \hookrightarrow \mathbb{Z}_p$, we have that the element $p \in \mathbb{N}$ corresponds to the element $\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$, (which we will also denote by p) where $a_0 = 0$, $a_1 = 1$, $a_i = 0$ for all $i \geq 2$. Note that, for all $b = \sum_{i=0}^{\infty} b_i p^i$, multiplication by p yields*

$$b \cdot p = \sum_{i=0}^{\infty} b_i p^{i+1};$$

that is to say, the digits of b "shift" one place to the right.

Now we want to introduce the *field* of p-adic numbers. In order to do this, we first need to prove the following lemma.

Lemma 1.17. *Let $a = \sum_{i=0}^{\infty} \in \mathbb{Z}_p$ be such that $a_0 \neq 0$. Then $a \in \mathbb{Z}_p^\times$.*

Proof. We will construct an element $b = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ such that $a \cdot b = 1$. In other words, we need to construct b satisfying that, for all $n \in \mathbb{N}$,

$$\left(\sum_{i=0}^{n} a_i p^i\right) \cdot \left(\sum_{i=0}^{n} b_i p^i\right) \equiv 1 \pmod{p^{n+1}}. \tag{1.5}$$

We will construct b recursively:

- $n = 0$: Since $a_0 \neq 0$ and $a_0 \in \{0, \dots, p-1\}$, in particular $p \nmid a_0$, and therefore there exist $r, s \in \mathbb{Z}$ such that $ra_0 + sp = 1$. Let b_0 be the unique element of $\{0, \dots, p-1\}$ such that $r \equiv b_0 \pmod{p}$. Note that, with this choice of b_0, Equation (1.5) is satisfied for $n = 0$.
- $n = 1$: We are looking for $b_1 \in \{0, \dots, p-1\}$ such that

  $$(a_0 + a_1 p) \cdot (b_0 + b_1 p) \equiv 1 \pmod{p^2}.$$

  That is to say,

  $$a_0 b_0 + p(a_0 b_1 + a_1 b_0) \equiv 1 \pmod{p^2}.$$

  Since $a_0 b_0 \equiv 1 \pmod{p}$, we can write $a_0 b_0 = 1 + p d_1$; replacing this in the previous equation, we get

  $$p(d_1 + a_0 b_1 + a_1 b_0) \equiv 0 \pmod{p^2},$$

  or equivalently

  $$d_1 + a_0 b_1 + a_1 b_0 \equiv 0 \pmod{p}.$$

  Now we can solve for b_1 (using again that $a_0 b_0 \equiv 1 \pmod{p}$), and we get

  $$b_1 \equiv -b_0(d_1 + a_1 b_0) \pmod{p}.$$

  Thus it suffices to set b_1 as the unique element in $\{0, \dots, p-1\}$ which is congruent to $-b_0(d_1 + a_1 b_0) \pmod{p}$.
- $\dots$
- $n - 1 \to n$: We are looking for $b_n \in \{0, \dots, p-1\}$ such that Equation (1.5) holds. By construction, we know that

  $$\left(\sum_{i=0}^{n-1} a_i p^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i p^i\right) \equiv 1 \pmod{p^n}.$$

  Thus we can write

  $$\left(\sum_{i=0}^{n-1} a_i p^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i p^i\right) = 1 + d_n p^n \text{ for some } d_n \in \mathbb{Z},$$

and we obtain

$$\left(\sum_{i=0}^{n} a_i p^i\right) \cdot \left(\sum_{i=0}^{n} b_i p^i\right) - 1 \equiv \left(\left(\sum_{i=0}^{n-1} a_i p^i\right) + a_n p^n\right) \cdot \left(\left(\sum_{i=0}^{n-1} b_i p^i\right) + b_n p^n\right) - 1$$
$$= (1 + d_n p^n) + p^n(a_0 b_n + a_n b_0) - 1 \pmod{p^{n+1}};$$

and Equation (1.5) is equivalent to

$$d_n + (a_0 b_n + a_n b_0) \equiv 0 \pmod{p}.$$

Solving for b_n, we obtain

$$b_n \equiv -b_0(d_n + a_n b_0) \pmod{p}.$$

Therefore it suffices to take b_n as the unique element in $\{0, \dots, p-1\}$ congruent to $-b_0(d_n + a_n b_0) \pmod{p}$.

□

Remark 1.18. *Reciprocally, if $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ satisfies that $a_0 = 0$, then a is* not *invertible in $\mathbb{Z}_p$. Indeed, assume that there exists $b = \sum_{i=0}^{\infty} b_i p^i$ with $a \cdot b = 1$. Then, in particular, $a_0 \cdot b_0 \equiv 1 \pmod{p}$, and this cannot happen.*

Corollary 1.19. *1. $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$.*

2. *Every nonzero element $a \in \mathbb{Z}_p$ can be written as $a = p^m \cdot u$ for some integer $m \geq 0$ and some invertible element $u \in \mathbb{Z}_p$.*

3. *$\mathbb{Z}_p$ is an integral domain.*

Proof. 1. It suffices to note that $p\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i : a_0 = 0\}$. Therefore, by Remark 1.18, the ideal $p\mathbb{Z}_p$ consist precisely of the non-invertible elements of $\mathbb{Z}_p$. The assertion now follows.

2. Let $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$, and let $m \in \mathbb{Z}$ be the first index such that $a_m \neq 0$ (this index must exist because a is nonzero). For all $i \geq 0$, let us define $u_i = a_{i+m}$, and let $u = \sum_{i=0}^{\infty} u_i p^i$. By Lemma 1.17, $u \in \mathbb{Z}_p^{\times}$, and

$$p^m \cdot u = p^m \left(\sum_{i=0}^{\infty} u_i p^i\right) = \sum_{i=0}^{\infty} u_i p^{i+m} = \sum_{i=0}^{\infty} a_{i+m} p^{i+m} = a.$$

3. To prove that $\mathbb{Z}_p$ is an integral domain, let us take two nonzero elements $a = \sum_{i=0}^{\infty} a_i p^i$ and $b = \sum_{i=0}^{\infty} b_i p^i$ in $\mathbb{Z}_p$; we want to show that $a \cdot b \neq 0$. We can write $a = p^m u$, $b = p^k v$ with $m, k \geq 0$ integers and $u, v \in \mathbb{Z}_p^{\times}$. Then

$$a \cdot b = p^{m+k}(u \cdot v).$$

Since $u \cdot v$ is invertible, we obtain that $a \cdot b = 0$ if and only if $p^{m+k} = 0$, which is not the case.

□

Definition 1.20. *We denote by $\mathbb{Q}_p$ the field of fractions of $\mathbb{Z}_p$. The elements of $\mathbb{Q}_p$ are called* p-adic numbers.

Lemma 1.21. *Every nonzero element in $\mathbb{Q}_p$ can be written in an unique way as $p^m u$ for some $m \in \mathbb{Z}$ and some $u \in \mathbb{Z}_p^\times$.*

Proof. Let $a, b \in \mathbb{Z}_p$ be nonzero elements; we know they can be written as $a = p^{k_1} v_1$, $b = p^{k_2} v_2$ for some integers k_1, k_2 and some $v_1, v_2 \in (\mathbb{Z}_p)^\times$. Therefore

$$ab^{-1} = p^{k_1} v_1 (p^{k_2})^{-1} v_2^{-1} = p^{k_1 - k_2} v_1 v_2^{-1}.$$

Since $v_2 \in \mathbb{Z}_p^\times$, $v_2^{-1} \in \mathbb{Z}_p^\times$. This proves the existence of the representation. Uniqueness is clear. □

Remark 1.22. *By the previous lemma, one can identify $\mathbb{Q}_p$ with the formal finite-tailed Laurent series*

$$\sum_{i=m}^{\infty} a_i p^i,$$

where $m \in \mathbb{Z}$ (maybe negative) and $0 \leq a_i < p$ for all $i \in \{m, m+1, \dots\}$.

Namely, we write the p-adic number $p^m u$, with $u = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^\times$, as $\sum_{i=m}^{\infty} a_{i-m} p^i$.

2 Absolute values and valuations

Let $(a_i)_i$ be a sequence of real numbers, and consider the series $\sum_{i=1}^{\infty} a_i$. In analysis, one is often interested in the case when this series converges, that is, when the sequence of partial sums $\sum_{i=1}^{n} a_i$ tends to a limit in the standard Euclidean metric of $\mathbb{R}$. In the previous section we dealt with infinite series $\sum_{i=0}^{\infty} a_i p^i$. These series do not converge in $\mathbb{R}$ unless all coefficients vanish from one point on. Therefore we defined the p-adic integers $\mathbb{Z}_p$ as the set of formal power series $\sum_{i=0}^{\infty} a_i p^i$, and introduced a ring structure on it. In this section we will see that one can actually define a metric on $\mathbb{Q}$ such that, the more powers of p appear in the factorisation of an integer $a \in \mathbb{Z}$, the *smaller* this integer a is. With respect to this metric, the sequence of partial sums $(\sum_{i=0}^{n-1} a_i p^i)_n$ will actually be a Cauchy sequence, and we will recover the p-adic numbers $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to this metric, in analogy with the construction of $\mathbb{R}$ as the completion of $\mathbb{Q}$ with respect to the Euclidean metric.

Definition 2.1. *Let X be a set. A* distance *on X is a map*

$$\begin{aligned} \mathrm{d} : X \times X &\to \mathbb{R}_{\geq 0} \\ (x, y) &\mapsto \mathrm{d}(x, y) \end{aligned}$$

satisfying that, for all $x, y, z \in X$,

- $\mathrm{d}(x, y) = 0$ *if and only if* $x = y$,
- $\mathrm{d}(x, y) = d(y, x)$,
- $d(x, z) \leq d(x, y) + d(y, z)$ *(Triangle inequality).*

The pair (X, d) *is called a* metric space.

Example 2.2. *The pair* $(\mathbb{Q}, \mathrm{d})$ *is a metric space, where* $\mathrm{d} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}_{\geq 0}$ *is defined as* $\mathrm{d}(x, y) = |x - y|$*. Here* $|\cdot|$ *denotes the standard absolute value in* $\mathbb{Q}$*.*

The example above constitutes one instance of metric space that is defined through an absolute value.

Definition 2.3. *Let* K *be a field. An* absolute value *is a map*

$$\begin{aligned} |\cdot| : K &\to \mathbb{R}_{\geq 0} \\ x &\mapsto |x| \end{aligned}$$

satisfying that, for all $x, y \in K$*,*

(1) $|x| = 0$ *if and only if* $x = 0$*,*

(2) $|x \cdot y| = |x| \cdot |y|$*,*

(3) $|x + y| \leq |x| + |y|$ *(Triangle inequality).*

Remark 2.4. *Since we will consider several absolute values, we will denote the standard absolute value on* $\mathbb{Q}$ *as* $|\cdot|_\infty$ *to avoid confusion (some motivation for this notation can be found in Exercise sheet 3).*

Remark 2.5. *Let* K *be a field, and* $|\cdot|$ *an absolute value. Define*

$$\begin{aligned} \mathrm{d} : K \times K &\to \mathbb{R}_{\geq 0} \\ (x, y) &\mapsto |x - y|. \end{aligned}$$

Then (K, d) *is a metric space.*

Example 2.6. *Let* K *be any field, and define for each* $x \in K$

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

This is the trivial absolute value*, which trivially satisfies all three properties from Definition 2.3.*

Let $p > 0$ be a prime number. In order to define the p-adic absolute value, we first introduce an auxiliary function, that measures "how divisible by p" is a rational number.

Definition 2.7. *We define a map* $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ *as follows: Let* $x \in \mathbb{Q}$ *be a nonzero rational number, and write it as* $x = p^m \frac{a}{b}$*, with* a, b *integers such that* $p \nmid a$*,* $p \nmid b$*. Then we define* $v_p(x) = m$*. Furthermore we define* $v_p(0) = \infty$*. Here we are using the convention that* ∞ *is a symbol satisfying* $\infty > a$ *for all* $a \in \mathbb{Z}$*,* $\infty + a = \infty$ *for all* $a \in \mathbb{Z}$ *and* $a^{-\infty} = 0$ *for all integers* $a > 1$*. The map* v_p *is called the* p-adic valuation*.*

Remark 2.8.

- *Note that the* p*-adic valuation of a nonzero* $x \in \mathbb{Q}$ *does not depend on the representation of* x *in the form* $p^m \frac{a}{b}$*, as long as* p *does not divide* ab*.*

- *By definition of the p-adic valuation, we have that for any nonzero $x \in \mathbb{Q}$, $x = p^{v_p(x)}\frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $p \nmid a$, $p \nmid b$.*

Definition 2.9. *Let $p > 0$ be a prime number. We define the* p-adic absolute value *as*

$$\begin{aligned} |\cdot| : \mathbb{Q} &\to \mathbb{Q}_{\geq 0} \\ x &\mapsto p^{-v_p(x)}. \end{aligned}$$

Lemma 2.10. *The p-adic absolute value is an absolute value, that is to say, satisfies the three properties of Definition 2.3*

Proof.

- (1) For each nonzero $x \in \mathbb{Q}$, $|x|_p = p^{-v_p(x)} \neq 0$. On the other hand, $|0| = p^{-\infty} = 0$.
- (2), (3) Let $x, y \in \mathbb{Q}$. If one of them is zero, then the equalities (2) and (3) are trivially satisfied, so we may assume they are both nonzero. Write $x = p^{v_p(x)}\frac{a}{b}$ and $y = p^{v_p(y)}\frac{c}{d}$ with $p \nmid a$, b, c, d.

  $$x \cdot y = p^{v_p(x)+v_p(y)}\frac{ac}{bd}.$$

  Since $p \nmid ac$, $p \nmid bd$, we obtain that $v_p(x \cdot y) = v_p(x) + v_p(y)$, hence

  $$|x \cdot y|_p = p^{-v_p(x\cdot y)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p \cdot |y|_p.$$

  To prove the triangle inequality, we distinguish two cases.

  - $v_p(x) = v_p(y)$. Then

    $$x + y = p^{v_p(x)}\frac{a}{b} + p^{v_p(y)}\frac{c}{d} = p^{v_p(x)}\left(\frac{ad+cb}{bd}\right).$$

    Let us write $ad + bc = p^k s$ with $p \nmid s$. Then

    $$x + y = p^{v_p(x)+k}\left(\frac{s}{bd}\right),$$

    and thus

    $$v_p(x + y) = v_p(x) + k \geq v_p(x).$$

    Therefore

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

  - $v_p(x) \neq v_p(y)$. Let us assume that $v_p(x) > v_p(y)$. Then

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

    But, since $p \nmid bc$, we conclude that $p \nmid p^{v_p(x)-v_p(y)}ad + bc$, and as a consequence $v_p(x + y) = v_p(y)$. Therefore

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

□

Remark 2.11. *1. In the proof of Lemma 2.10, we have seen that the p-adic valuation v_p satisfies three properties: for all $x, y \in \mathbb{Q}$,*

(1) $v_p(x) = \infty$ if and only if $x = 0$,

(2) $v_p(x \cdot y) = v_p(x) + v_p(y)$,

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

It will turn out to be useful to generalise the notion of p-adic valuation to arbitrary fields (cf. Definition 2.12)

2. The third property of v_p above actually implies something stronger than the triangle inequality, namely, for all $x, y \in \mathbb{Q}$,

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} \text{ (Strong triangle inequality).}$$

Now we have many examples of absolute values on $\mathbb{Q}$ (namely, one for each different prime number $p > 0$, plus the standard absolute value $|\cdot|_\infty$).

Definition 2.12. *Let K be a field. A valuation is a map*

$$v : K \to \mathbb{R} \cup \{\infty\}$$

satisfying that, for all $x, y \in K$,

(1) $v(x) = \infty$ if and only if $x = 0$,

(2) $v(x \cdot y) = v(x) + v(y)$,

(3) $v(x + y) \geq \min\{v(x), v(y)\}$,

with the convention that ∞ is a symbol satisfying $\infty + r = \infty$ and $r < \infty$ for all $r \in \mathbb{R}$, and $r^{-\infty} = 0$ for all $r \in \mathbb{R}_{>1}$.

Proposition 2.13. *Let K be a field, $r \in \mathbb{R}_{>1}$ and $v : K \to \mathbb{R} \cup \{\infty\}$ a valuation. Then the map*

$$\begin{aligned} |\cdot| : K &\to \mathbb{R}_{\geq 0} \\ x &\mapsto r^{-v(x)} \end{aligned}$$

is an absolute value, which satisfies the strong triangle inequality

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

Proof. See Exercise Sheet 3. □

Remark 2.14. *Since $|\cdot|_p$ is an absolute value, by Remark 2.5 it defines a distance on $\mathbb{Q}$, namely the p-adic distance, given as*

$$\mathrm{d}_p(x, y) = |x - y|_p \text{ for all } x, y \in \mathbb{Q}.$$

The p-adic distance has some properties that clash with our intuition. For example, the following lemma shows that every triangle is isosceles!

