university of groningen

faculty of mathematics and natural sciences

Rationality of Igusa's local Zeta function

Bachelor Project Mathematics

March 2015

Student: T. Evink

First supervisor: Prof.dr. J. Top

Second supervisor: H.S.V. de Snoo

Abstract

In this thesis we discuss the rationality of Igusa's local zeta function. Some commutative algebra is treated and a construction of the field of p-adic numbers is given and some basic properties of p-adic numbers are proven. We then consider p-adic integration and define Igusa's local zeta function and relate the function to a formal power series of which the coefficients arise from the number of roots of a polynomial mod p^m. The rationality of the zeta function is then proven in some special cases and some worked examples are given.

Contents

1 Some commutative algebra

To make for smoother arguments, some commutative algebra is treated here first. Unless stated otherwise, all rings are assumed to be commutative and have a unit. I mainly followed [6] for this section.

1.1 Noetherian rings

Proposition-Definition 1.1.1. *A ring R is said to be Noetherian if it satisfies the following equivalent conditions:*

(i) Every increasing chain

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

of ideals in R eventually stabilizes, i.e. there exists $n \in \mathbb{Z}_{>0}$ such that $I_n = I_{n+1} = \cdots$.

(ii) Every non-empty collection S of ideals in R has a maximal element $J \in S$. That is if $J \subset I$ for some $I \in S$ we have $I = J$.

(iii) Every ideal of R is finitely generated.

Proof. $(i) \Rightarrow (ii)$.
Suppose for contradiction that there exists a non-empty collection of ideals S without a maximal element. Choose $I_1 \in S$ arbitrary, then I_1 is not maximal we have $I_1 \subsetneq I_2$ for some $I_2 \in S$. Similarly we have $I_2 \subsetneq I_3$ for some $I_3 \in S$ and continuing inductively we obtain a non-stabilizing chain

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

of ideals in R, contradicting our assumption.
$(ii) \Rightarrow (iii)$.
Let I be an ideal of R and let S be the collection of all finitely generated ideals contained in I. Then S is non-empty (since $0 \in I$) so it has a maximal element J. The inclusion $J \subset I$ is in fact an equality, for if we would have $J \subsetneq I$ there exists $r \in I \setminus J$ and this implies that $J \subsetneq J + (r) \subset I$, contradicting the maximality of J.
$(iii) \Rightarrow (i)$.
Let $I_1 \subset I_2 \subset \cdots$ be an increasing chain of ideals. Then $J = \bigcup_{k=1}^{\infty} I_k$ is an ideal of R and hence $J = (a_1, \ldots, a_r)$ for certain $a_1, \ldots, a_r \in R$. For $i \in \{1, \ldots, r\}$ we have $a_i \in I_{k_i}$ for some $k_i \in \mathbb{Z}_{>0}$ so that $J = I_k$ for $k = \max\{k_1, \ldots, k_r\}$. It follows that $I_k = I_{k+1} = \cdots$ and hence the proof is complete. □

For future reference we state the following lemma here.

Lemma 1.1.2. *Let R be a Noetherian integral domain and suppose that $x \in R$ is not a unit. Then $\bigcap_{n=1}^{\infty}(x^n) = 0$.*

Proof. The statement is trival when $x = 0$ so assume $x \neq 0$. Let $y \in \bigcap_{n=1}^{\infty}(x^n)$. Then there exist $r_1, r_2, \ldots \in R$ such that $y = r_n x^n$ for all $n \in \mathbb{Z}_{>0}$. For such n we have $r_n x^n = r_{n+1} x^{n+1}$ so that $r_n = r_{n+1} x$ since $x^n \neq 0$. This results in an increasing chain of ideals:

$$(r_1) \subset (r_2) \subset (r_3) \subset \cdots .$$

Since R is Noetherian the chain stabilizes so we have $r_{n+1} = a r_n$ for certain $a \in R$ and $n \in \mathbb{Z}_{>0}$ and hence

$$y = r_{n+1} x^{n+1} = a r_n x^{n+1} = axy.$$

This gives $(1 - ax)y = 0$ and since R is an integral domain and x is not a unit it follows that $y = 0$. □

The Noetherian condition is very general finiteness condition and its also easy to work with. The following theorem, known as the Hilbert basis theorem provides many examples of Noetherian rings.