Lemma 2.15. *Let $q_1, q_2, q_3 \in \mathbb{Q}$. Then two of the three numbers $\mathrm{d}_p(q_1, q_2)$, $\mathrm{d}_p(q_1, q_3)$, $\mathrm{d}_p(q_2, q_3)$ coincide.*

Proof. Since $\mathrm{d}_p(x, y) = \mathrm{d}_p(x-q_3, y-q_3)$ for all $x, y \in \mathbb{Q}$, we can assume, without loss of generality, that $q_3 = 0$. Call $q_1 = p^{v_1}a_1/b_1$, $q_2 = p^{v_2}a_2/b_2$ ($p \nmid a_1$, b_1, a_2, b_2). We claim that two of the three numbers $\mathrm{d}_p(0, q_1)$, $\mathrm{d}_p(0, q_2)$, $\mathrm{d}_p(q_1, q_2)$ are equal. Indeed, assume the three of them are different. Since $\mathrm{d}_p(0, q_1) = |q_1|_p = p^{-v_1}$ and $\mathrm{d}_p(0, q_2) = |q_2|_p = p^{-v_2}$, we obtain that $v_1 \neq v_2$. Assume $v_1 > v_2$. Then

$$\mathrm{d}_p(q_1, q_2) = |q_1 - q_2|_p = |p^{v_2}\frac{p^{v_1-v_2}a_1b_2 - a_2b_1}{b_1b_2}|_p = p^{-v_2} = \mathrm{d}_p(0, q_2),$$

which is a contradiction. □

These remarkable properties of the p-adic distance that separate it from the standard one stem from the fact that the p-adic absolute value satisfies the strong triangle inequality. This leads to the following definition.

Definition 2.16. *Let K be a field and let $|\cdot|$ be an absolute value on K. We will say that $|\cdot|$ is* nonarchimedean *(or* ultrametric*) if it satisfies the following: for all $x, y \in K$,*

$$|x + y| \leq \max\{|x|, |y|\} \text{ (Strong triangle inequality).}$$

Otherwise $|\cdot|$ is called an archimedean absolute value.

Nonarchimedean absolute values can be characterised in the following way.

Lemma 2.17. *Let K be a field and $|\cdot|$ an absolute value on K. Then the following are equivalent:*

(i) $|\cdot|$ *is nonarchimedean.*

(ii) For all $n \in \mathbb{N}$, $|n \cdot 1_K| \leq 1$.

(iii) $\{|n \cdot 1_K| : n \in \mathbb{N}\} \subset \mathbb{R}$ is bounded (with respect to the standard absolute value $|\cdot|_\infty$).

Proof.

- (i) ⇒ (ii) If $|\cdot|$ satisfies the strong triangle inequality, we have that
$$|n \cdot 1_K| = |1_K + \overset{n}{\cdots} + 1_K| \leq \{\max|1_K|\} = |1_K| = 1.$$
- (ii) ⇒ (iii) By (ii), 1 is an upper bound on the set $\{|n \cdot 1_K| : n \in \mathbb{N}\} \subset \mathbb{R}$. A trivial lower bound is 0.
- (iii) ⇒ (i) Let $x, y \in K$; we will prove the strong triangle inequality for x, y. Let $B \in \mathbb{N}$ be such that, for all $n \in \mathbb{N}$, $|n \cdot 1_K| \leq B$. Let us assume that $|x| \geq |y|$. Then for all $n \in \mathbb{N}$
$$|x + y|^n \leq \sum_{i=0}^{n} \left|\binom{n}{i} \cdot 1_K\right| \cdot |x|^i \cdot |y|^{n-i} \leq \sum_{i=0}^{n} \left|\binom{n}{i} \cdot 1_K\right| \cdot |x|^i \cdot |x|^{n-i} =$$
$$\left(\sum_{i=0}^{n} \left|\binom{n}{i} \cdot 1_K\right|\right) \cdot |x|^n \leq B(n+1) \cdot |x|^n.$$

Taking n-th roots, we obtain

$$|x+y| \leq B^{\frac{1}{n}}(1+n)^{\frac{1}{n}}|x|.$$

We can now take limit as $n \to \infty$, and we get $|x+y| \leq |x| = \max\{|x|, |y|\}$.

□

Remark 2.18. *Let K be a field.*

1. *To shorten notation, we will write $n \cdot 1_K \in K$ as $n \in K$, whenever there is no possibility of confusion. Recall that, when the characteristic of K is not zero, the map $\mathbb{N} \to K$ sending 1 into 1_K is not injective.*

2. *Let $|\cdot|$, $|\cdot|'$ be two different absolute values. It does not hold, in general, that $|n|$ and $|n|'$ coincide for every $n \in \mathbb{N}$. For instance, take $K = \mathbb{Q}$, and let $p > 0$ be a prime number. Then $|p|_p = p^{-1} \neq p = |p|_\infty$.*

Definition 2.19. *Let K be a field, and $|\cdot|$ an absolute value. We will say that a sequence $(x_n)_n$ of elements of K* converges to zero with respect to $|\cdot|$ *if and only if $(|x_n|)_n$ converges to zero in $\mathbb{R}$ with respect to the standard absolute value $|\cdot|_\infty$.*

Definition 2.20. *Let K be a field. We will say that two absolute values $|\cdot|$, $|\cdot|'$ are* equivalent *if, for all sequence $(x_n)_n$ of elements of K, the sequence $(x_n)_n$ converges to zero with respect to $|\cdot|$ if and only if it converges to zero with respect to $|\cdot|'$.*

We will now give a very strong characterisation of equivalence of absolute values.

Proposition 2.21. *Let K be a field, and let $|\cdot|$, $|\cdot|'$ be two nontrivial absolute values on K. The following conditions are equivalent:*

(i) *$|\cdot|$ and $|\cdot|'$ are equivalent.*

(ii) *For all $x \in K$, $|x| < 1 \Rightarrow |x|' < 1$.*

(iii) *There exists a real number $s > 0$ such that, for all $x \in K$,*

$$|x| = (|x|')^s.$$

Proof.

- (i)⇒ (ii) Assume that there exists $x \in K$ such that $|x| < 1$ but $|x|' \geq 1$. Then the sequence $(|x^n|)_n$ converges to zero, but the sequence $(|x^n|')_n$ does not converge to zero since all the terms satisfy $|x^n|' \geq 1$.

- (ii)⇒ (iii) Since $|\cdot|$ is a nontrivial absolute value, there exists $y \in K^\times$ such that $|y| \neq 1$. Let us fix such an element. The equality $|y| \cdot |y^{-1}| = |1| = 1$ shows that, from the two quantities $|y|$ and $|y^{-1}|$, one is greater than one and the other is smaller than one. Replacing y by y^{-1} if necessary, we can assume that $|y| > 1$.

  Therefore, we have $|y^{-1}| < 1$ and, by (ii), we obtain that $|y^{-1}|' < 1$, and the equality $|y|' \cdot |y^{-1}|' = 1$ implies that $|y|' > 1$.

Now let $x \in K$ be a nonzero element. Let $\alpha = \log(|x|)/\log(|y|)$; we have the equality

$$|x| = |y|^{\alpha}.$$

Let us consider a strictly decreasing sequence of rational numbers $(m_k/n_k)_k$ that approximates α from above; we have that

$$|x| = |y|^{\alpha} < |y|^{\frac{m_k}{n_k}},$$

so that

$$\left|\frac{x^{n_k}}{y^{m_k}}\right| < 1.$$

By (ii), this implies that

$$\left|\frac{x^{n_k}}{y^{m_k}}\right|' < 1,$$

thus

$$|x|' < (|y|')^{\frac{m_k}{n_k}},$$

and passing to the limit as $k \to \infty$, we obtain that $|x|' \leq (|y|')^{\alpha}$. We can repeat the same proceeding with a strictly increasing sequence of rational numbers $(m_k/n_k)_k$ approximating α from below; namely,

$$|x| = |y|^{\alpha} \geq |y|^{\frac{m_k}{n_k}},$$

hence

$$\left|\frac{y^{m_k}}{x^{n_k}}\right| < 1$$

and therefore by (ii)

$$\left|\frac{y^{m_k}}{x^{n_k}}\right|' < 1,$$

thus

$$(|y|')^{\frac{m_k}{n_k}} < |x|',$$

and passing to the limit when $k \to \infty$ we obtain that $(|y|')^{\alpha} \leq |x|'$. Hence we have equality

$$|x|' = (|y|')^{\alpha}$$

and in particular $\alpha = \log(|x|')/\log(|y|')$ (note that $|y|' > 1$, hence $\log(|y|') \neq 0$). Therefore we see that, for all nonzero $x \in K$, we have the equality

$$\log(|x|)/\log(|y|) = \log(|x|')/\log(|y|'). \tag{2.6}$$

Let $s := \log(|y|)/\log(|y|')$. Note that $s > 0$ because both $|y|$ and $|y|'$ are greater than 1. Equation 2.6 shows that $\log(|x|) = s\log(|x|')$, hence $|x| = (|x|')^s$, and this equality holds for all $x \in K^{\times}$.

- (iii)$\Rightarrow$ (i) This follows from the fact that, for all $s > 0$ and all sequence of positive real numbers $(r_n)_n$, we have that $r_n \to 0$ if and only if $r_n^s \to 0$.

□

Remark 2.22. *On $\mathbb{Q}$, we have defined the following absolute values, with are pairwise non-equivalent (Exercise 3 of Sheet 5):*

- *The trivial absolute value.*
- *The standard absolute value $|\cdot|_\infty$.*
- *For all prime number $p > 0$, the p-adic absolute value $|\cdot|_p$.*

We will now see that they are essentially (that is, up to equivalence) the only ones.

Theorem 2.23. *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime number $p > 0$.*

Proof. Let $|\cdot|$ be an absolute value on $\mathbb{Q}$. We will distinguish two cases.

- Case 1: $|\cdot|$ is nonarchimedean. By Lemma 2.17, this means that, for all $n \in \mathbb{N}$, $|n| \leq 1$. Since $|-1| = 1$, we have that, for all $a \in \mathbb{Z}$, $|a| \leq 1$. Consider the set

$$\mathfrak{p} := \{a \in \mathbb{Z} : |a| < 1\} \subset \mathbb{Z}.$$

  It is an ideal of $\mathbb{Z}$. Moreover, for all $a, b \in \mathbb{Z}$, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. That is to say, $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}$. And since $|\cdot|$ is not trivial, then $\mathfrak{p}$ is not the zero ideal (0). Therefore, there exists a prime number $p > 0$ such that

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

  In particular, $p \in \mathfrak{p}$, hence $|p| < 1$. Let us call $C = \frac{1}{|p|}$.

  Let now $u = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$, $p \nmid ab$. Then $|a| = |b| = 1$ (because they do not belong to $\mathfrak{p}$), hence $|u| = 1$.

  Consider now any $x \in \mathbb{Q}^\times$, and write it as $x = up^m$ for some u as above and $m \in \mathbb{Z}$. Then

$$|x| = |up^m| = |u| \cdot |p|^m = |p|^m = C^{-m} = C^{-v_p(x)}.$$

  By Exercise 2 of Sheet 4, we get that $|\cdot|$ is equivalent to $|\cdot|_p$.

- Case 2: $|\cdot|$ is archimedean. By Lemma 2.17 there exists an $n_0 \in \mathbb{N}$ such that $|n_0| > 1$. We are going to see that, for all $n > 1$, $|n| > 1$. Namely, pick $n > 1$. For all integers $m > 1$, for all $k \in \mathbb{N}$, we can write m^k in base n as follows:

$$m^k = \sum_{i=0}^{s} a_i n^i, \tag{2.7}$$

  where $0 \leq a_i < n$, and $a_s \neq 0$. Note that, in Equation (2.7), $m^k \geq n^s$, thus $k \log m \geq s \log n$.

Taking $|\cdot|$ in Equation (2.7), we obtain

$$|m^k| = \left|\sum_{i=0}^{s} a_i n^i\right| \leq \sum_{i=0}^{s} |a_i||n|^i \leq \left(\sum_{i=0}^{s} |a_i|\right) \max\{|n|^i : i = 0, \ldots, s\} \leq$$
$$\left(\sum_{i=0}^{s} |a_i|\right) \max\{|n|^s, 1\} \leq (s+1)(n-1)\max\{|n|^s, 1\}$$
$$\leq (k\frac{\log m}{\log n} + 1)(n-1)\max\{|n^{k\frac{\log m}{\log n}}|, 1\}.$$

Taking k-th roots of unity, we obtain

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

Letting now k tend to infinity, we obtain that

$$|m| \leq \max\{|n^{\frac{\log m}{\log n}}|, 1\} = \max\{|n|, 1\}^{\frac{\log m}{\log n}}. \tag{2.8}$$

This is valid for all $m \in \mathbb{N}$; in particular it holds for n_0. That is to say,

$$1 < |n_0| \leq \max\{|n|, 1\}^{\frac{\log n_0}{\log n}}. \tag{2.9}$$

Thus the maximum $\max\{|n|, 1\}$ cannot be 1, and therefore $|n| > 1$.

In particular, going back to Equation (2.8), we obtain that, for all integers $m, n \geq 1$

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

Interchanging the roles of m and n, we obtain

$$|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}.$$

Call $\alpha = |m|^{\frac{1}{\log m}}$, and note that $\alpha > 1$, thus $\log \alpha > 0$. We have that, for all $n \in \mathbb{N}$

$$|n| = \alpha^{\log n} = e^{(\log \alpha)(\log n)} = n^{\log \alpha} = |n|_\infty^{\log \alpha}.$$

Taking into account that $|-1| = 1 = |-1|_\infty$, we can extend the equation above to $n \in \mathbb{Z}$ as

$$|n|_\infty^{\log \alpha} = |n|.$$

Finally, for all $x \in \mathbb{Q}$, write $x = a/b$ with $a, b \in \mathbb{Z}$, $b \neq 0$. Then

$$|x| = \left|\frac{a}{b}\right| = \frac{|a|}{|b|} = \frac{|a|_\infty^{\log \alpha}}{|b|_\infty^{\log \alpha}} = \left|\frac{a}{b}\right|_\infty^{\log \alpha} = |x|_\infty^{\log \alpha}.$$

By Proposition 2.21, we obtain that $|\cdot|$ and $|\cdot|_\infty$ are equivalent.

□

Theorem 2.24 (Weak approximation theorem)**.** *Let K be a field, and let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise non-equivalent nontrivial absolute values. For each $a_1, \ldots, a_n \in K$, and for each $\varepsilon > 0$, there exists $x \in K$ such that*

$$|x - a_i|_i < \varepsilon$$

for all $i = 1, \ldots, n$.

Remark 2.25. *This statement is reminiscent of the classical Chinese remainder theorem, which claims the following: Let $m_1, \ldots, m_n$ positive integers which are pairwise coprime. Then, for any integers $a_1, \ldots, a_n$, there exists a positive integers x such that*

$$x \equiv a_i \pmod{m_i}.$$

for all $i = 1, \ldots n$. Decomposing each m_i into prime powers, one might reduce this statement to the case where each m_i is of the form $p_i^{r_i}$, for some prime number p_i and some exponent r_i. Now note that each of the congruences

$$x \equiv a_i \pmod{p_i^{r_i}}$$

is equivalent to the condition

$$|x - a_i|_{p_i} \leq p_i^{-r_i}. \tag{2.10}$$

Note that the weak approximation theorem produces an element $x \in \mathbb{Q}$ satisfying the conditions (2.10)*, but it may not be an integer.*

Proof of Theorem 2.24. First of all, note that it suffices to show that, for all $\delta > 0$, we can find a collection of elements $z_1, \ldots, z_n \in K$ such that

$$\begin{cases} |z_i|_j < \delta \text{ for } i \neq j \\ |z_i - 1|_i < \delta. \end{cases} \tag{2.11}$$

Indeed, given any set of elements $a_1, \ldots, a_n \in K$ and any $\varepsilon > 0$, set $B := \max\{|a_i|_j : 1 \leq i, j \leq n\}$, and produce a collection of elements $z_1, \ldots, z_n \in K$ as above with some $\delta < \frac{\varepsilon}{nB}$. Then the element $x = \sum_{j=1}^n a_j z_j$ satisfies that, for all $i = 1, \ldots, n$,

$$|x - a_i|_i = \left| \sum_{j \neq i} a_j z_j + a_i(z_i - 1) \right|_i \leq \sum_{j \neq i} |a_j|_i |z_j|_i + |a_i|_i |z_i - 1|_i \leq nB\delta < \varepsilon.$$

Thus it suffices to find z_1 satisfying Equations (2.11) with $i = 1$ (for other values of i it is analogous). Next we observe that it suffices to find z such that

$$\begin{cases} |z|_1 > 1 \\ |z|_j < 1 \text{ for } j = 2, \ldots, n \end{cases}$$

Namely, if we have such a z, then for all $m \in \mathbb{N}$, it holds that

$$|1 + z^m|_1 \geq ||1|_1 - |z|_1^m|_\infty = |z|_1^m - 1 \xrightarrow{m \to \infty} \infty.$$

Thus

$$\left|\frac{z^m}{1+z^m}-1\right|_1=\left|\frac{-1}{1+z^m}\right|_1 \xrightarrow{m\to\infty} 0.$$

On the other hand, for all $j\neq 1$, it holds that

$$|1+z^m|_j \geq ||1|_j-|z|_j^m|_\infty = 1-|z|_j^m \geq \frac{1}{2} \text{ for all } m \text{ sufficiently large,}$$

hence, for m large enough,

$$\left|\frac{z^m}{1+z^m}\right|_j \leq 2|z|^m \xrightarrow{m\to\infty} 0.$$

This shows that given any $\delta>0$ we can produce $z_1=\frac{z^m}{1+z^m}$ as in Equation (2.11) by choosing m large enough. Therefore, the proof of the theorem boils down to the following claim:

Fact 2.26. *There exists $z\in K$ such that*

$$\begin{cases} |z|_1>1 \\ |z|_j<1 \textit{ for all } j=2,\dots,n. \end{cases}$$

We will prove this fact this by induction on n.

- $n=2$: Since $|\cdot|_1$ and $|\cdot|_2$ are not equivalent (and $|\cdot|_1$ is nontrivial), there exists some $x\in K$ with $|x|_1<1$ but $|x|_2\geq 1$. Similarly there exists some $y\in K$ with $|y|_2<1$ but $|y|_1\geq 1$. Thus

  $$\left|\frac{y}{x}\right|_1 \geq \frac{1}{|x|_1}>1$$

  and

  $$\left|\frac{y}{x}\right|_2 \leq \frac{|y|_2}{1}<1.$$

- $n\Rightarrow n+1$: Assume we have $z\in K$ with $|z|_1>1$, $|z|_j<1$ for all $j=2,\dots,n$. Since we already know the result for just two absolute values, we can apply it to $|\cdot|_1$ and $|\cdot|_{n+1}$ to obtain some $y\in K$ such that $|y|_1>1$, $|y|_{n+1}<1$. We distinguish now three cases, according to the value of $|z|_{n+1}$:

  - Case 1: $|z|_{n+1}<1$. Then z already satisfies the required condition.
  - Case 2: $|z|_{n+1}=1$. Then for all $m\in\mathbb{N}$ we have that

    $$\begin{cases} |y\cdot z^m|_1>1 \\ |y\cdot z^m|_{n+1}=|y|_{n+1}<1 \\ |y\cdot z^m|_j=|y|_j\cdot|z|_j^m \xrightarrow{m\to\infty} 0<1 \text{ for } j=2,\dots,n. \end{cases}$$

    Thus it suffices to choose m large enough to ensure that $|y\cdot z^m|_j<1$ for all $j=2,\dots,n$.

– Case 3: $|z|_{n+1} > 1$. Then for all $m \in \mathbb{N}$ we have that

$$\begin{cases} |y \cdot \frac{z^m}{1+z^m}|_1 \xrightarrow{m\to\infty} |y|_1 > 1 \\ |y \cdot \frac{z^m}{1+z^m}|_{n+1} \xrightarrow{m\to\infty} |y|_{n+1} < 1 \end{cases}$$

Finally, for m big enough, we have that $|1 + z^m|_j \geq 1/2$ for all $j = 2, \dots n$. Then, for big enough m, we have

$$\left| y \cdot \frac{z^m}{1+z^m} \right|_j \leq |y|_j \frac{|z|_j^m}{1/2} \xrightarrow{m\to\infty} 0 < 1 \text{ for all } j = 2, \dots, n.$$

Again, it suffices to choose an integer m which is big enough to ensure that the desired inequalities hold.

□

Now we will take a closer look at nonarchimedean absolute values, and the filtration they induce on a field.

Proposition 2.27. *Let K be a field and let $|\cdot|$ be a nonarchimedean absolute value. Then the map*

$$v : K \to \mathbb{R} \cup \{\infty\}$$

defined as

$$v(x) = \begin{cases} -\log|x| \text{ if } x \neq 0 \\ \infty \text{ if } x = 0 \end{cases}$$

is a valuation on K, and

$$|x| = e^{-v(x)}.$$

Proof. Exercise 1 in Sheet 7. □

Remark 2.28. *Let $|\cdot|$, $|\cdot|'$ be two equivalent nonarchimedean absolute values on a field K. Let v and v' be the valuations attached to $|\cdot|$ and $|\cdot|'$ as above. By Proposition 2.21, there exists a real number $s > 0$ such that*

$$|\cdot|' = |\cdot|^s.$$

We obtain thus that $v' = s \cdot v$.

Definition 2.29. *We will say that two valuations $v, v' : K \to \mathbb{R} \cup \{\infty\}$ are* equivalent *if there exists some real number $s > 0$ such that $v' = s \cdot v$.*

By Proposition 2.27, the study of nonarchimedean absolute values on a field K is equivalent to the study of valuations $v : K \to \mathbb{R} \cup \{\infty\}$.

Proposition 2.30. *Let K be a field and $v : K \to \mathbb{R} \cup \{\infty\}$ a valuation. The set*

$$\mathcal{O} := \{x \in K : v(x) \geq 0\}$$

is a local ring with maximal ideal

$$\mathfrak{m} := \{x \in K : v(x) > 0\}.$$

Furthermore the invertible elements of $\mathcal{O}$ are

$$\mathcal{O}^\times = \{x \in K : v(x) = 0\}.$$

Proof.

- First we will see that $\mathcal{O}$ is a subring of K. We have to check the following conditions:

  1. Closed under addition: Let $a, b \in \mathcal{O}$. Then
  $$v(a+b) \geq \min\{v(a), v(b)\} \geq 0,$$
  thus $a + b \in \mathcal{O}$.
  2. Closed under multiplication: Let $a, b \in \mathcal{O}$. Then
  $$v(a \cdot b) = v(a) + v(b) \geq 0,$$
  thus $a \cdot b \in \mathcal{O}$.
  3. Neutral element for multiplication: Since $v(1) = 0$, $1 \in \mathcal{O}$.
  4. Closed under additive inverse: Let $a \in \mathcal{O}$, then
  $$v(-a) = v((-1) \cdot a) = v(-1) + v(a) = v(a) \geq 0,$$
  thus $-a \in \mathcal{O}$.

- Let us now check that $\mathfrak{m}$ is an ideal of $\mathcal{O}$:

  1. Closed under addition: Let $a, b \in \mathfrak{m}$. Then
  $$v(a+b) \geq \min\{v(a), v(b)\} > 0,$$
  thus $a + b \in \mathfrak{m}$.
  2. Closed under multiplication by elements of $\mathcal{O}$: Let $a \in \mathcal{O}$, $b \in \mathfrak{m}$. Then
  $$v(a \cdot b) = v(a) + v(b) > 0,$$
  thus $a \cdot b \in \mathfrak{m}$.

- The invertible elements in $\mathcal{O}$ are those $x \in \mathcal{O}$ such that $x^{-1} \in \mathcal{O}$. Since $v(x^{-1}) = -v(x)$, we obtain that x is invertible if and only if $v(x) \geq 0$ and $-v(x) \geq 0$, in other words, if and only if $v(x) = 0$.

  In particular, this shows that the elements of $\mathcal{O}$ which are not invertible are precisely the elements of $\mathfrak{m}$, which is an ideal. Thus we can conclude that $\mathfrak{m}$ is a maximal ideal, and moreover that it is the unique maximal ideal of $\mathcal{O}$.

□

Definition 2.31. *Let K be a field and v a valuation on K. We will call the ring $\mathcal{O} = \{x \in K : v(x) \geq 0\}$ the* valuation ring of v.

Remark 2.32. *Let K be a field, v a valuation on K and $\mathcal{O}$ the valuation ring.*

- *For every nonzero element in K, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ (of course, elements in $\mathcal{O}^\times$ satisfy both).*
- *Let v be a valuation on K and $\mathcal{O}$ the valuation ring of v. We can recover K as the fraction field of $\mathcal{O}$ (this follows easily from the first part of the remark).*
- *Let v' be another valuation on K which is equivalent to v. Then the valuation ring of v' coincides with $\mathcal{O}$.*

Example 2.33. *Let $p > 0$ be a prime number, and consider the p-adic valuation v_p in $\mathbb{Q}$. Then the valuation ring is*

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

the localisation of the ring $\mathbb{Z}$ at the prime ideal (p). This is a local ring, with maximal ideal $p\mathbb{Z}_{(p)}$.

Note that

$$\mathbb{Z} \subsetneq \mathbb{Z}_{(p)} \subsetneq \mathbb{Q}.$$

Proposition 2.34. *Let K be a field, v a valuation. Then the valuation ring $\mathcal{O}$ of v is integrally closed.*

Proof. Let $x \in K$ be an element which is integral over $\mathcal{O}$; we have to prove that $x \in \mathcal{O}$. We can assume $x \neq 0$. Assume moreover that $x \notin \mathcal{O}$. Then $v(x) < 0$. Therefore $v(x^{-1}) > 0$, thus $x^{-1} \in \mathcal{O}$.

On the other hand, the condition that x is integral over $\mathcal{O}$ means that there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in \mathcal{O}$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Dividing by x^{n-1} in the equation above, we get that

$$x = -a_{n-1} - \cdots - a_1 x^{-(n-2)} - a_0 x^{-(n-1)} = -a_{n-1} - \cdots - a_1 (x^{-1})^{n-2} - a_0 (x^{-1})^{n-1} \in \mathcal{O},$$

contradicting the assumption that $x \notin \mathcal{O}$. □

Now we focus on a special kind of valuations.

Definition 2.35. *Let K be a field and let $v : K \to \mathbb{R} \cup \{\infty\}$ be a valuation. We say that v is a* discrete valuation *if the set*

$$\{v(x) : x \in K^\times \text{ satisfies } v(x) > 0\}$$

has a minimum (that is to say, if the infimum of the set is an element of the set).

Example 2.36. *The p-adic valuation on $\mathbb{Q}$ is a discrete valuation; namely, we have*

$$\{x \in \mathbb{Q}^\times \text{ with } v_p(x) > 0\} = \left\{ \frac{a}{b} : p|a \text{ and } p \nmid b \right\}$$

and

$$\{v_p(x) : x \in \mathbb{Q}^\times \text{ with } v_p(x) > 0\} = \{1, 2, 3, \dots\}$$

has a minimal value, namely $1 = v_p(p)$.

Remark 2.37. *Not all valuations need to be discrete. We will see examples of non-discrete valuations later in the lecture.*

Lemma 2.38. *Let K be a field and v a discrete valuation on K. Let*

$$s = \min\{v(x) : x \in K^\times \text{ satisfies } v(x) > 0\}.$$

Then

$$v(K^\times) = s\mathbb{Z}.$$

Proof. Let $x \in K^\times$ be such that $v(x) = s$. Then, for all $m \in \mathbb{Z}$,

$$v(x^m) = m \cdot s,$$

thus $v(K^\times) \supset s\mathbb{Z}$.

Reciprocally, let us take $y \in K^\times$.

$$v(y) \in \mathbb{R} = \bigsqcup_{m\in\mathbb{Z}} [ms, (m+1)s)$$

Thus $v(y)$ belongs to one of the intervals in the above union, say $[ms, (m+1)s)$, for some $m \in \mathbb{Z}$. Therefore

$$v(yx^{-m}) \in [0, s).$$

But by the definition of s, we cannot have that $0 < v(yx^{-m}) < s$, thus $v(yx^{-m}) = 0$. Therefore $v(y) = v(x^m) = ms \in s\mathbb{Z}$, as we wanted to prove. □

Remark 2.39. *Recall that, if R is an integral domain, an element $r \in R$ is called a* prime element *if r is a nonzero, nonunit element such that, for all $s, t \in R$, it holds:*

$$r|(s \cdot t) \text{ if and only if } r|s \text{ or } r|t.$$

Let K be a field and let v a discrete valuation on K. Then the valuation ring $\mathcal{O}$ of v is an integral domain, and π is a prime element if and only if

$$v(\pi) = \min\{v(x) : x \in K^\times \text{ satisfies } v(x) > 0\}$$

(see Exercise 2 of Sheet 9). In other words, π is a prime element if and only if $v(K^\times) = v(\pi)\mathbb{Z}$.

Definition 2.40. *We will say that v is* normalised *if $v(K^\times) = \mathbb{Z}$.*

Remark 2.41.

- *Every discrete valuation is equivalent to a normalised discrete valuation.*
- *Let v, v' be equivalent valuations on a field K. We know that their valuation rings coincide; let us call it $\mathcal{O}$. Then π is a prime element of v if and only if π is a prime element of v'.*
- *Let K be a field, v a normalised discrete valuation of K, $\mathcal{O}$ the valuation ring of v, and $\pi \in K^\times$. Then π is a prime element of $\mathcal{O}$ if and only if the ideal $\pi\mathcal{O}$ is a prime ideal of $\mathcal{O}$ (see Exercise 1 of Sheet 9).*

Corollary 2.42. *Let K be a field, v a discrete valuation on K and $\mathcal{O}$ the valuation ring of v. Fix a prime element $\pi \in \mathcal{O}$. Then every element $x \in K^\times$ can be uniquely written as*

$$x = u \cdot \pi^m$$

for some $m \in \mathbb{Z}$ and some $u \in \mathcal{O}^\times$.

Proof. We may assume without loss of generality that v is normalised. Let $x \in K^\times$, and call $m = v(x)$. Then $v(x\pi^{-m}) = 0$, thus $u = x\pi^{-m} \in \mathcal{O}^\times$, and $x = u\pi^m$.

As for the uniqueness, if we had

$$u\pi^m = u'\pi^{m'} \tag{2.12}$$

for some $u, u' \in \mathcal{O}^\times$ and $m, m' \in \mathbb{Z}$, then

$$m = v(u\pi^m) = v(u'\pi^{m'}) = m';$$

and the equality (2.12) boils down to $u\pi^m = u'\pi^m$, whence $u = u'$. □

Proposition 2.43. *Let K be a field and let v be a discrete valuation on K. Fix a prime element π. Then the proper nonzero ideals of $\mathcal{O}$ are precisely those of the form*

$$(\pi^n) : n \in \mathbb{N}.$$

In particular, if v is normalised, the proper ideals of $\mathcal{O}$ are precisely those of the form

$$\{x \in \mathcal{O} : v(x) \geq n\} : n \in \mathbb{N} \cup \{\infty\}.$$

Proof. We may assume, without loss of generality, that v is normalised. Since $v(K^\times) = \mathbb{Z}$ and $\mathcal{O} = \{x \in K : v(x) \geq 0\}$, we obtain that

$$v(\mathcal{O}) = \{0, 1, 2, \dots\} \cup \{\infty\} = \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

Let $\mathfrak{a}$ be a proper nonzero ideal of $\mathcal{O}$. The properness of $\mathfrak{a}$ implies that there is no unit of $\mathcal{O}$ contained in $\mathfrak{a}$; thus we have the inclusion of sets

$$\{v(x) : x \in \mathfrak{a}\} \subseteq \mathbb{Z}_{>0} \cup \{\infty\}.$$

Hence the set $\{v(x) : x \in \mathfrak{a}\}$ has a minimum (which is not ∞), say $n_0 \geq 1$. Let $x \in \mathfrak{a}$ be such that $v(x) = n_0$. We can write x as $x = u_0 \cdot \pi^{n_0}$ for some u_0 with $v(u_0) = 0$. Thus $u_0 \in \mathcal{O}^\times$, and $\pi^{n_0} \in \mathfrak{a}$, whence $(\pi^{n_0}) \subset \mathfrak{a}$. We will now show that $\mathfrak{a} = (\pi^{n_0})$. Namely, let $a \in \mathfrak{a}$. We can write $a = u\pi^m$ for some $m \in \mathbb{Z}_{\geq 0}$. But then by definition of n_0, we have $m \geq n_0$, so that $\pi^{m-n_0} \in \mathcal{O}$ and $a = u\pi^{m-n_0} \cdot \pi^{n_0} \in (\pi^{n_0})$. □

Lemma 2.44. *Let K be a field, v a discrete valuation on K, $\mathcal{O}$ the valuation ring of v, π a prime element of $\mathcal{O}$ and $\mathfrak{m} = (\pi)$ the maximal ideal of $\mathcal{O}$, $k = \mathcal{O}/\mathfrak{m}$. Then for all $n \in \mathbb{N}$, we have an isomorphism*

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} \simeq \mathcal{O}/\mathfrak{m}$$

as k-vector spaces.