Theorem 1.1.3. *If R is a Noetherian ring then so is the polynomial ring $R[X]$.*

Proof. Let I be an ideal of $R[X]$ and define the sets I_n ($n \in \mathbb{Z}_{\geq 0}$) as

$$I_n = \left\{ r \in R : r = a_n \text{ for some } f = \sum_{i=0}^{n} a_i X^i \in I \right\}.$$

Then the I_n from an increasing chain of ideals

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

and hence $I_m = I_{m+1} = \cdots$ for some $m \in \mathbb{Z}_{\geq 0}$ since R is Noetherian.
For $k \in \{0, \ldots, m\}$ we have $I_k = (a_{k1}, \ldots, a_{ki_k})$ for certain $a_{kj} \in R$. By definition of the I_n we can pick for each such a_{kj} some $f_{kj} \in I$ that has a_{kj} as leading coefficient. I claim that I is generated by the collection $\{f_{kj} : 1 \leq k \leq m, 1 \leq j \leq i_k\}$.
Let I' denote the ideal generated by the $f_{k,j}$. The inclusion $I' \subset I$ is immediate. The reverse inclusion is proven with induction on the degree of the members of I. Note that we only need to consider the non-zero members of I.
Suppose that $f \in I$ has degree 0. Then $f \neq 0$ and $f \in R$ so that $f \in I_0 = (a_{01}, \ldots a_{0i_0})$. For $j \in \{0, \ldots, i_0\}$ we have $a_{0j} = f_{0j}$ as f_{0j} as a constant polynomial equals its leading coefficient, so we have $f \in (f_{01}, \ldots, f_{0i_0}) \subset I'$ as desired.
Suppose now that for some $k \in \mathbb{Z}_{\geq 0}$ we have that I' contains all members of I of degree smaller than k and let $f \in I$ have degree k. Let a_k be the leading coefficient of f so that $a_k \in I_k$. Distinquish two cases: $k \leq m$ and $k > m$.
Assume that $k \leq m$. Then $a_k \in I_k = (a_{k1}, \ldots, a_{ki_k})$ so that $a_k = r_{k1} a_{k1} + \cdots + r_{ki_k} a_{ki_k}$ for certain $r_{kj} \in R$. Then let $g = r_{k1} f_{k1} + \cdots + r_{ki_k} f_{ki_k} \in I'$ and note that the degree of g equals k with leading coefficient equal to a_k. Thus $h := f - g$ has degree less then k so by the induction hypothesis we have $h \in I'$.

It follows that $f = g + h \in I'$ as desired.
For the remaining case, assume that $k > m$. Then $a_k \in I_k = I_m = (a_{m1}, \ldots, a_{mi_m})$ so that $a_k = r_{m1}a_{m1} + \cdots + r_{mi_m}a_{mi_m}$ for certain $r_{mj} \in R$. Then define

$$g := r_{m1}f_{m1}X^{k-m} + \cdots + r_{mi_m}f_{mi_m}X^{k-m},$$

and observe that g has degree equal to k with leading coefficient equal to a_k. Then just as in the previous case it follows that $f \in I'$ as $f - g \in I'$ by the induction hypothesis. This completes the proof. □

1.2 Local rings and localisation

Definition 1.2.1. *A ring R is called a local ring if it has a unique maximal ideal $\mathfrak{m}$. The residue field of R is defined as the field $k := R/\mathfrak{m}$.*

A local ring R with maximal ideal $\mathfrak{m}$ and residue field k is sometimes written as $(R, \mathfrak{m})$ or $(R, \mathfrak{m}, k)$ for simplicity.

Lemma 1.2.2. *A ring R is local if and only if $R \setminus R^*$ is an ideal of R.*

Proof. Suppose that R is local with maximal ideal $\mathfrak{m}$. If $a \in R \setminus R^*$ then by Zorn's lemma a is contained in a maximal ideal and hence $a \in \mathfrak{m}$. This implies that $R \setminus R^* = \mathfrak{m}$ and hence $R \setminus R^*$ is an ideal of R.
The converse follows immediately from the fact that $I \subset R \setminus R^*$ for any proper ideal I of R. □

Local rings can be constructed out of any ring R through a process called localisation. It is a generalization of the construction of the field of fractions of an integral domain: it introduces denominators from a multiplicative set making the members of this set invertible.
A subset S of a ring R is called a multiplicative set if $1 \in S$ and $s, t \in S$ implies $st \in S$.