Proof. Clearly $\mathcal{O}/\mathfrak{m} = k$ is a 1-dimensional k-vector space.

On the other hand, $\mathfrak{m}^n$, as an ideal of $\mathcal{O}$, is an commutative group with the addition, and $\mathfrak{m}^{n+1}$ is a subgroup of $\mathfrak{m}^n$. Hence the quotient $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ has a structure of commutative group. One can define a map

$$\begin{aligned} \mathcal{O}/\mathfrak{m} \times \mathfrak{m}^n/\mathfrak{m}^{n+1} &\to \mathfrak{m}^n/\mathfrak{m}^{n+1} \\ (a+\mathfrak{m}, \alpha + \mathfrak{m}^{n+1}) &\mapsto a\alpha + \mathfrak{m}^{n+1}. \end{aligned}$$

This is well defined map, and endows $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ with a structure of $\mathcal{O}/\mathfrak{m}$-module, that is to say, of k-vector space.

Consider the map

$$\begin{aligned} \varphi : \mathcal{O}/\mathfrak{m} &\to \mathfrak{m}^n/\mathfrak{m}^{n+1} \\ a+\mathfrak{m} &\mapsto a\pi^n + \mathfrak{m}^{n+1}. \end{aligned}$$

This map is a morphism of k-vector spaces, and one easily sees that it is bijective. □

Remark 2.45. *Let K be a field, v a normalised discrete valuation and $\mathcal{O}$ the valuation ring. Proposition 2.43 shows in particular that $\mathcal{O}$ is a principal ideal domain, and Proposition 2.30 shows that $\mathcal{O}$ is a local ring. From Proposition 2.43 one can also deduce that $\mathcal{O}$ is a Noetherian ring. We can also read the Krull dimension of $\mathcal{O}$ from Proposition 2.43; namely, the zero ideal is prime (because $\mathcal{O}$ is an integral domain), and of all the proper nonzero ideals, only (π) is prime. Thus the Krull dimension of $\mathcal{O}$ is 1. Finally, Lemma 2.44 shows that $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1 = \dim_{\mathrm{Krull}} \mathcal{O}$; in other words, $\mathcal{O}$ is regular.*

Recall that a discrete valuation ring *is a regular local ring of Krull dimension* 1. *We just saw that the valuation ring of a discrete valuation is a discrete valuation ring. The reciprocal is also true, and will be proven in Exercise 1 of Sheet 8.*

Definition 2.46. *Let K be a field, v a discrete valuation on K, $\mathcal{O}$ the valuation ring of v and $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$. For each $n \in \mathbb{N}$, we define the n-*th higher unit group *as the multiplicative group*

$$U^{(n)} := 1 + \mathfrak{m}^n.$$

Furthermore we call $U^{(1)}$ the group of principal units.

Remark 2.47.

1. *For all $n \in \mathbb{N}$, we have the inclusion $U^{(n)} \subset \mathcal{O}^\times$. Namely, let $u = 1+x \in U^{(n)}$. Then $x \in \mathfrak{m}^n \subset \mathfrak{m}$, thus $v(x) > 0$. Therefore $v(x) \neq v(1)$ and we obtain that $v(1+x) = \min\{v(1), v(x)\} = 0$. Thus $u \in \mathcal{O}^\times$.*

2. *$U^{(n)}$ is a subgroup of $\mathcal{O}^\times$. Namely, it is clearly closed under multiplication, and the neutral element of $\mathcal{O}^\times$, which is* 1*, belongs to $U^{(n)}$. Let us see that it is closed under taking inverses. Let $u = 1 + x \in U^{(n)}$. To prove that $u^{-1} \in U^{(n)}$, we have to show that $u^{-1} - 1 \in \mathfrak{m}^n$. But*

$$u^{-1} - 1 = (1+x)^{-1} - 1 = (1+x)^{-1}(1 - (1+x)) = (1+x)^{-1}(-x) \in \mathfrak{m}^n.$$

As a conclusion, we have the following decreasing sequence of multiplicative groups

$$\mathcal{O}^\times \supset U^{(1)} \supset U^{(2)} \supset \cdots \supset U^{(n)} \supset \cdots$$

Proposition 2.48. *For each $n \geq 1$, we have the group isomorphisms*

$$\mathcal{O}^\times / U^{(n)} \simeq (\mathcal{O}/\mathfrak{m}^n)^\times$$

Proof. Consider the projection $p_n : \mathcal{O} \to \mathcal{O}/\mathfrak{m}^n$, which is a ring morphism. If $x \in \mathcal{O}^\times$, then it follows that $p_n(x) \in (\mathcal{O}/\mathfrak{m}^n)^\times$ (namely, the inverse of $p_n(x)$ in $\mathcal{O}/\mathfrak{m}^n$ is $x^{-1} + \mathfrak{m}^n$). Therefore we can restrict p_n to $\mathcal{O}^\times$ and obtain a map (which we still call p_n)

$$p_n : \mathcal{O}^\times \to (\mathcal{O}/\mathfrak{m}^n)^\times.$$

This map is still a group morphism with respect to the multiplication. Moreover, it is surjective. Namely, for any $x + \mathfrak{m}^n \in (\mathcal{O}/\mathfrak{m}^n)^\times$, let $y + \mathfrak{m}^n \in \mathcal{O}/\mathfrak{m}^n$ be such that

$$(x + \mathfrak{m}^n)(y + \mathfrak{m}^n) = 1 + \mathfrak{m}^n$$

In particular, we obtain that $xy - 1 \in \mathfrak{m}^n$; in particular, xy is a unit in $\mathcal{O}$. Thus $x \in \mathcal{O}^\times$, and $p_n(x) = x + \mathfrak{m}^m$.

Finally, we need to compute the kernel of p_n: if $x \in \mathcal{O}^\times$ is such that $p_n(x) = 1 + \mathfrak{m}^m$, then $x - 1 \in \mathfrak{m}^n$, that is to say, $x \in U^{(n)}$.

□

3 Completions

Our aim in this section is to generalise the construction of the real numbers from the rational numbers. Recall briefly that one defines $\mathbb{R}$ as the set of all Cauchy sequences of elements of $\mathbb{Q}$, modulo the subset of sequences that converge to zero, and endows this with the natural addition and multiplication (one defines the addition and multiplication of two sequences component-wise). Of course, here the notion of Cauchy sequence is defined with respect to the standard absolute value $|\cdot|_\infty$. But nothing prevents us from repeating this process using a different absolute value!

Definition 3.1. *Let K be a field and let $|\cdot|$ be an absolute value. We say that a sequence $(a_n)_{n\in\mathbb{N}}$ of elements of K is a* Cauchy sequence *if, for all $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that*

$$|a_n - a_m| < \varepsilon \qquad \text{for all } m, n \in \mathbb{N} \text{ such that } m, n \geq N.$$

Definition 3.2. *Let K be a field and let $|\cdot|$ be an absolute value on K. We say that K is* complete with respect to $|\cdot|$ *if every Cauchy sequence $(a_n)_n$ of element of K converges to an element of K. In other words, if there exists $a \in K$ such that*

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Example 3.3. *$\mathbb{Q}$ is not a complete field with respect to the standard absolute value $|\cdot|_\infty$, whereas $\mathbb{R}$ and $\mathbb{C}$ are complete with respect to the standard absolute value $|\cdot|_\infty$.*

Definition 3.4. *Let K be a field and let $|\cdot|$ be an absolute value on K. A* completion *of $(K, |\cdot|)$ is a field $\widehat{K}$, endowed with an absolute value $|\cdot|'$, such that*

- *K is a subfield of $\widehat{K}$, and the restriction of $|\cdot|'$ to K coincides with $|\cdot|$.*
- *K is dense in $\widehat{K}$, that is to say, for each $\varepsilon > 0$ and each $y \in \widehat{K}$ there exists an $x \in K$ such that $|y - x|' < \varepsilon$.*
- *$\widehat{K}$ is complete with respect to $|\cdot|'$.*

Remark 3.5. *A field K endowed with an absolute value $|\cdot|$ has at most one completion up to isomorphism. That is to say, if $(\widehat{K}_1, |\cdot|_1)$ and $(\widehat{K}_2, |\cdot|_2)$ are two completions of K, then there exists a field isomorphism $\varphi : \widehat{K}_1 \to \widehat{K}_2$ such that for all $x \in \widehat{K}_1$, $|x|_1 = |\varphi(x)|_2$ (see Exercise 1 of Sheet 9). Thus by abuse of notation we will speak about* the *completion of a field*

Example 3.6. *$(\mathbb{R}, |\cdot|_\infty)$ is the completion of $\mathbb{Q}$ with respect to the standard absolute value.*

Our aim now is to prove that every field endowed with an absolute value has a completion. We start with a simple lemma.

Lemma 3.7. *Let K be a field and let $|\cdot|$ be an absolute value. The set R of all Cauchy sequences of elements of K is a ring with the addition and multiplication defined as:*

$$\begin{aligned} + : R \times R \to R & \qquad \cdot : R \times R \to R \\ (a_n)_n, (b_n)_n \mapsto (a_n + b_n)_n & \qquad (a_n)_n, (b_n)_n \mapsto (a_n \cdot b_n)_n. \end{aligned}$$

The set

$$\mathfrak{m} := \{(a_n)_n : a_n \xrightarrow{n\to\infty} 0\}$$

is an ideal of R.

Proof. Exercise 2 of Sheet 9. □

Proposition 3.8. *The quotient ring $R/\mathfrak{m}$ is a field.*

Proof. Let $(a_n)_n$ be a Cauchy sequence which does not belong to $\mathfrak{m}$. We have to prove that its class in $R/\mathfrak{m}$, which we denote by $[(a_n)_n]$, is invertible in $R/\mathfrak{m}$.

First of all, $(a_n)_n$ does not tend to zero as n tends to ∞. That is to say, there exists some $\varepsilon_0 > 0$ such that, for all $M \in \mathbb{N}$ there exists some $m > M$ satisfying

$$|a_m| \geq \varepsilon_0. \tag{3.13}$$

On the other hand, since $(a_n)_n$ is a Cauchy sequence, given the positive number $\varepsilon_0/2$, there exists some $N_0 \in \mathbb{N}$ such that, for all $n, n' \geq N_0$,

$$|a_n - a_{n'}| < \varepsilon_0/2.$$

In particular, by Equation (3.13) there exists an $m_0 \in \mathbb{N}$, $m_0 \geq N_0$ satisfying that $|a_{m_0}| \geq \varepsilon_0$. Therefore, for all $n \geq N_0$, we have that

$$|a_n| = |a_n - a_{m_0} + a_{m_0}| \geq ||a_n - a_{m_0}| - |a_{m_0}|| > \varepsilon_0/2.$$

In particular, $|a_n| \neq 0$, thus $a_n \neq 0$ and we may consider a_n^{-1}.

Define the sequence $(b_n)_n$ as

$$b_n = \begin{cases} 1 \text{ if } n \leq N_0 \\ a_n^{-1} \text{ if } n > N_0. \end{cases}$$

Let us see that $(b_n)_n$ is a Cauchy sequence. Let $\varepsilon > 0$. Since $(a_n)_n$ is a Cauchy sequence, we know that there exists some $N_1 \in \mathbb{N}$ such that, for all $n, n' \geq N_1$,

$$|a_n - a_{n'}| < \frac{1}{4}\varepsilon \cdot \varepsilon_0^2.$$

We may assume, without loss of generality, that $N_1 \geq N_0$. Then

$$|b_n - b_{n'}| = \left|\frac{1}{a_n} - \frac{1}{a_{n'}}\right| = \frac{|a_n - a'_n|}{|a_n a'_n|} \leq \frac{|a_n - a'_n|}{(\varepsilon_0/2)^2} < \varepsilon.$$

On the other hand, we have that

$$a_n b_n - 1 = \begin{cases} a_n - 1 \text{ if } n \leq N_0 \\ 0 \text{ if } n > N_0. \end{cases}$$

In other words, if we denote by $\mathbf{1}$ the sequence which is constantly 1, we have that $(a_n)_n \cdot (b_n)_n - \mathbf{1}$ is a sequence which is constantly equal to zero from one point onwards, and thus lies in $\mathfrak{m}$. That is to say,

$$[(a_n)_n] \cdot [(b_n)_n] = [\mathbf{1}],$$

thus $[(a_n)_n]$ is invertible in $R/\mathfrak{m}$.

□

Let us denote

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

Remark 3.9. *The map*

$$\begin{aligned} i : K &\to \widehat{K} \\ a &\mapsto (a)_n \end{aligned}$$

is an injective ring morphism.

Remark 3.10. *Let K be a field, let $|\cdot|$ be an absolute value, and $(a_n)_n$ a Cauchy sequence. Then we can consider the sequence $(|a_n|)_n$ of real numbers. This is a Cauchy sequence in $\mathbb{R}$ (with respect to the standard absolute value $|\cdot|_\infty$), because of the inequality*

$$||a_n| - |a_m||_\infty < |a_n - a_m|.$$

Since in $\mathbb{R}$ all Cauchy sequences have a limit, we can consider the real number

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

Lemma 3.11. *Let K be a field, $|\cdot|$ an absolute value, $\widehat{K}$ its completion. Then the map*

$$\begin{aligned} |\cdot|_{\widehat{K}} : \widehat{K} &\to \mathbb{R}_{\geq 0} \\ [(a_n)_n] &\mapsto \lim_{n\to\infty} |a_n| \end{aligned}$$

is an absolute value on $\widehat{K}$. Moreover $|\cdot|_{\widehat{K}}$ is nonarchimedean if and only if the absolute value $|\cdot|$ on K is nonarchimedean.

Proof. Exercise 3 of Sheet 9. □

Remark 3.12. *The image of the map $i : K \to \widehat{K}$ defined in Remark 3.9 is dense in $\widehat{K}$ with respect to the absolute value $|\cdot|_{\widehat{K}}$. In other words, every element of $\widehat{K}$ can be approximated by elements of K (viewed inside $\widehat{K}$ via i) with respect to the absolute value $|\cdot|_{\widehat{K}}$.*

Lemma 3.13. *Let K be a field, $|\cdot|$ an absolute value on K. Then the field $\widehat{K}$ is complete with respect to $|\cdot|_{\widehat{K}}$.*

Proof. Consider a Cauchy sequence $(C_m)_m$ in $\widehat{K}$. Namely, for each $m \in \mathbb{N}$, C_m is the class of a sequence $(a_n^{(m)})_n$, such that the corresponding sequence of classes $(C_m)_m$ is a Cauchy sequence in $\widehat{K}$. We define an element $C = [(c_n)_n] \in \widehat{K}$ as follows. Since the image of K inside $\widehat{K}$ via the map i defined in Remark 3.9 is dense, we can choose, for each $n \in \mathbb{N}$, an element $c_n \in K$ such that

$$|C_n - i(c_n)|_{\widehat{K}} < \frac{1}{n}$$

We claim that the sequence $(c_n)_n$ is a Cauchy sequence in K. Indeed, fix $\varepsilon > 0$. Since $(C_m)_m$ is a Cauchy sequence, there exist $M > 0$ such that, for all $m_1, m_2 > M$, $|C_{m_1} - C_{m_2}|_{\widehat{K}} < \varepsilon/2$. Then for all $n_1, n_2 > \max\{4/\varepsilon, M\}$ it holds that

$$\begin{aligned} |c_{n_1} - c_{n_2}| = |i(c_{n_1}) - i(c_{n_2})|_{\widehat{K}} &\leq |i(c_{n_1}) - C_{n_1}|_{\widehat{K}} + |C_{n_1} - C_{n_2}|_{\widehat{K}} + |C_{n_2} - i(c_{n_2})|_{\widehat{K}} \\ &< \frac{1}{n_1} + \varepsilon/2 + \frac{1}{n_2} < \varepsilon/4 + \varepsilon/2 + \varepsilon/4 = \varepsilon. \end{aligned}$$

Hence, we may consider the class $C = [(c_n)_n)] \in \widehat{K}$. It remains to prove that the sequence $(C_m)_m$ converges to C with respect to $|\cdot|_{\widehat{K}}$. Fix $\varepsilon > 0$. We have just proved that $(c_n)_n$ is a Cauchy sequence; hence there exists $N > 0$ such that, for all $n_1, n_2 > N$, $|c_{n_1} - c_{n_2}| < \varepsilon/2$. Then it follows that, for all $m > \max\{2/\varepsilon, N\}$ it holds that

$$|C_m - C|_{\widehat{K}} \leq |C_m - i(c_m)|_{\widehat{K}} + |i(c_m) - C|_{\widehat{K}} < \frac{1}{m} + \lim_{n\to\infty} |c_m - c_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

□

We have thus proven the following proposition.