Definition 1.2.3. *Let R be a ring and $S \subset R$ a multiplicative set. Define the localisation of R with respect to S as $S^{-1}R := (R \times S)/\sim$, where $\sim$ is the equivalence relation on $R \times S$ given by*

$$(r, s) \sim (r', s') \quad \Leftrightarrow \quad (rs' - r's)u = 0 \text{ for some } u \in S. \tag{1}$$

The equivalence class $[(r, s)] \in S^{-1}R$ is usually written as $\frac{r}{s} = [(r, s)]$.

Proposition 1.2.4. *The relation given in (1) is indeed an equivalence relation, and $S^{-1}R$ is a ring with addition and multiplication given by*

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

Furthermore, we have a ring homomorphism $\varphi : R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$ with kernel $\{r \in R : sr = 0 \text{ for some } s \in S\}$, and $\varphi(S) \subset (S^{-1}R)^*$.

Proof. We first verify that $\sim$ is an equivalence relation. Reflexivity and symmetry are immediate, to prove transitivity, suppose that $(r,s) \sim (r',s')$ and $(r',s') \sim (r'',s'')$. Then

$$(rs' - r's)u = 0 \text{ and } (r's'' - r''s')u' = 0 \text{ for certain } u, u' \in S.$$

Then

$$\begin{aligned}(rs'' - r''s)uu's' &= (rs's'' - r'ss'' + r'ss'' - r''ss')uu' \\ &= (rs' - r's)u \cdot u's'' - (r's'' - r''s')u' \cdot us = 0.\end{aligned}$$

This gives $(r,s'') \sim (r'',s)$ as required since $uu's' \in S$.
The verifications that the addition and multiplication are well defined and provide $S^{-1}R$ with the structure of a ring are completely analogous to the corresponding verification for the field of fractions of an integral domain and hence we omit it.
It is clear that φ is a ring homomorphism, for $r \in R$ we have

$$\varphi(r) = 0 \quad \Leftrightarrow \quad \frac{r}{1} = \frac{0}{1} \quad \Leftrightarrow \quad sr = 0 \text{ for some } s \in S.$$

This proves the assertion about the kernel of φ. The last statement is immediate: if $s \in S$ then the inverse of $\varphi(s) = \frac{s}{1}$ is simply given by $\frac{1}{s}$. □

Note that $S^{-1}R$ is the zero ring if and only if $0 \in S$. If $0 \in S$ we have $(r,s) \sim (r',s')$ for all $(r,s),(r',s') \in R \times S$: one can simply take $u = 0$ in (1). If $S^{-1}R$ is the zero ring then $\frac{0}{1} = \frac{1}{1}$ so that $s = 0$ for some $s \in S$.
Since the kernel of φ is non-zero in general it is, contrary to the field of fractions, not always possible to think of R as a subring of $S^{-1}R$.
When R is an integral domain and $0 \notin S$ we do have $\ker \varphi = \{0\}$ and by making the identification $r = \frac{r}{1}$ we can write $R \subset S^{-1}R$. We also have that (1) reduces to $r's = rs'$ just as in the case of the field of fractions, and one can think of $S^{-1}R$ as a subring of the field of fractions:

$$S^{-1}R = \{\frac{r}{s} \in Q(R) : s \in S\}.$$

Hence we have $R \subset S^{-1}R \subset Q(R)$ so that non-zero localisations of an integral domain produce ring extensions contained in the field of fractions.

Theorem 1.2.5. *Let R be a ring with multiplicative subset $S \subset R$. Then $S^{-1}R$ is Noetherian if R is.*

Proof. Let $J \subset S^{-1}R$ be an ideal. Let $\varphi : R \to S^{-1}R$ be the homomorphism given by $r \mapsto \frac{r}{1}$. Then the inverse image $I := \varphi^{-1}J$ is an ideal of R and hence $I = (a_1, \ldots, a_n)$ for certain $a_1, \ldots, a_n \in R$ since R is Noetherian. I claim that

$$J = \left(\frac{a_1}{1}, \ldots, \frac{a_r}{1}\right). \tag{2}$$

The inclusion $\supset$ is immediate: we have $\frac{a_i}{1} = \varphi(a_i) \in J$ for $1 \leq i \leq n$ by definition of I. Conversely, let $x = \frac{r}{s} \in J$. Multiplying with $\frac{s}{1}$ we see that $r \in I$ so that $r = r_1 a_1 + \cdots + r_n a_n$ for $r_1, \ldots, r_n \in R$. This gives