Proposition 3.14. *Let K be a field, $|\cdot|$ an absolute value. Then the field $\widehat{K} := R/\mathfrak{m}$, together with $|\cdot|_{\widehat{K}}$, is a completion of $(K, |\cdot|)$.*

We state and prove a lemma about fields of positive characteristic. This lemma could have been proven immediately after the characterisation of nonarchimedean absolute values (Lemma 2.17).

Lemma 3.15. *Let K be a field of positive characteristic, and $|\cdot|$ an absolute value. Then $|\cdot|$ is nonarchimedean.*

Proof. Since the characteristic of K is positive, there exists some prime number $p > 0$ such that $p \cdot 1_K = 0$. Therefore

$$\{|n \cdot 1_K| : n \in \mathbb{N}\} = \{|1_K|, |2 \cdot 1_K|, \ldots, |(p-1) \cdot 1_K|, |0|\}$$

is a finite subset of $\mathbb{R}$. But a finite subset of $\mathbb{R}$ is always bounded. Therefore by Lemma 2.17, we conclude that $|\cdot|$ is nonarchimedean. □

Our aim now is to study complete fields. First we will consider the case of complete fields with respect to an archimedean absolute value. We have two very familiar examples, namely $(\mathbb{R}, |\cdot|_\infty)$, $(\mathbb{C}, |\cdot|_\infty)$.

Theorem 3.16 (Ostrowski)**.** *Let K be a complete field with respect to an archimedean valuation $|\cdot|$. Then K is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, and $|\cdot|$ is equivalent to the standard absolute value $|\cdot|_\infty$.*

Proof. Since $|\cdot|$ is archimedean, the characteristic of K is zero (cf. Lemma 3.15). Therefore we have an inclusion $\mathbb{Q} \subset K$. The restriction of $|\cdot|$ to $\mathbb{Q}$ is an achimedean absolute value on $\mathbb{Q}$, hence by Theorem 2.23 it is equivalent to the standard absolute value $|\cdot|_\infty$. That is to say, there is an $s > 0$ such that, for all $x \in \mathbb{Q}$, $|x|^s = |x|_\infty$. Without loss of generality, we may replace $|\cdot|$ by $|\cdot|^s$, and thus assume that $|\cdot|$ and $|\cdot|_\infty$ coincide on $\mathbb{Q}$.

Since K is complete, every Cauchy sequence in $\mathbb{Q}$ (with respect to $|\cdot|$) converges in K. In this way we can construct an injective ring morphism $\mathbb{R} \to K$; namely, for each $r \in \mathbb{R}$, choose a sequence of rational numbers $(a_n)_n$ such the limit of $(a_n)_n$ in $\mathbb{R}$, with respect to the standard absolute value, coincides with r. Then we can define

$$\varphi(r) := \lim_{n\to\infty} a_n,$$

where this limit is taken in K, with respect to $|\cdot|$.

We have thus

$$\mathbb{R} \simeq \varphi(\mathbb{R}) \subset K.$$

We will identify $\mathbb{R}$ with $\varphi(\mathbb{R})$, and say that $\mathbb{R} \subset K$ (via φ). Moreover, by the definition of φ, the restriction of $|\cdot|$ to $\mathbb{R}$ coincides with the standard absolute value on $\mathbb{R}$.

If $K = \mathbb{R}$, then we are done. We will therefore assume the inclusion $\mathbb{R} \subset K$ is strict.

We will reduce the proof of the theorem to the following fact.

Fact 3.17. *Every element of K satisfies a quadratic equation with coefficients in $\mathbb{R}$.*

Let us assume Fact 3.17. Take an element $\alpha \in K \setminus \mathbb{R}$. By the fact above, there exist some $a, b \in \mathbb{R}$ such that $\alpha^2 + a\alpha + \beta = 0$. Thus $[\mathbb{R}(\alpha) : \mathbb{R}] = 2$, and we have the inclusions

$$\mathbb{R} \subset \mathbb{R}(\alpha) \subset K.$$

There is an isomorphism

$$\psi : \mathbb{R}[X]/\langle X^2 + aX + B\rangle \to \mathbb{R}[\alpha].$$

Since $\mathbb{C}$ is algebraically closed, there exists an element $z \in \mathbb{C}$ satisfying that $z^2 + az + b = 0$. This allows us to define an injective map

$$\varphi : \mathbb{R}[X]/\langle X^2 + aX + b\rangle \to \mathbb{C}$$

such that φ acts as the identity on $\mathbb{R}$, and maps X to z.

The composition $\varphi \circ \psi^{-1}$ gives us an injective ring morphism $\mathbb{R}[\alpha] \to \mathbb{C}$, which can be extended to an injective ring morphism

$$\Phi : \mathbb{R}(\alpha) \to \mathbb{C}.$$

Thus we have the inclusions

$$\mathbb{R} \subset \mathbb{R}(\alpha) \subset \mathbb{C},$$

where $[\mathbb{C} : \mathbb{R}] = 2 = [\mathbb{R} : \mathbb{R}(\alpha)]$, thus $\mathbb{R}(\alpha) = \mathbb{C}$.

In other words, we have proven that $\mathbb{C} \subset K$. Reciprocally, let $\beta \in K$. Then, by the Fact above, β satisfies a quadratic equation with coefficients in $\mathbb{R}$, say $f(\beta) = 0$ for $f(X) = Z^2 + cX + d \in \mathbb{R}[X]$. The polynomial $f(X)$ has at most two roots in K. But since $\mathbb{C}$ is algebraically closed, $f(X)$ has two roots (counting multiplicities) in $\mathbb{C}$, thus β must belong to $\mathbb{C}$. Finally, note that there is a unique extension of the standard absolute value $|\cdot|_\infty$ on $\mathbb{R}$ to $\mathbb{C}$, namely the standard absolute value on $\mathbb{C}$ (Exercise on some future Sheet).

Therefore the proof of the theorem boils down to Fact 3.17.

Proof of Fact. Let $\alpha \in K$. Consider the function

$$\begin{aligned} f : \mathbb{C} &\to \mathbb{R} \\ z &\mapsto |\alpha^2 - (z + \overline{z})\alpha + z\overline{z}| \end{aligned}$$

where $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$.

We have that

$$\begin{aligned} &|f(z_1) - f(z_2)|_\infty = ||\alpha^2 - (z_1 + \overline{z}_1)\alpha + z_1\overline{z}_1| - |\alpha^2 - (z_2 + \overline{z}_2)\alpha + z_2\overline{z}_2||_\infty \\ &\leq |(\alpha^2 - (z_1 + \overline{z}_1)\alpha + z_1\overline{z}_1) - (\alpha^2 - (z_2 + \overline{z}_2)\alpha + z_2\overline{z}_2)| = |(z_2 - z_1 + \overline{z}_2 - \overline{z}_1)\alpha + z_1\overline{z}_1 - z_2\overline{z}_2| \\ &\leq (|z_2 + \overline{z}_2 - (z_1 + \overline{z}_1)|)|\alpha| + |z_1\overline{z}_1 - z_2\overline{z}_2| = (|z_2 + \overline{z}_2 - (z_1 + \overline{z}_1)|_\infty)|\alpha| + |z_1\overline{z}_1 - z_2\overline{z}_2|_\infty. \end{aligned}$$

Since both functions $f_1(z) = z + \overline{z}$ and $f_2(z) = z\overline{z}$ are continuous with respect to $|\cdot|_\infty$, we obtain that the function f is a continuous function (with respect to the standard absolute value on both sides).

Clearly the limit of $|f(z)|_\infty$ is ∞ when $|z|_\infty \to \infty$. Therefore it has a minimum value, say $|f(z_0)|_\infty = m$. If we prove that $m = 0$, then we are done, because we would have the equality $\alpha^2 - (z_0 + \overline{z}_0)\alpha + z_0\overline{z}_0 = 0$, and the numbers $z_0 + \overline{z}_0, z_0\overline{z}_0$ belong to $\mathbb{R}$.

Consider the set

$$S = \{z \in \mathbb{C} : f(z) = m\}.$$

Note that this set is nonempty, closed and different from $\mathbb{C}$ (since $|f(z)|_\infty$ goes to ∞ as $|z|_\infty$ grows). We will prove that, if $m > 0$, it is also open, which is a contradiction because $\mathbb{C}$ is a connected space with respect to the topology induced by $|\cdot|_\infty$.

Let us assume that $m > 0$, and fix $z_0 \in S$. Consider the function

$$\begin{aligned} h : \mathbb{C} &\to \mathbb{C} \\ z &\mapsto z^2 - (z_0 + \overline{z}_0)z + z_0\overline{z}_0. \end{aligned}$$

Note that $h(z_0) = 0$. Moreover, h is clearly a continuous function (since it is a polynomial), thus there is a $\delta > 0$ such that, if $|z_1 - z_0|_\infty < \delta$, then $|h(z_1) - h(z_0)|_\infty < m$. We will prove that the whole open ball B with centre z_0 and radius δ is contained in S.

Fix some $z_1 \in B$. Then

$$|h(z_1)|_\infty = |h(z_1) - h(z_0)|_\infty = \varepsilon$$

for some positive number $\varepsilon < m$. Call $\xi := h(z_1)$.

For each $n \in \mathbb{N}$, consider the following polynomial of degree $2n$ with complex coefficients:

$$G(X) = (X^2 - (z_0 + \overline{z}_0)X + z_0\overline{z}_0)^n - \xi^n$$

By the definition of ξ, we have that $G(z_1) = 0$ Let us name the roots of $G(X)$ as $\beta_1 := z_1, \beta_2, \beta_3, \ldots, \beta_{2n}$ (since $\mathbb{C}$ is algebraically closed, all β_i belong to $\mathbb{C}$). Thus we have

$$G(X) = (X - z_1)\prod_{k=2}^{2n}(X - \beta_k).$$

Consider now $\overline{G}(X) = (X^2 - (z_0 + \overline{z}_0)X + z_0\overline{z}_0)^n - \overline{\xi}^n$ obtained from $G(X)$ by applying the complex conjugation to all its coefficients; note that $z_0 + \overline{z}_0$ and $z_0\overline{z}_0$ are real numbers. We have $\overline{G}(\overline{z}_1) = 0$ and $\overline{G}(\overline{\beta}_i) = 0$ for all $i = 2, \ldots, 2n$. Hence

$$\begin{aligned} G(X)\overline{G}(X) &= ((X - z_1)(X - \overline{z}_1))\prod_{k=2}^{2n}(X - \beta_k)(X - \overline{\beta}_k) \\ &= \left(X^2 - (z_1 + \overline{z}_1)X + z_1\overline{z}_1\right)\prod_{k=2}^{2n}(X^2 - (\beta_k + \overline{\beta}_k)X + \beta_k\overline{\beta}_k). \end{aligned}$$

Replacing X by α and computing the absolute value in K, we obtain

$$\begin{aligned} |G(\alpha)\overline{G}(\alpha)| &= \left|(\alpha^2 - (z_1 + \overline{z}_1)\alpha + z_1\overline{z}_1)\prod_{k=2}^{2n}(\alpha^2 - (\beta_k + \overline{\beta}_k)\alpha + \beta_k\overline{\beta}_k)\right| \\ &= |f(z_1)| \cdot \prod_{k=2}^{2n}|f(\beta_k)| \geq |f(z_1)|m^{2n-1}. \end{aligned}$$

Thus we obtain the bound

$$|G(\alpha)\overline{G}(\alpha)| \geq |f(z_1)|m^{2n-1}.$$

Going back to the definition of $G(X)$ and replacing X by α, we have that

$$|G(\alpha)| = |(\alpha^2 - (z_0 + \overline{z}_0)\alpha + z_0\overline{z}_0)^n - \xi^n| \leq |f(z_0)|^n + |\xi|^n = |f(z_0)|^n + \varepsilon^n = m^n + \varepsilon^n.$$

Similarly, $|\overline{G}(\alpha)| \leq m + \varepsilon^n$, thus

$$|G(\alpha)\overline{G}(\alpha)| \leq (m^n + \varepsilon^n)^2.$$

Combining the two inequalities, we get

$$|f(z_1)|m^{2n-1} \leq (m^n + \varepsilon^n)^2.$$

Thus

$$\left|\frac{f(z_1)}{m}\right| \leq \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)^2.$$

Letting $n \to \infty$, we obtain that $f(z_1) \leq m$. Thus $f(z_1) = m$, and $z_1 \in S$, as we wanted to prove. □

□

Now that we know what complete fields with respect to an archimedean valuation look like, we consider the fields which are complete with respect to a nonarchimedean absolute value.

Example 3.18. *Let $p > 0$ be a prime number. Then $\mathbb{Q}$ is not complete with respect to the p-adic absolute value.*

Assume first that $p > 2$ is a prime number. Let $m \in \mathbb{N}$ be such that $p \nmid m$, m is not a square in $\mathbb{Q}$, but m is a square modulo p. We will construct a sequence $(a_i)_i$ such that the limit $A = \sum_{i=0}^{\infty} a_i p^i$ in $\mathbb{Q}_p$ satisfies that $A^2 - m = 0$. Since we chose m such that m is not a square, it follows that $A \notin \mathbb{Q}$. More precisely, we construct a sequence $(a_i)_i$ such that: $a_i \in \{0, \ldots, p-1\}$ for all i, and $(\sum_{i=0}^{n} a_i p^i)^2 \equiv m \pmod{p^{n+1}}$.

We construct the sequence by induction:

- *$n = 0$: Choose $a_0 \in \{0, \ldots, p-1\}$ such that $a_0^2 \equiv m \pmod{p}$ (it exists because we chose m to be a square mod p).*
- *$n \Rightarrow n+1$: Assume we have $a_0, \ldots, a_n \in \{0, \ldots, p-1\}$ such that the sum $A_n := (\sum_{i=0}^{n} a_i p^i)$ satisfies $A_n^2 \equiv m \pmod{p^{n+1}}$. Thus the difference $A_n^2 - m$ is divisible by p^{n+1}; call d_n the integer such that $A_n^2 - m = d_n p^{n+1}$. Then define a_{n+1} as the only element in $\{0, \ldots, p-1\}$ such that $a_{n+1} \equiv -d_n(2A_{n+1})^{-1} \pmod{p}$ (Note that A_{n+1} is invertible modulo p because its square is congruent to m modulo p, and $p \nmid m$; 2 is invertible modulo p because $p > 2$).*

The relation $a_{n+1} \equiv -d_n(2A_{n+1})^{-1} \pmod{p}$ ensures that the partial sum $A_{n+1} := \sum_{i=0}^{n+1} a_i p^i$ satisfies that $A_{n+1}^2 \equiv m \pmod{p^{n+2}}$; so the sequence above satisfies our claim.

For $p = 2$, we could have done something similar with the equation $x^3 + 2x + 1 = 0$.

Example 3.19. *Let $p > 0$ be a prime number. Then $\mathbb{Q}_p$ is complete with respect to the p-adic absolute value (Exercise 2 of Sheet 10).*

Remark 3.20. *We have already seen that, if K is a field and $|\cdot|$ a nonarchimedean absolute value, then the absolute value $|\cdot|_{\widehat{K}}$ is also nonarchimedean. We can explicitly describe the corresponding valuation.*

Namely, let v be valuation on a field K, and let $\widehat{K}$ its completion with respect to the absolute value $|\cdot|$ attached to v according to Proposition 2.27, that is to say,

$$v(x) = \begin{cases} -\log|x| \text{ if } x \neq 0 \\ \infty \text{ if } x = 0. \end{cases}$$

For each nonzero class $[(a_n)_n] \in \widehat{K}$, we can choose a representative, say $(b_n)_n$, such that for all $n \in \mathbb{N}$, $b_n \neq 0$. Indeed, since $[(a_n)_n]$ is nonzero, the sequence $(a_n)_n$ does not converge to zero. Hence only finitely many terms are zero, say $a_{i_1}, \ldots, a_{i_r} = 0$. Then the sequence $(c_n)_n$ defined as

$$c_n = \begin{cases} 1 \text{ if } i = i_j \text{ for some } j = 1, \ldots, r \\ 0 \text{ otherwise} \end{cases}$$

belongs to $\mathfrak{m}$, and thus the sequence $(b_n)_n$ defined as $b_n = a_n - c_n$ for all $n \in \mathbb{N}$ satisfies the conditions above.