$$x = \frac{r_1 a_1 + \cdots + r_n a_n}{s} = \frac{r_1}{s} \cdot \frac{a_1}{1} + \cdots + \frac{r_n}{s} \cdot \frac{a_n}{1} \in \left(\frac{a_1}{1}, \ldots, \frac{a_r}{1} \right),$$

which proves (2) and hence $S^{-1}R$ is Noetherian. □

An important special case of localisation occurs when taking $S = R \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ in R. In this case the resulting localisation $S^{-1}R$ is usually written as $R_\mathfrak{p}$. The ring $R_\mathfrak{p}$ is called the localisation of R the the prime ideal $\mathfrak{p}$.

Theorem 1.2.6. *Let R be a ring with prime ideal $\mathfrak{p}$. Then $R_\mathfrak{p}$ is a non-zero local ring with maximal ideal given by*

$$\mathfrak{p}R_p = \left\{ \frac{r}{s} \in R_\mathfrak{p} : r \in \mathfrak{p}, s \in R \setminus \mathfrak{p} \right\}.$$

Proof. Since $0 \notin R \setminus \mathfrak{p}$ we see that $R_\mathfrak{p}$ is non-zero. To see that $R_\mathfrak{p}$ is a local ring with maximal ideal as above, note that

$$R_\mathfrak{p}^* = \left\{ \frac{r}{s} \in R_\mathfrak{p} : r, s \in R \setminus \mathfrak{p} \right\}. \tag{3}$$

To prove (3), note that the inclusion $\supset$ is immediate: the inverse of $\frac{r}{s}$ is given by $\frac{s}{r}$. For the converse, suppose that $\frac{r}{s} \in R_\mathfrak{p}^*$. We need to show that $r \in R \setminus \mathfrak{p}$. Since $\frac{r}{s}$ is a unit we see that

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} = \frac{1}{1}$$

for some $\frac{r'}{s'} \in R_\mathfrak{p}$. This means that $rr'u = ss'u$ for some $u \in R \setminus \mathfrak{p}$. Note that $rr'u \in R \setminus \mathfrak{p}$ as $s, s', u \in R \setminus \mathfrak{p}$ so that $r \in R \setminus \mathfrak{p}$ since $\mathfrak{p}$ is an ideal. This proves (3).
It is clear that $\mathfrak{p}R_\mathfrak{p}$ is an ideal of $R_\mathfrak{p}$ and the computation of the unit group shows that we have $\mathfrak{p}R_\mathfrak{p} = R_\mathfrak{p} \setminus R_\mathfrak{p}^*$ so that $R_\mathfrak{p}$ is a local ring by lemma 1.2.2. □

Example 1.2.7. *An important example is the local ring*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : b \in \mathbb{Z} \setminus p\mathbb{Z} \right\},$$

obtained by localisation of the integers $\mathbb{Z}$ at the prime ideal $(p) = p\mathbb{Z}$.

1.3 Modules and Nakayama's lemma

Modules will be treated here to an extent which is sufficient for proving Nakayama's lemma and using it in the ideal case.

Definition 1.3.1. *Let R be a ring. An R-module is an abelian group M together with a scalar multiplication $R \times M \to M$ written as $(r, m) \mapsto rm$ such that for all $m, n \in M$ and $r, s \in R$ we have*

(i) $r(m+n) = rm + rn$,

(ii) $(r+s)m = rm + sm$,

(iii) $(rs)m = r(sm)$,

(iv) $1_R m = m$.

Note that when R is a field, this is precisely the definition of a vector space. Just as for vector spaces, a subset N of an R-module M is called a submodule if it is an R-module itself under restriction of the addition and scalar multiplication. This happens precisely when $rm + sn \in N$ whenever $r, s \in R$ and $m, n \in N$. Any ring R is an R-module using the multiplication in R. Note that the R-submodules of a ring R are precisely the ideals of R.

If M and N are R-modules, an R-module homomorphism (or an R-linear map) is a group homomorphism $\varphi : M \to N$ such that $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$. It is easily verified that when M' is a submodule of M and N' is a submodule of N it holds that $\varphi(M')$ is a submodule of N and $\varphi^{-1}(N)$ is a submodule of M. An isomorphism of R-modules is a bijective R-module homomorphism. The inverse of an isomorphism is then also an R-module homomorphism.

Just as in linear algebra one can consider quotient modules. Specifically, if N is a submodule of M, the additive group M/N becomes an R-module with scalar multiplication $R \times M/N \to M/N$ given by

$$(r, m+N) \mapsto rm + N$$

This is well defined, for if $m + N = m' + N$ then $m - m' \in N$ so that $rm - rm' = r(m - m') \in N$ which gives $rm + N = rm' + N$. It is then clear that this scalar multiplication makes M/N into an R-module. The canonical map $\pi : M \to M/N$ given by $m \mapsto m + N$ is a surjective R-module homomorphism with $\ker(\pi) = N$.
The homomorphism and isomorphism theorems known for groups also hold in the context of modules. For example, an R-linear map $\varphi : M \to N$ induces an R-module isomorphism $M/\ker(\varphi) \to \operatorname{im}(\varphi)$. The proofs are completely analogous to the corresponding proofs for groups (or rings, or vector spaces).

Lemma 1.3.2. *Let M be an R-module and $\mathfrak{m} \subset R$ a maximal ideal. Then $M/\mathfrak{m}M$ is an $R/\mathfrak{m}$-vector space with scalar multiplication defined by*

$$(r \bmod \mathfrak{m}) \cdot (m \bmod \mathfrak{m}M) := rm \bmod \mathfrak{m}M.$$

As a special case $\mathfrak{m}/\mathfrak{m}^2$ is an $R/\mathfrak{m}$-vector space.

Proof. It suffices to show that the scalar multiplication is well defined for then the vector space axioms clearly hold. Suppose that $r \bmod \mathfrak{m} = r' \bmod \mathfrak{m}$ and that $m \bmod \mathfrak{m}M = m' \bmod \mathfrak{m}M$. Then $a - a' \in \mathfrak{m}$ and $m - m' \in \mathfrak{m}M$. This implies that $(a - a')m \in \mathfrak{m}M$ so that

$$am - a'm' = (a - a')m + a'(m - m') \in \mathfrak{m}M. \qquad \square$$

If M is an R-module and $m_1, \ldots, m_n \in M$ then we can consider the R-linear combinations of the m_i. We have an R-submodule of M given by

$$(m_1, \ldots, m_n) = \left\{ \sum_{i=1}^{r} r_i m_i : r_1, \ldots, r_n \in R \right\}.$$

This is the smallest submodule of M containing $m_1, \ldots, m_n$, and is called the submodule generated by the m_i. If there exist $m_1, \ldots, m_n \in M$ such that $M = (m_1, \ldots, m_n)$ we say that M is a finite R-module. When R is a ring, the finitely generated ideals are precisely the finitely generated R-submodules of R.

If M is an R-module and $I \subset R$ an ideal we define

$$IM = \left\{ \sum_{i=1}^{n} r_i m_i : r_i \in I, m_i \in M \text{ and } n \in \mathbb{Z}_{>0} \right\}.$$

This is a submodule of M. It is the smallest submodule of M that contains all elements of the form im for $i \in I$ and $m \in M$. When M is a finite R-module with generators $m_1, \ldots, m_n$ it is straightforward to verify that

$$IM = \left\{ \sum_{i=1}^{n} r_i m_i : r_1, \ldots, r_n \in I \right\}.$$

We now prove Nakayama's lemma.

Theorem 1.3.3 (Nakayama's lemma)**.** *Let $(R, \mathfrak{m})$ be a local ring and M a finite R-module. Then $\mathfrak{m}M = M$ implies $M = 0$.*