Let us then assume that, for all $n \in \mathbb{N}$, $a_n \neq 0$. We have that

$$\lim_{n\to\infty} v(a_n) = \lim_{n\to\infty} -\log|a_n| = -\log \lim_{n\to\infty}(|a_n|) = -\log|[(a_n)_n]|_{\widehat{K}}.$$

Therefore the valuation $\widehat{v}$ attached to $|\cdot|_{\widehat{K}}$ satisfies that

$$v([(a_n)_n]) = \lim_{n\to\infty} v(a_n). \tag{3.14}$$

Assume now that v is a discrete valuation, say $v(K^\times) = s\mathbb{Z}$ for some $s > 0$. Let $[(a_n)_n] \in \widehat{K}^\times$, where we assume that all elements $a_n \in K$ are nonzero as above. Then the sequence $(v(a_n))_n$ becomes constant from some point onwards. Namely, if we take some $\varepsilon \in (0, s)$, then there exists an $N_0 \in \mathbb{N}$ such that, for all $n, n' \geq N_0$,

$$|v(a_n) - v(a_{n'})| < \varepsilon < s.$$

Since both $v(a_n)$ and $v(a_{n'})$ belong to $s\mathbb{Z}$, we conclude that they coincide. Therefore $\widehat{v}([(a_n)_n]) = v(a_{N_0}) \in s\mathbb{Z}$.

As a consequence, we obtain that

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

In particular, the valuation $\widehat{v}$ on $\widehat{K}$ is also discrete.

One very useful property of fields which are complete with respect to a nonarchimedean absolute value is that, if a the reduction of a polynomial $f(x)$ with coefficients in the valuation ring has a root in the residue field, then this root can be "lifted" to a root of $f(x)$ in K. This is a consequence of the general result, known as Hensel's lemma. Before stating and proving it, we need some notations and definitions.

Notation 3.21. *In the rest of the section we will use the following notation:*

- *K is a field, endowed a nonarchimedean absolute value $|\cdot|$.*
- *$\mathcal{O}$ denotes the valuation ring of K, $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$, and $\kappa = \mathcal{O}/\mathfrak{m}$ is the residue field.*

Lemma 3.22. *Let K be a local field and v a valuation on K. Let $(a_n)_n$ be a sequence of elements of K that converges to a with respect to v. Assume that there exist $B > 0$, $N_0 \in \mathbb{N}$ such that, for all $n \geq N_0$, $v(a_n) \geq B$. Then $v(a) \geq B$.*

Proof. Since the sequence $a - a_n$ converges to zero, we know that there exists $N_1 \in \mathbb{N}$ such that, for all $n \geq N_1$, $v(a - a_n) \geq B + 1$. Hence if we choose $n > \max\{N_0, N_1\}$, we have that $v(a) \geq \min\{v(a - a_n), v(a_n)\} \geq \min\{B + 1, B\} = B$. □

Corollary 3.23. *Let K be a local field and v a valuation on K, $\pi \in K$ with $v(\pi) > 0$. Let $(a_n)_n$ be a sequence of elements of $\mathcal{O}$ that converges to a with respect to v. Assume that there exist $m \in \mathbb{N}$, $N_0 \in \mathbb{N}$ such that, for all $n \geq N_0$, $a_n \in (\pi^m)$. Then $a \in (\pi^m)$.*

Proof. Let $M = v(\pi^m)$. Then for any $b \in \mathcal{O}$, the condition $b \in (\pi^m)$ is equivalent to the condition $v(b) \geq M$. Indeed, $b \in (\pi^m)$ if and only if there exists $c \in \mathcal{O}$ with $b = c\pi^m$, which holds if and only if the element $b\pi^{-m}$ belongs to $\mathcal{O}$. This condition is equivalent to $v(b\pi^{-m}) \geq 0$, or, equivalently, $v(b) \geq v(\pi^m) = M$. The corollary then follows rewriting the lemma in terms of this condition. □

Remark 3.24. *Assume the setting in Notation 3.21. In what follows, we will often consider polynomials $f(x) \in \mathcal{O}[x]$, and reduce them modulo an ideal $\mathfrak{a}$ of $\mathcal{O}$. Formally, there are two ways to define the process of reduction mod $\mathfrak{a}$.*

- *We can consider the ideal $\mathfrak{A}$ generated by $\mathfrak{a}$ in the ring $\mathcal{O}[x]$, namely, the smallest ideal of $\mathcal{O}[x]$ containing the all elements in $\mathfrak{a}$. Then, by abuse of notation, we will say that two polynomials $f(x), g(x) \in \mathcal{O}[x]$ are congruent modulo $\mathfrak{a}$ if*

$$f(x) \equiv g(x) \pmod{\mathfrak{A}}.$$

- *On the other hand, given two polynomials $f(x), g(x) \in \mathcal{O}[x]$, we can say that they are congruent modulo $\mathfrak{a}$ if all the coefficients of $f(x) - g(x)$ lie in $\mathfrak{a}$.*

These two definitions are equivalent. Indeed, note first that

$$\mathfrak{A} = \{\sum_{i=1}^{r} a_i h_i(x) \text{ for some } r \in \mathbb{N}, \text{ and for some } h_i(x) \in \mathcal{O}[x], a_i \in \mathfrak{a}; i \in \{0, \dots, r\}\} =$$
$$= \{\sum_{i=1}^{s} b_i x^i \text{ for some } s \in \mathbb{N}, \text{ and for some } b_i \in \mathfrak{a}; i \in \{0, \dots, s\}\};$$

in other words, we can write all the elements of $\mathfrak{A}$ as a polynomial with coefficients in $\mathfrak{a}$.

Let $f(x), g(x) \in \mathcal{O}[x]$. Then

$$\begin{aligned} f(x) \equiv g(x) \pmod{\mathfrak{A}} &\Leftrightarrow f(x) - g(x) \in \mathfrak{A} \\ &\Leftrightarrow \exists s \in \mathbb{N}, b_i \in \mathfrak{a} : f(x) - g(x) = \sum_{i=1}^{s} b_i x^i \\ &\Leftrightarrow \textit{ all coefficients of } f(x) - g(x) \textit{ lie in } \mathfrak{a}. \end{aligned}$$

In particular, we can consider the case where $\mathfrak{a} = (\pi^n)$ for some element π with valuation $v(\pi) > 0$. Then for every element $a \in \mathcal{O}$, $a \in (\pi^n)$ if and only if $v(a) \geq nv(\pi)$. Thus $f(x)$ is congruent to $g(x) \pmod{(\pi^n)}$ if and only if all the coefficients of $f(x) - g(x)$ have valuation greater than or equal to $nv(\pi)$.

Definition 3.25. *A polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{O}[x]$ is called* primitive *if $f(x) \not\equiv 0 \pmod{\mathfrak{m}}$, that is to say, if*

$$\max\{|a_0|, |a_1|, \ldots, |a_n|\} = 1.$$

Lemma 3.26 (Hensel's Lemma)**.** *Let K be complete with respect to a nonarchimedean absolute value $|\cdot|$. Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial whose reduction mod $\mathfrak{m}$ admits a factorisation*

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

for some $\overline{g}(x), \overline{h}(x) \in \kappa[x]$ which are coprime.

Then there exist $g(x), h(x) \in \mathcal{O}[x]$ with $\deg(g) = \deg(\overline{g})$ such that

$$\begin{cases} g(x) \equiv \overline{g}(x) \pmod{\mathfrak{m}} \\ h(x) \equiv \overline{h}(x) \pmod{\mathfrak{m}} \end{cases}$$

and

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

An immediate application of this result concerns the lifting of roots of a polynomial:

Corollary 3.27. *Let K be complete with respect to a nonarchimedean absolute value $|\cdot|$. Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial, let $\overline{\alpha}$ in k such that*

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

Assume that $\overline{\alpha}$ is not a root of the reduction of the formal derivative of $f(x)$.

Then there exists $\alpha \in \mathcal{O}$ with $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{m}}$ and $f(\alpha) = 0$.

Proof of the Corollary. Since $\overline{f}(\overline{\alpha}) = 0$, we have that $x - \overline{\alpha}$ divides $\overline{f}(x)$. Let $\overline{f}_0(x)$ be such that

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

Take $\overline{g}(x) = x - \overline{\alpha}$, $\overline{h}(x) = \overline{f}_0(x)$. The condition on the reduction of the derivative of $f(x)$ ensures that $\overline{g}(x), \overline{h}(x)$ are coprime. Now we can apply Hensel's Lemma and obtain a polynomial of degree 1, $g(x) = ax - b$ for some $a, b \in K$ with $a \equiv 1 \pmod{\mathfrak{m}}$, $b \equiv \overline{\alpha} \pmod{\mathfrak{m}}$, and $f(x) = (ax - b)h(x)$ for some $h(x) \in \mathcal{O}[x]$. Since $a \equiv 1 \pmod{\mathfrak{m}}$, we have that $a \in \mathcal{O}^\times$, thus we can write

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

Take $\alpha = b/a$; clearly $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{m}}$ and $f(\alpha) = 0$. □

Proof of Hensel's Lemma. Let us denote by $d_f = \deg_K f$ and $d_{\overline{g}} = \deg_\kappa \overline{g}$. Choose polynomials $g_0(x), h_0(x) \in \mathcal{O}[x]$ such that

$$\begin{cases} g_0(x) \equiv \overline{g}(x) \pmod{\mathfrak{m}} & \text{and } \deg_K g_0 = d_{\overline{g}} \\ h_0(x) \equiv \overline{h}(x) \pmod{\mathfrak{m}} & \text{and } \deg_K h_0 \leq d_f - d_{\overline{g}}. \end{cases}$$

Moreover we choose $a(x), b(x) \in \mathcal{O}[x]$ such that

$$a(x)g_0(x) + b(x)h_0(x) \equiv 1 \pmod{\mathfrak{m}}.$$

Note that we can make this choice because the greatest common divisor of $\overline{g}(x), \overline{h}(x) \in \kappa[x]$ is 1.

Once we make all these choices, we can consider the minimum of the valuations of the coefficients of the polynomials $f(x) - g_0(x)h_0(x)$ and $a(x)g_0(x) + b(x)h_0(x) - 1$ (which is necessarily positive). Let us pick some $\pi \in K$ such that $v(\pi)$ equals this minimum (for instance, we can take π to be one of the coefficients where the minimum is achieved).

Note that, with this choice of π, we have the following congruences modulo (π):

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

and not just modulo $\mathfrak{m}$. This will play an important role later in the proof.

Our aim is to construct, for each $n \in \mathbb{N}_{\geq 0}$, polynomials $g_n(x), h_n(x) \in \mathcal{O}[x]$ satisfying

$$\begin{cases} (1)\, \deg_K g_n = d_{\overline{g}} \text{ and } \deg_K h_n \leq d_f - d_{\overline{g}}. \\ (2) \begin{cases} g_n(x) \equiv g_{n-1}(x),\ h_n(x) \equiv h_{n-1}(x) \pmod{(\pi^n)} \text{ for } n \geq 1, \\ g_0(x) \equiv \overline{g}(x), h_0(x) \equiv \overline{h}(x) \pmod{\mathfrak{m}} \end{cases} \\ (3) f(x) - g_n(x)h_n(x) \equiv 0 \pmod{(\pi^{n+1})} \end{cases} \tag{3.15}$$

Assume we have such a sequence. Then, if we write $g_n(x) = c_{d_{\overline{g}}}^{(n)} x^{d_{\overline{g}}} + \cdots + c_1^{(n)} x + c_0^{(n)}$, then for each $i = 0, \ldots, d_{\overline{g}}$, the sequence $(c_i^{(n)})_n$ is a Cauchy sequence, and hence converges in K. Call

$$c_i := \lim_{n \to \infty} c_i^{(n)} \in K.$$

For all $n \in \mathbb{N}$, $c_i^{(n)} \in \mathcal{O}$, that is to say, $v(c_i^{(n)}) \geq 0$. Hence

$$v(c_i) = \lim_{n \to \infty} v(c_i^{(n)}) \geq 0,$$

that is to say, $c_i \in \mathcal{O}$.

Define

$$g(x) := c_{d_{\overline{g}}} x^{d_{\overline{g}}} + \cdots + c_1 x + c_0.$$

It clearly satisfies that $g(x) \in \mathcal{O}[x]$ and $\deg_K g \leq d_{\overline{g}}$ (it will be an equality if $c_{d_{\overline{g}}} \neq 0$). Moreover $g(x) \equiv \overline{g}(x) \pmod{\mathfrak{m}}$. Indeed, there exists some N such that, for all $i \geq N$, $g(x) - g_i(x) \equiv 0 \pmod{\pi}$. Thus

$$g(x) - g_0(x) = g(x) - g_N(x) + g_N(x) - g_{N-1}(X) + g_{N-1}(X) - \cdots - g_1(x) + g_1(x) - g_0(x);$$

the first difference $g(x) - g_N(x) \in (\pi)$, and for each n, $g_n(x) - g_{n-1}(x) \in (\pi^n) \subseteq (\pi)$. Now it suffices to recall that $g_0(x) \pmod{\mathfrak{m}} \equiv \overline{g}(x)$.

The equality $g(x) \equiv \overline{g}(x) \pmod{\mathfrak{m}}$ implies that the leading coefficient $c_{d_{\overline{g}}} \pmod{\mathfrak{m}}$ equals the leading coefficient of $\overline{g}(x)$, which is nonzero because the degree of $\overline{g}(x)$ is $d_{\overline{g}}$. Thus $\deg_K g = d_{\overline{g}}$.

Analogously one defines $h(x) \in \mathcal{O}[x]$ such that $\deg_K(h) \leq d_f - d_{\overline{g}}$ and $h(x) \equiv \overline{h}(x) \pmod{\mathfrak{m}}$.

Moreover $f(x) - g(x)h(x) \in (\pi^n)$ for all $n \in \mathbb{N}$. Since $v(\pi) > 0$, for any given constant M, there exists some $n \in \mathbb{N}$ such that $v(\pi)n > M$, and thus all the coefficients of $f(x) - g(x)h(x)$ have valuation greater M. In other words, the valuation of the coefficients of $f(x) - g(x)h(x)$ is ∞, that is, $f(x) = g(x)h(x)$.

Therefore the proof boils down to constructing sequences of polynomials $(g_n(x))_n$, $(h_n(x))_n$ satisfying (3.15).

- $n = 0$: $g_0(x), h_0(x)$ already satisfy (3.15). Note that here we are using $f(x) - g_0(x)h_0(x) \equiv 0 \pmod{(\pi)}$ and not just $\pmod{\mathfrak{m}}$.
- $n \to n+1$: We will define $g_{n+1}(x) = g_n(x) + \pi^{n+1}p_n(x)$, $h_{n+1}(x) = h_n(x) + \pi^{n+1}q_n(x)$ for some polynomials $p_n(x), q_n(x) \in \mathcal{O}[x]$, so that the second condition of (3.15) will be trivially satisfied.

  The third condition of (3.15) reads

  $$f(x) - g_{n+1}(x)h_{n+1}(x) \equiv 0 \pmod{(\pi^{n+2})}.$$

  We know that

  $$f(x) - g_n(x)h_n(x) \equiv 0 \pmod{(\pi^{n+1})},$$

  say $f(x) - g_n(x)h_n(x) = \pi^{n+1}A_n(x)$ for some $A_n(x) \in \mathcal{O}[x]$. Note that $\deg_K A_n \leq d_f$.

  We obtain

  $$\begin{aligned} f(x) - g_{n+1}(x)h_{n+1}(x) &= f(x) - (g_n(x) + \pi^{n+1}p_n(x))(h_n(x) + \pi^{n+1}q_n(x)) = \\ &f(x) - h_n(x)g_n(x) - \pi^{n+1}(g_n(x)q_n(x) + p_n(x)h_n(x) + \pi^{2(n+1)}p_n(x)q_n(x) = \\ &\pi^{n+1}(A_n(x) - (g_n(x)q_n(x) + p_n(x)h_n(x))) + \pi^{2(n+1)}p_n(x)q_n(x). \end{aligned}$$

  Therefore

  $$f(x) - g_{n+1}(x)h_{n+1}(x) \equiv \pi^{n+1}(A_n(x) - (g_n(x)q_n(x) + p_n(x)h_n(x))) \pmod{(\pi^{n+2})},$$

  and condition 3 of (3.15) is equivalent to

  $$A_n(x) - (g_n(x)q_n(x) + p_n(x)h_n(x)) \equiv 0 \pmod{(\pi)}. \tag{3.16}$$

  The second condition of (3.15) implies that $g_n(x) \equiv g_0(x)$, $h_n(x) \equiv h_0(x) \pmod{(\pi)}$. Therefore Equation (3.16) reads

  $$A_n(x) \equiv g_0(x)q_n(x) + p_n(x)h_0(x) \pmod{(\pi)}. \tag{3.17}$$

Recall now that we had polynomials $a(x), b(x) \in \mathcal{O}[x]$ such that $a(x)g_0(x) + b(x)h_0(x) \equiv 1 \pmod{(\pi)}$. Therefore the polynomials $q_n^*(x) = A_n(x)a(x)$ and $p_n^*(x) = A_n(x)b(x)$ satisfy the desired congruence, namely

$$\begin{aligned} A_n(x) &\equiv A_n(x)(a(x)g_0(x) + b(x)h_0(x)) \pmod{(\pi)} \\ &\equiv g_0(x)(A_n(x)a(x)) + h_0(x)(A_n(x)b(x)) \pmod{(\pi)} \\ &\equiv g_0(x)q_n^*(x) + h_0(x)p_n^*(x) \pmod{(\pi)} \end{aligned} \tag{3.18}$$

Note that here, again, we make use of the fact that $a(x)g_0(x) + b(x)h_0(x) \equiv 1 \bmod (\pi)$ and not just mod $\mathfrak{m}$.