Proof. Let $n \in \mathbb{Z}_{\geq 0}$ be the minimum number of generators of M. We need to prove that $n = 0$. Assume that $n > 0$ and let $\{m_1, \ldots, m_n\}$ be a set of generators for M. The generators are non-zero by minimality of n. Since $m_n \in M = \mathfrak{m}M$ there exist $r_1, \ldots, r_n \in \mathfrak{m}$ such that

$$m_n = \sum_{i=1}^{n} r_i m_i. \tag{4}$$

Note that $1 - r_n \in R^*$ since R is local and $1 - r_n \notin \mathfrak{m}$. If $n = 1$ equation (4) reduces to $m_n = r_n m_n$ and hence

$$m_n = \frac{(1 - r_n) m_n}{1 - r_n} = 0$$

which is a contradiction. If $n > 1$ equation (4) implies that

$$0 = m_n - \sum_{i=1}^{n} r_i m_i = (1 - r_n) m_n - \sum_{i=1}^{n-1} r_i m_i.$$

From this see that $m_n = \sum_{i=1}^{n-1} \frac{r_i}{1 - r_n} m_i$ and this implies that M is generated by $\{m_1, \ldots, m_{n-1}\}$ which contradicts the minimality of n. We conclude that $n = 0$ and hence the proof is complete. $\square$

Nakayama's lemma can be used to reduce problems concerning modules to problems concerning vector spaces.

Corollary 1.3.4. *Let $(R, \mathfrak{m})$ be a local ring and M a finite R-module. If $t_1, \ldots, t_n \in M$ are such that $\overline{t_1}, \ldots, \overline{t_n} \in \overline{M} = M/\mathfrak{m}M$ span the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$ then M is generated by $t_1, \ldots, t_n$.*

Proof. let N be the submodule of M generated by the t_i. It suffices to show that $\mathfrak{m}(M/N) = M/N$ for then Nakayama's lemma implies that $M/N = 0$, i.e. $M = N$ (note that M/N is finite since M is finite).
The inclusion $\mathfrak{m}(M/N) \subset M/N$ is immediate since M/N is an R-module. For the converse, let $x \bmod N \in M/N$ be arbitary. Then there exist $\alpha_1, \ldots, \alpha_n \in R$ such that

$$x \bmod \mathfrak{m}M = \alpha_1 t_1 + \cdots + \alpha_n t_n \bmod \mathfrak{m}M,$$

and this implies that there exist $r_1, \ldots, r_k \in \mathfrak{m}$ and $m_1, \ldots, m_k \in M$ such that

$$x = \alpha_1 t_1 + \cdots + \alpha_n t_n + r_1 m_1 + \cdots + r_k m_k.$$

It follows that

$$x \bmod N = r_1(m_1 \bmod N) + \cdots + r_k(m_k \bmod N) \in \mathfrak{m}(M/N),$$

and hence $\mathfrak{m}(M/N) = M/N$ as desired. This completes the proof. □

1.4 Discrete valuation rings

Definition 1.4.1. *A discrete valuation on a field K is a surjective map $v : K^* \to \mathbb{Z}$ such that for $x, y \in K^*$ we have*

(i) $v(xy) = v(x) + v(y)$.

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$ *if* $x + y \neq 0$.

Note that surjectivity of v follows from the existence of an element $t \in K^*$ such that $v(t) = 1$ since then $v(t^n) = n$ for $n \in \mathbb{Z}$.

Proposition-Definition 1.4.2. *An integral domain R with field of fractions K is called a discrete valuation ring (DVR) if it satisfies the following equivalent conditions:*

(i) There exists a discrete valuation v on K such that

$$R = \{x \in K^* : v(x) \geq 0\} \cup \{0\}.$$

(ii) R is a Noetherian local ring with the property that the maximal ideal $\mathfrak{m}$ satisfies $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$ as a vector space over $R/\mathfrak{m}$.

(iii) R is a Noetherian local ring with principal and non-zero maximal ideal $\mathfrak{m}$.

(iv) R is a local principal ideal domain with non-zero maximal ideal $\mathfrak{m}$.

(v) There exists $\pi \in R$ such that every $x \in K^*$ can be written uniquely as $x = u\pi^k$ for $u \in R^*$ and $k \in \mathbb{Z}$.