But, with this choice, $g_{n+1}^*(x) = g_n(x) + \pi^{n+1}p^*(x)$ and $h_{n+1}^*(x) = h_n(x) + \pi^{n+1}q^*(x)$ may fail to satisfy the first condition of (3.15), namely, that $\deg_K g_{n+1}^* = d_{\overline{g}}$ and $\deg_K h_{n+1}^* \leq d_f - d_{\overline{g}}$.

To overcome this problem, we divide $p_n^*(x)$ by $g_0(x)$ (whose degree coincides with $d_{\overline{g}}$), and obtain

$$p_n^*(x) = g_0(x)Q_n(x) + r_n(x),$$

where $Q_n(x) \in K[x]$ and $r_n(x) \in K[x]$ has degree smaller than $d_{\overline{g}}$. We wanted polynomials with coefficients in $\mathcal{O}[x]$. But note that, since $g_0(x) \equiv \overline{g}(x) \pmod{\mathfrak{m}}$ and both have the same degree, then the leading coefficient of $g_0(x)$ must be a unit. Therefore the division actually yields polynomials with coefficients in $\mathcal{O}$.

Replacing $p_n^*(x)$ in Equation (3.18) by the expression obtained in the division, we obtain

$$\begin{aligned} A_n(x) \equiv g_0(x)q_n^*(x) + h_0(x)(g_0(x)Q_n(x) + r_n(x)) \equiv \\ g_0(x)(A_n(x)a(x) + h_0(x)Q_n(x)) + h_0 r_n(x) \pmod{(\pi)}. \end{aligned} \tag{3.19}$$

Set

$$\begin{cases} p_n(x) := r_n(x) \\ q_n(x) := \text{ Sum of all terms of } A_n(x)a(x) + h_0(x)Q_n(x) \text{ which do not belong to } (\pi). \end{cases}$$

Note that $q_n(x) \equiv A_n(x)a(x) + h_0(x)Q_n(x) \pmod{(\pi)}$. We remove the coefficients divisible by π to ensure that $\deg_K q_n$ equals the degree of the reduction of $q_n(x) \pmod{(\pi)}$. With these values of $p_n(x)$ and $q_n(x)$, condition 2 of (3.15) is trivially satisfied and condition 3 is satisfied because Equation (3.19) ensures that the congruence (3.17).

Let us look at the different degrees that appear in the expression. We know that $\deg_K p_n < d_{\overline{g}}$, thus $g_{n+1}(x) = g_n(x) + \pi^{n+1}p_n(x)$ has degree exactly $d_{\overline{g}}$.

On the left hand side of Equation (3.19), we have the polynomial $A_n(x) \pmod{(\pi)}$, which has degree $\deg_\kappa(A_n \pmod{(\pi)}) \leq d_f$ and, on the right hand side, we know that $\deg_\kappa(h_0 r_n \pmod{(\pi)}) < d_f - d_{\overline{g}} + d_{\overline{g}} = d_f$. Thus $\deg_\kappa(g_0(A_n a + h_0 Q_n)) \pmod{\pi}) \leq d_f$, and since $\deg_\kappa(g_0 \pmod{(\pi)}) = d_{\overline{g}}$, we conclude that $\deg_K q_n(x) = \deg_\kappa(q_n \pmod{\pi}) = \deg_\kappa(A_n a + h_0 Q_n \pmod{(\pi)}) \leq d_f - d_{\overline{g}}$. Therefore $\deg_K h_{n+1} = \deg_K(h_n + \pi^{n+1}q_n)$ is less than or equal to $d_f - d_{\overline{g}}$.

□

Remark 3.28. *Note that, in the proof of Lemma 3.26, π is not a prime element of K; actually the valuation on K need not be discrete, so the notion of "prime element of K" may not even make sense. Nevertheless, this π plays the role of a prime element, in the sense that, in the proof, only the valuation of finitely many elements of K will be involved, and, of those, $v(\pi)$ is minimum positive value.*

Our next aim is to prove that valuations behave "well" with respect to finite separable extensions. We start with a lemma, which, in turn, is an application of Hensel's Lemma.

Lemma 3.29. *Let K be a complete field with respect to a nonarchimedean absolute value $|\cdot|$. Let*

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

be an irreducible polynomial with $n > 1$ and such that $a_0 \in \mathcal{O}$. Then all coefficients $a_{n-1}, \ldots, a_1$ belong to $\mathcal{O}$.

Proof. Set $a_n := 1$, and let

$$s = \max\{|a_i| : i = 0, \ldots, n\};$$

say $|a_{i_0}| = s$. If we define $b_i = a_i \cdot a_{i_0}^{-1}$, then $|b_i| \leq 1$, and moreover $|b_{i_0}| = 1$. Call $f_0(x) = a_{i_0}^{-1} f(x)$. Let us further define

$$r = \min\{i : |b_i| = 1\}.$$

We can consider this minimum because the set $\{i : |b_i| = 1\}$ is not empty. Then

$$f_0(x) \equiv x^r(b_r + \cdots + b_n x^{r-n}) \pmod{\mathfrak{m}}.$$

We have a factorisation of the reduction of $g(x)$ modulo $\mathfrak{m}$, and we are in the conditions to apply Hensel's Lemma. Thus we can lift this factorisation; there exist $g(x), h(x) \in \mathcal{O}[x]$ with

$$f_0(x) = g(x)h(x),$$

where $\deg_K g = r$. Since $f(x)$ is by hypothesis irreducible, this cannot be a factorisation in $K[x]$; thus either $\deg_K g = 0$ or $\deg_K g = n$.

- $\deg_K g = 0$: Then $\min\{i : |b_i| = 1\} = 0$. In particular, $|b_0| = 1$, that is to say, $|a_0| = |a_{i_0}| = \max\{|a_i| : i = 0, \ldots, n\}$. But $|a_0| \leq 1$ because, by hypothesis, $a_0 \in \mathcal{O}$. Hence, for all $i = 0, \ldots, n-1$, $|a_i| \leq 1$.

- $\deg_K g = n$: Then $\min\{i : |b_i| = 1\} = n$. Then $|b_n| = 1$; that is to say, $|a_{i_0}| = 1$. Thus for all $i = 1, \ldots, n-1$, $|a_i| \leq 1$.

□

In the following remark recall some notions from Chapter 2 of [1].

Remark 3.30. *1. Let L/K be an extension of fields of degree $n < \infty$. Then L has a natural K-vector space structure (for all $a \in K$, for all $\alpha \in L$, $a \cdot \alpha$ is defined as the product of a and α inside L). The dimension of L as a K-vector space coincides with n. For each α in L, we can consider the map*

$$\begin{aligned} T_\alpha : L &\to L \\ \beta &\mapsto \alpha\beta. \end{aligned}$$

Since it is a morphism of K-vector spaces, it can be represented by a $n \times n$ matrix T_α with entries in K with respect to some prefixed K-basis of L. Then we define the norm *of α in the extension L/K as*

$$\mathrm{Norm}_{L/K}(\alpha) := \det T_\alpha.$$

When L/K is separable, we have an equivalent definition of $\mathrm{Norm}_{L/K}(\alpha)$. Namely, fix an algebraic closure $\overline{K}/K$ containing L. Let

$$\mathcal{S} := \{\sigma : L \to \overline{K} \text{ ring morphism such that } \sigma|_K = \mathrm{id}_K\}.$$

Then it holds that

$$\mathrm{Norm}_{L/K}(\alpha) = \prod_{\sigma \in \mathcal{S}} \sigma(\alpha).$$

The norm of α is related to the product of the roots of the minimal polynomial of α over K. Namely, let $\alpha = \alpha_1, \ldots, \alpha_r$ be the roots of the minimal polynomial of α over K, and let $e = [L : K(\alpha)]$. Then $n = er$, and

$$\mathrm{Norm}_{L/K}(\alpha) = \left(\prod_{i=1}^{r} \alpha_i \right)^e. \tag{3.20}$$

2. *Let L/K be a field extension, $A \subset K$ a subring. Then the* integral closure of A in L *is defined as the ring B consisting of the elements of L that are integral over A; in other words,*

$$B = \{\alpha \in L : \exists n \in \mathbb{N}, \exists a_0, \ldots, a_{n-1} \in A \text{ such that } \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0\}.$$

Theorem 3.31. *Let K be a complete field with respect to a nonarchimedean absolute value $|\cdot|_K$. Let L/K be a finite separable extension of degree n. Then there is a unique extension of $|\cdot|_K$ to an absolute value on L, which can be defined as follows: for all $\alpha \in L$,*

$$|\alpha|_L := \sqrt[n]{|\mathrm{Norm}_{L/K}(\alpha)|_K}. \tag{3.21}$$

Moreover the valuation ring of $|\cdot|_L$ is the integral closure in L of the valuation ring of $|\cdot|_K$.

Proof. • First of all, we will prove that the map

$$\begin{aligned} |\cdot|_L : L &\to \mathbb{R}_{\geq 0} \\ \alpha &\mapsto \sqrt[n]{|\mathrm{Norm}_{L/K}(\alpha)|_K} \end{aligned}$$

is a nonarchimedean absolute value on L. We have to check three conditions, namely:

1. For all $\alpha \in L$, $|\alpha|_L = 0$ if and only if $\alpha = 0$.
2. For all $\alpha, \beta \in L$, $|\alpha \cdot \beta|_L = |\alpha|_L \cdot |\beta|_L$.
3. For all $\alpha, \beta \in L$, $|\alpha + \beta|_L \leq \max\{|\alpha|_L, |\beta|_L\}$.

The first two conditions are clear by the definition of $|\cdot|_L$. To see the third condition, let us take $\alpha, \beta \in L$. We can assume, without loss of generality, that they are both different from zero. Let us assume that $|\alpha|_L \geq |\beta|_L$ (otherwise, we interchange α and β). Then the condition $|\alpha + \beta|_L \leq \max\{|\alpha|_L, |\beta|_L\}$ is equivalent to $|1 + \beta/\alpha|_L \leq 1$. We will see that, for all $\beta \in L$ satisfying that $|\beta|_L \leq 1$, then $|\beta + 1|_L \leq 1$.

This will follow from the more general fact:

Fact 3.32. *Let $\mathcal{O}_K$ be the valuation ring of $|\cdot|_K$, and let A the integral closure of $\mathcal{O}_K$ in L. Then*

$$A = \{\alpha \in L : |\alpha|_L \leq 1\}.$$

Proof of Fact. First of all, note that, for all $\alpha \in L$,

$$|\alpha|_L \leq 1 \Leftrightarrow \sqrt[n]{|\mathrm{Norm}_{L/K}(\alpha)|_K} \leq 1 \Leftrightarrow |\mathrm{Norm}_{L/K}(\alpha)|_K \leq 1 \Leftrightarrow \mathrm{Norm}_{L/K}(\alpha) \in \mathcal{O}_K.$$

Thus we have to prove

$$A = \{\alpha \in L : \mathrm{Norm}_{L/K}(\alpha) \in \mathcal{O}_K\}.$$

Take $\alpha \in L$ be integral over $\mathcal{O}_K$. If we fix a separable closure $\overline{K}$ of K, then all the conjugates $\sigma(\alpha)$ of α in K are also integral over $\mathcal{O}_K$. Therefore $\mathrm{Norm}_{L/K}(\alpha)$ is integral over $\mathcal{O}_K$. But, on the other hand, it is also an element of K. Since $\mathcal{O}_K$ is integrally closed (cf. Proposition 2.34) we obtain $\mathrm{Norm}_{L/K}(\alpha) \in \mathcal{O}_K$.

Reciprocally, let $\alpha \in L$ be such that $\mathrm{Norm}_{L/K}(\alpha) \in \mathcal{O}_K$. Consider the minimal polynomial $f(x) \in K[x]$ of α over K, say

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

This polynomial is irreducible, and $\mathrm{Norm}_{L/K}(\alpha) = \pm a_0^m$ for some positive integer m (this follows from Equation (3.20)). From the condition $\mathrm{Norm}_{L/K}(\alpha) \in \mathcal{O}_K$ it follows that $a_0 \in \mathcal{O}_K$. We can apply Lemma 3.29 to conclude that all coefficients of $f(x)$ belong to $\mathcal{O}_K$, thus α is integral over $\mathcal{O}_K$. □

Now it is easy to show that $|\cdot|_L$ satisfies the strong triangle inequality. Namely, denote by $\mathcal{O}_L = \{\alpha \in L : |\alpha|_L \leq 1\}$ and let $\beta \in \mathcal{O}_L$. Since $\mathcal{O}_L$ is a ring (because it is the integral closure of $\mathcal{O}_K$ in L), we conclude that $\beta + 1$ also belongs to $\mathcal{O}_L$, that is to say, $|\beta + 1|_L \leq 1$. Thus Equation (3.21) defines a nonarchimedean absolute value on L. Note that, by the Fact above, the valuation ring of $|\cdot|_L$ is the integral closure $\mathcal{O}_L$ of $\mathcal{O}_K$ in L.

- Now we want to prove uniqueness of the extension of $|\cdot|_K$ to L. Assume that we have some other absolute value $|\cdot|'$ on L such that, for all $a \in K$, $|a|' = |a|_L$.

Fact 3.33. *For all $\beta \in L$, $|\beta|_L \leq 1$ implies that $|\beta|' \leq 1$.*

Proof of Fact. Let $\beta \in L$ with $|\beta|_L \leq 1$, and let

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

the minimal polynomial of β over K. Like in the proof of Fact 3.32, we have that all coefficients $a_{d-1}, \ldots, a_0 \in \mathcal{O}_K$. Assume $|\beta|' > 1$. Then

$$\begin{aligned} 1 = |1|' = |-a_{d-1}\beta^{-1} - a_{d-2}\beta^{-2} \cdots - a_1\beta^{-(d-1)} - a_0\beta^{-d}|' \leq \\ \max\{|a_{d-1}|_K(|\beta|')^{-1}, |a_2|_K(|\beta|')^{-2}, \ldots, |a_1|_K(|\beta|')^{-(d-1)}, |a_0|_K(|\beta|')^{-d}\} \leq \\ \max\{(|\beta|')^{-1}, (|\beta|')^{-2}, \ldots, (|\beta|')^{-(d-1)}, (|\beta|')^{-d}\} < 1, \end{aligned}$$

where the last inequality follows from the fact that we are assuming $|\beta|' > 1$. □

Assume now that $|\cdot|'$ and $|\cdot|_L$ are not equivalent. We now distinguish two possibilities

- $|\cdot|_K$ is not the trivial absolute value. Then there exist some $a \in K$ with $|a|_K > 2$. By the Weak Approximation Theorem 2.24, there exists $\beta \in L$ with $|\beta|_L < 1$, $|\beta - a|' < 1$. In particular, $|\beta|' > 1$, and this contradicts the implication

$$|\beta|_L \leq 1 \Rightarrow |\beta|' \leq 1.$$

- $|\cdot|_K$ is the trivial absolute value. Then $|\cdot|_L$ is also the trivial absolute value, and since $|\cdot|_L$ and $|\cdot|'$ are not equivalent, then $|\cdot|'$ is not the trivial absolute value. Hence there exists some $\alpha \in L$ with $|\alpha|' > 1$. This contradicts the implication

$$|\beta|_L \leq 1 \Rightarrow |\beta|' \leq 1.$$

Thus they are equivalent and, since they coincide on K, they must actually coincide on L.

□

Proposition 3.34. *Let L/K be a field extension of finite degree, and let $|\cdot|$ be an absolute value on L. Assume that K is complete with respect to the restriction of $|\cdot|$. Then L is complete with respect to $|\cdot|$.*

The proof follows easily from the following lemma:

Lemma 3.35. *Let L/K be a field extension of finite degree n, and let $|\cdot|$ be an absolute value on L. Assume that K is complete with respect to the restriction of $|\cdot|$. Fix a basis $\{x_1, \ldots, x_n\}$ of L as a K-vector space, and define, for all $x \in L$,*

$$\|x\| := \max\{|a_i| : x = \sum_{i=1}^{n} a_i x_i\}.$$

Then there exist positive constants $C_1, C_2 \in \mathbb{R}$ such that, for all $x \in L$,

$$C_1\|x\| \leq |x| \leq C_2\|x\|.$$

Proof. Let $C_2 = \sum_{i=1}^n |x_i|$. Then, for all $x = \sum_{i=1}^n a_i x_i \in L$, we have that

$$|x| = \left|\sum_{i=1}^n a_i x_i\right| \leq \sum_{i=1}^n |a_i| \cdot |x_i| \leq \max_i\{|a_i|\} \left(\sum_{i=1}^n |x_i|\right) = \|x\| C_2.$$

To prove the existence of C_1, we will proceed by induction on the dimension n of the K-vector space L. For $n = 1$ the result is clear. Assume now we know the result whenever L is a finite extension of K of dimension $n-1$.