Proof. $(i) \Rightarrow (ii)$.
Since $v(1/x) = -v(x)$ for $x \in K^*$ it follows that a nonzero $x \in R$ is a unit if and only if $v(x) = 0$. Note that

$$R \setminus R^* = \{x \in R \setminus \{0\} : v(x) > 0\} \cup \{0\}$$

is an ideal which implies that R is a local ring. Let $\pi \in R$ satisfy $v(\pi) = 1$. I claim that the nonzero ideals of R are given by (π^n) for $n \in \mathbb{Z}_{>0}$.
To see this, let I be a nonzero ideal of R and let $x \in I$ be such that $n = v(x) = \min\{v(y) : y \in I \setminus \{0\}\}$. Then $v(\pi^n/x) = 0$ so that $u = \pi^n/x \in R$. Then $\pi^n = ux \in I$ which gives $(\pi^n) \subset I$. Conversely, if $x \in I$ we have $v(x/\pi^n) \geq 0$ so that $u = x/\pi^n \in R$. Then $x = u\pi^n \in (\pi^n)$ and hence $I = (\pi^n)$. For $I = \mathfrak{m}$ we see that $\mathfrak{m} = (\pi)$ and $(\pi^n) = \mathfrak{m}^n$ for $n \in \mathbb{Z}_{>0}$.
Observe that $\pi \bmod \mathfrak{m}^2 \neq 0 \bmod \mathfrak{m}^2$ since $v(\pi) = 1 < 2$, so to show that $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$ it suffices to show that $\pi \bmod \mathfrak{m}^2$ spans $\mathfrak{m}/\mathfrak{m}^2$. To see this, let $x \bmod \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$ be arbitrary. Then $x/\pi \in R$ and we obtain

$$x \bmod \mathfrak{m}^2 = \left(\frac{x}{\pi} \bmod \mathfrak{m}\right)(\pi \bmod \mathfrak{m}^2).$$

$(ii) \Rightarrow (iii)$.
Let $\pi \in \mathfrak{m}$ be such that $\pi \bmod \mathfrak{m}^2$ spans $\mathfrak{m}/\mathfrak{m}^2$. Since R is Noetherian, $\mathfrak{m}$ is a finite R-module and hence we can use corollary 1.3.4 with $M = \mathfrak{m}$. This implies immediatly that $\mathfrak{m}$ is generated by π. Note that $\mathfrak{m}$ is non-zero since $\dim(\mathfrak{m}/\mathfrak{m}^2) > 0$.

$(iii) \Rightarrow (iv)$. Let $\pi \neq 0$ be a generator of $\mathfrak{m}$. I claim that every non-zero $x \in R$ can be written as $x = \pi^n u$ for $n \in \mathbb{Z}_{\geq 0}$ and $u \in R^*$. This is clear for units, so suppose that $x \in R$ is non-zero and not a unit. Then $x \in \mathfrak{m} = (\pi)$ since R is local. Since we have (using lemma 1.1.2)

$$0 \neq x \in (\pi) \supset (\pi^2) \supset (\pi^3) \supset \cdots \quad \text{and} \quad \bigcap_{k=1}^{\infty} (\pi^k) = 0,$$

we can set $n = \max\{k \in \mathbb{Z}_{>0} : x \in (\pi^k)\}$. Then $x = \pi^n u$ for some $u \in R$. Then u is a unit, for if not it would be contained in $\mathfrak{m} = (\pi)$ so that $x \in (\pi^{n+1})$, contradicting the maximality of n. This proves the claim.
To prove that R is a principal ideal domain, let I be an non-zero ideal of R. By the previous claim we can set

$$n = \min\{k \in \mathbb{Z}_{\geq 0} : \pi^k u \in I \text{ for some } u \in R^*\}.$$

Then $\pi^n \in I$ so $(\pi^n) \subset I$ and the converse follows by minimality of n: if $\pi^k u \in I$ then $k - n \geq 0$ so that $\pi^k u = \pi^n \pi^{k-n} u \in (\pi^n)$.

$(iv) \Rightarrow (v)$.
Let $\pi \neq 0$ be a generator of $\mathfrak{m}$ and suppose that $\pi' \in R$ is irreducible. Then (π') is a maximal ideal since R is a PID. Since R is local we see that $(\pi') = (\pi)$. It follows that every irreducible element of R is associated to π and hence unique factorization in R reduces to expressions of the form $u\pi^k$ for $u \in R^*$ and $k \in \mathbb{Z}_{\geq 0}$ and it follows that any $x \in K^*$ can be uniquely written as $x = u\pi^k$ for $u \in R^*$ and $k \in \mathbb{Z}$.