Let L be an extension of K of dimension n, together with a fixed basis $\{x_1, \ldots, x_n\}$. Assume that there is no constant C_1 such that, for all $x \in L$, $C_1\|x\| \leq |x|$. Namely, assume that, for all $\varepsilon > 0$ there exists some $x \in L$ with

$$\varepsilon\|x\| > |x|.$$

For each $m \in \mathbb{N}$, take $\varepsilon = \frac{1}{m}$, and let $y_m = \sum_{i=1}^n a_i^{(m)} x_i$ be such that $|y_m| < \frac{1}{m}\|y_m\|$. Clearly $\|y_m\| \neq 0$ (otherwise the inequality cannot possibly hold!). Define

$$z_m := \frac{1}{\|y_m\|} y_m. \tag{3.22}$$

The sequence $(z_m)_m$ satisfies that, for all $m \in \mathbb{N}$,

$$|z_m| < \frac{1}{m},$$

hence it converges to zero with respect to $|\cdot|$. Moreover

$$z_m = \frac{1}{\|y_m\|} y_m = \frac{1}{\max_i\{|a_i^{(m)}|\}} \left(\sum_{i=1}^n a_i^{(m)} x_i\right).$$

There is at least one $i_0 \in \{1, \ldots, n\}$ such that the equality $\max_i\{|a_i^{(m)}|\} = a_{i_0}^{(m)}$ occurs infinitely often. Thus we have an infinite subsequence of $(z_m)_m$, which by abuse of notation we call again $(z_m)_m$, satisfying that, for all $m \in \mathbb{N}$, if we write $z_m = \sum_{i=1}^n b_i^{(m)} x_i$, then

$$|b_{i_0}| = \|z_m\| = 1$$

Call $w_n = \sum_{i \neq i_0} b_i^{(m)}$. Equation (3.22) implies that the sequence $(w_n)_n$ converges to v_{i_0} in L. Hence the sequence $(w_n)_n$ is a Cauchy sequence, contained in the sub-K-vector space L' spanned by $\{x_i : i \neq i_0\}$. By the induction hypothesis, there exists C_1 such that, for all $x \in L'$, $C_1\|x\| \leq |x|$. Hence, the fact that $(w_n)_n$ is a Cauchy sequence implies that for each $i \neq i_0$, the sequence $(b_i^{(m)})_m$ is a Cauchy sequence in K. Since K is complete, it has a limit $b_i \in K$. Let $w = \sum_{i \neq i_0} b_i x^i \in L'$. We have (for a certain constant C_2, as proven above) that

$$|w_n - w| \leq C_2\|w_n - w\| = C_2 \max\{|w_i^{(n)} - w_i|\} \longrightarrow 0 \text{ as } n \to +\infty.$$

Hence (w_n) converges to w in L' and a fortiori also in L. Since $(w_n)_n$ also converges to v_{i_0} in L, and the limit of a sequence (if it exists) is unique, we have that $w = v_{i_0}$. But $w \in L'$ and $v_{i_0} \notin L'$, which is a contradiction. □

4 Local fields and number fields

In this last section we will define local fields, and explore -briefly- the relationship between number fields and local fields, and offer a glimpse of why local fields play a central role in the study of number fields.

Definition 4.1. *A field L, together with a valuation v, is called a* local field *if it satisfies the following conditions:*

- *v is a discrete valuation.*
- *L is complete with respect to the absolute value attached to v.*
- *The residue field $\mathcal{O}/\mathfrak{m}$ is finite, where as usual $\mathcal{O} = \{x \in L : v(x) \geq 0\}$ and $\mathfrak{m} = \{x \in L : v(x) > 0\}$.*

Remark 4.2. *By abuse of notation, one usually says that L is a local field without mentioning the valuation if it is clear from the context.*

Example 4.3. *1. Let $p > 0$ be a prime number. $(\mathbb{Q}_p, v_p)$ is a local field. Let us check the three conditions of the definition.*

- *$v_p(\mathbb{Q}_p^\times) = \mathbb{Z}$, hence v_p is discrete.*
- *$\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$.*
- *$\kappa = \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

2. Let $L/\mathbb{Q}_p$ be a finite extension, and let v be the valuation attached to the unique extension $|\cdot|_L$ of $|\cdot|_p$ to L (cf. Theorem 3.31). We claim that L is a local field. Let us check that the conditions in the definition hold. Call $n = [L : \mathbb{Q}_p]$. Let $\alpha \in L^\times$. Then

$$|\alpha|_L = \sqrt[n]{|\mathrm{Norm}_{L/\mathbb{Q}_p}(\alpha)|_p} = \sqrt[n]{p^{-v_p(\mathrm{Norm}_{L/\mathbb{Q}_p}(\alpha))}} = p^{-\frac{1}{n}v_p(\mathrm{Norm}_{L/\mathbb{Q}_p}(\alpha))}.$$

If we choose the constant $p > 1$ to define the valuation v_L attached to $|\cdot|_L$, we obtain that

$$v_L(\alpha) = \frac{1}{n}v_p(\mathrm{Norm}_{L/\mathbb{Q}_p}(\alpha)).$$

Note that if $\alpha \in \mathbb{Q}_p$, then

$$\mathrm{Norm}_{L/\mathbb{Q}_p}(\alpha) = \prod_{\sigma: L \hookrightarrow \overline{\mathbb{Q}}_p} \sigma(\alpha) = \prod_{\sigma: L \hookrightarrow \overline{\mathbb{Q}}_p} \alpha = \alpha^n,$$

thus

$$v(\alpha) = \frac{1}{n}v_p(\mathrm{Norm}_{L/\mathbb{Q}_p}(\alpha)) = \frac{1}{n}v_p(\alpha^n) = v_p(\alpha).$$

Hence $v_L|_{\mathbb{Q}_p}$ coincides with v_p.

- *For all $\alpha \in L^\times$, we have that $v_L(\alpha) \subseteq \frac{1}{n}\mathbb{Z}$. Therefore there exists $d|n$ such that*

$$v_L(L^\times) \subseteq \frac{1}{d}\mathbb{Z},$$

hence v_L is a discrete valuation.

- *L is complete with respect to v (cf. Proposition 3.34).*

- *Define a map*

$$\varphi : \mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \longrightarrow \kappa = \mathcal{O}_L/\mathfrak{m}_L$$
$$a + p\mathbb{Z}_p \mapsto a + \mathfrak{m}_L.$$

φ is a well-defined ring morphism, which is injective. Via φ we have an inclusion $\mathbb{F}_p \hookrightarrow \kappa$. To prove that κ is finite, it suffices to see that $[\kappa : \mathbb{F}_p]$ is finite. Actually, we will show that $[\kappa : \mathbb{F}_p] \leq [L : \mathbb{Q}_p]$.

Let $x_1 + \mathfrak{m}_L, \dots, x_{n+1} + \mathfrak{m}_L \in \kappa$. We want to show that they are linearly dependent over $\mathbb{F}_p$. Since $[L : \mathbb{Q}_p] = n$, we have that $x_1, \dots, x_{n+1}$ are not linearly independent over $\mathbb{Q}_p$, so there exist $a_1, \dots, a_{n+1} \in \mathbb{Q}_p$, not all zero, such that

$$\sum_{i=1}^{n+1} a_i x_i = 0.$$

Let $i_0 \in \{1, \dots, n+1\}$ be such that $v_p(a_{i_0}) \leq v_p(a_i)$ for all $i = 0, \dots, n+1$. Note that, since not all the a_i are zero, then $v(a_{i_0}) \neq +\infty$, thus $a_{i_0} \neq 0$. Let $b_i = \frac{a_i}{a_{i_0}}$. Then we have that $v_p(b_i) \geq 0$ for all $i = 1, \dots, n+1$ and $v(b_{i_0}) = 0$. Moreover

$$\sum_{i=1}^{n+1} b_i x_i = \frac{1}{a_{i_0}} \sum_{i=1}^{n+1} a_i x_i = 0.$$

Reducing this equation mod $\mathfrak{m}_L$, we obtain that

$$\sum_{i=1}^{n+1} (b_i + \mathfrak{m}_L)(x_i + \mathfrak{m}_L) = 0 + \mathfrak{m}_L$$

is a linear combination of $x_1 + \mathfrak{m}_L, \dots, x_{n+1} + \mathfrak{m}_L$ with coefficients in $\mathbb{F}_p$, and $b_{i_0} + \mathfrak{m}_L \neq 0 + \mathfrak{m}_L$. Thus $x_1 + \mathfrak{m}_L, \dots, x_{n+1} + \mathfrak{m}_L$ are linearly dependent over $\mathbb{F}_p$.

Proposition 4.4. *Let L be a field of characteristic zero endowed with a valuation v. The following are equivalent:*

(i) L, together with v, is a local field.

(ii) L is a finite field extension of $\mathbb{Q}_p$ for some prime number p and $v|_{\mathbb{Q}_p}$ is equivalent to v_p.

Proof. We have already seen $(ii) \Rightarrow (i)$. For the other implication, see Chapter II of [4], Prop. (5.2). □

Let K be a number field, i.e., a finite degree extension of $\mathbb{Q}$. Let us denote by $\mathbb{Z}_K$ be the ring of integers of K.

Proposition 4.5. *Let $I \subset \mathbb{Z}_K$ be an ideal. Then I can be written uniquely as a product*

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

for some $r \in \mathbb{N}$, $\mathfrak{p}_i$ different prime ideals for all $i = 1, \dots, r$, $e_i \in \mathbb{N}_{\geq 1}$.

Fix a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$. Proposition 4.5 allows us to define a valuation v on K in the following way: for all $a \in \mathbb{Z}_K$, write

$$(a) = \mathfrak{p}^e \cdot \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$$

and define

$$v_\mathfrak{p}(a) := e.$$

We extend this definition in the natural way to K, namely

$$v_\mathfrak{p}\left(\frac{a}{b}\right) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b).$$

In this way we obtain a map

$$\begin{aligned} \Phi : \{\text{prime ideals of } \mathbb{Z}_K\} &\to \{\text{valuations on } K\}/ \text{ equivalence of valuations} \\ \mathfrak{p} &\mapsto \text{ class of } v_\mathfrak{p}. \end{aligned}$$

Lemma 4.6. *The map Φ is a bijection.*

Proof. Let us consider the map

$$\begin{aligned} \Psi : \{\text{valuations on } K\}/ \text{ equivalence of valuations } &\to \{\text{prime ideals of } \mathbb{Z}_K\} \\ \text{class of } v &\mapsto \mathfrak{m}_v := \{\alpha \in K^\times : v(\alpha) > 0\} \cup \{0\}. \end{aligned}$$

One can check that $\mathfrak{m}_v$ is a prime ideal of $\mathbb{Z}_K$, and furthermore $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$. □

Let now consider a finite extension of number fields M/K, and fix a prime ideal $\mathfrak{p}$ in the ring of integers $\mathbb{Z}_K$ of K. We can consider the ideal $\mathfrak{p}\mathbb{Z}_M$ of $\mathbb{Z}_M$, and write its factorisation as a product of prime ideals in $\mathbb{Z}_M$, say

$$\mathfrak{p}\mathbb{Z}_M = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

The prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ induces a valuation on K, and, for all $i = 1, \dots, r$, the prime ideal $\mathfrak{P}_i$ induces a valuation on L.

Lemma 4.7. *With the notations as above, for all $i = 1, \dots, r$, the restriction of $v_{\mathfrak{P}_i}$ to K is equivalent to the valuation $v_\mathfrak{p}$.*

Proof. Fix some $i = 1, \dots, r$, and let $\alpha \in \mathbb{Z}_K$. We have the following factorisations into prime ideals:

$$\begin{cases} \alpha\mathbb{Z}_K = \mathfrak{p}^{\tilde{e}} \prod_{j=2}^{s} \mathfrak{p}_j^{\tilde{e}_j} \\ \alpha\mathbb{Z}_M = \mathfrak{P}_i^{c_i} \cdot (\text{product of some prime ideals of } \mathbb{Z}_M), \end{cases}$$

yielding $v_{\mathfrak{p}}(\alpha) = \tilde{e}$, $v_{\mathfrak{P}_i}(\alpha) = c_i$. But we also have the factorisation

$$\mathfrak{p}\mathbb{Z}_M = \prod_{h=1}^{r} \mathfrak{P}_h^{e_h}.$$

Therefore

$$\alpha\mathbb{Z}_M = \left(\mathfrak{p}^{\tilde{e}} \prod_{j=2}^{s} \mathfrak{p}_j^{\tilde{e}_j}\right) \mathbb{Z}_M = (\mathfrak{p}\mathbb{Z}_M)^{\tilde{e}} \prod_{j=2}^{s} (\mathfrak{p}_j\mathbb{Z}_M)^{\tilde{e}_j} = \left(\prod_{h=1}^{r} \mathfrak{P}_h^{e_h}\right)^{\tilde{e}} \prod_{j=2}^{s} (\mathfrak{p}_j\mathbb{Z}_M)^{\tilde{e}_j} =$$
$$\left(\prod_{h=1}^{r} \mathfrak{P}_h^{\tilde{e}e_h}\right) \prod_{j=2}^{s} (\mathfrak{p}_j\mathbb{Z}_M)^{\tilde{e}_j} = \mathfrak{P}_i^{\tilde{e}e_i} \cdot (\text{product of some prime ideals of } \mathbb{Z}_M).$$

By the uniqueness of the factorisation in prime ideals of $\mathbb{Z}_M$, we obtain that $c_i = \tilde{e}e_i$, that is to say,

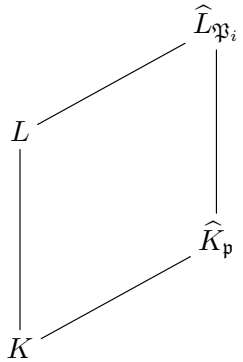
$$v_{\mathfrak{P}_i}(\alpha) = e_i v_{\mathfrak{p}}(\alpha).$$

□

Let us denote by $\widehat{L}_{\mathfrak{P}_i}$ the completion of L with respect to $v_{\mathfrak{P}_i}$, and by $\widehat{K}_{\mathfrak{p}}$ the completion of K with respect to $v_{\mathfrak{p}}$.

By Proposition 3.34, $\widehat{L}_{\mathfrak{P}_i}$ is a complete field, which contains K; thus it contains the completion of K with respect to the restriction of $v_{\mathfrak{P}_i}$ to K, that is, the completion of K with respect to $v_{\mathfrak{p}}$.

We thus have a diagram



Let us assume that L/K is a Galois extension. A fundamental question in algebraic number theory is the study of the Galois group $\mathrm{Gal}(L/K)$. The main idea in this part is that Galois groups of local fields are much simpler than Galois groups of number fields.

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_K$ and let $\mathfrak{P}$ be a prime ideal of $\mathbb{Z}_M$ dividing $\mathfrak{p}\mathbb{Z}_M$.

We have a natural map

$$\varphi : \mathrm{Gal}(\widehat{M}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}}) \to \mathrm{Gal}(M/K),$$

that maps an automorphism $\sigma \in \mathrm{Gal}(\widehat{M}_{\mathfrak{P}_i}/\widehat{K}_{\mathfrak{p}})$ to its restriction to M. It can be proved that φ is an injective group morphism, hence a description of $\mathrm{Gal}(\widehat{M}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}})$ provides information on $\mathrm{Gal}(M/K)$ concerning the primes $\mathfrak{P}$ and $\mathfrak{p}$, or, as it is usually written in the literature, "locally at the prime $\mathfrak{P}$ lying above $\mathfrak{p}$".

References

[1] *Algebraic Number Theory*, Summer Term 2014, Université du Luxembourg, lecture notes written by Sara Arias-de-Reyna and Gabor Wiese.

[2] Koblitz, Neal *p-adic numbers, p-adic analysis, and zeta-functions*. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984.

[3] Lang, Serge. *Algebraic number theory*. Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[4] Neukirch, Jürgen. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften, Vol. 322, Springer-Verlag, Berlin, 1999.

[5] Serre, Jean-Pierre. *Local fields*. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[6] *Commutative Algebra*, Winter Term 2014, Université du Luxembourg, lecture notes written by Gabor Wiese.