$(v) \Rightarrow (i)$.
By the unique factorisation property we have a well defined map $v : K^* \to \mathbb{Z}$ given by $v(u\pi^k) = k$. It is clear that $v(xy) = v(x) + v(y)$ holds for $x, y \in K^*$. It suffices to prove $v(x+y) \geq \min\{v(x), v(y)\}$ for nonzero $x, y \in R$ with $x + y \neq 0$, for if $x, y \in K^*$ are such that $x + y \neq 0$ and $n \in \mathbb{Z}$ is such that $x\pi^n, y\pi^n \in R$ we have

$$\begin{aligned} v(x+y) &= v(x\pi^n + y\pi^n) - v(\pi^n) \\ &\geq \min\{v(x\pi^n), v(y\pi^n)\} - v(\pi^n) \\ &= \min\{v(x\pi^n) - v(\pi^n), v(y\pi^n) - v(y\pi^n)\} \\ &= \min\{v(x), v(y)\}. \end{aligned}$$

To see that it holds in the case that $x, y \in R$, write $x = u\pi^k$ and $y = v\pi^m$ for $u, v \in R^*$ and $k, m \in \mathbb{Z}_{\geq 0}$. Then $\pi^n | x$ and $\pi^n | y$ where $n = \min\{v(x), v(y)\} = \min\{k, m\}$ so that $\pi^n | x + y$. The factorization of $x + y$ now implies that $n \leq v(x + y)$ as desired.
Since $v(\pi) = 1$ and clearly $R = \{x \in K^* : v(x) \geq 0\} \cup \{0\}$ this completes the proof. □

For clarity we summarize the properties of DVR's as seen in the proofs above.

Theorem 1.4.3. *Let R be a discrete valuation ring with field of fractions K and discrete valuation $v : K^* \to \mathbb{Z}$. Then for any $\pi \in R$ with $v(\pi) = 1$ we have that every non-zero element of K can be uniquely written as $u\pi^k$ for $u \in R^*$ and $k \in \mathbb{Z}$, the non-zero ideals of R are given by (π^k) for $k \in \mathbb{Z}_{\geq 0}$ and we have $v(u\pi^k) = k$ for all $u\pi^k \in K \setminus \{0\}$.*

We now consider an important example using the established theory.

Example 1.4.4. *The local ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ as seen in example 1.2.7 is a discrete valuation ring.*

This follows from part *(iii)* of theorem 1.4.2: it is Noetherian by theorem 1.2.5, it is local by theorem 1.2.6 and the non-zero maximal ideal

$$(p)\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : a \in (p), b \in \mathbb{Z} \setminus (p) \right\}$$

is principal: it has generator p. The units of $\mathbb{Z}_{(p)}$ are those $\frac{a}{b} \in \mathbb{Z}_{(p)}$ such that $a, b \in \mathbb{Z} \setminus (p)$. The field of fractions of $\mathbb{Z}_{(p)}$ is $\mathbb{Q}$ so we see that every non-zero $x \in \mathbb{Q}$ can be written uniquely as $x = \frac{a}{b} \cdot p^k$ for a and b not divisible by p and $k \in \mathbb{Z}$. The corresponding valuation v_p on $\mathbb{Q}$ is then given by

$$v_p(x) = v_p\left(\frac{a}{b}p^k\right) = k.$$

This valuation is called the p-adic valuation on $\mathbb{Q}$.
Lastly, we have surjective ring homomorphism $\mathbb{Z}_{(p)} \to \mathbb{Z}/p\mathbb{Z}$ given by $a/b \mapsto (a \bmod p)(b \bmod p)^{-1}$. As $\mathbb{Z}/p\mathbb{Z}$ is a field the kernel of this map is a maximal ideal, and because $\mathbb{Z}_{(p)}$ is local it follows that $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. Hence we have $k = \mathbb{F}_p$ for the residue field k of $\mathbb{Z}_{(p)}$.

1.5 Formal power series

For a ring R one can consider the polynomial ring $R[X]$, which can be constructed as the collection of all sequences $\{a_i\}_{i=0}^{\infty}$ in R for which a_i is non-zero for a finite number of indices i. One then uses the notation $\{a_i\}_{i=0}^{\infty} = \sum_{i=0}^{n} a_i X^i$, where n is such that $a_i = 0$ for $i \geq n$.

Definition 1.5.1. *Let R be a ring. The ring of formal power series $R[[X]]$ is defined as the set of all sequences $\{a_n\}_{n=0}^{\infty}$ in R and for such a sequence one uses the notation*

$$\sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \cdots.$$

For $f \in R[[X]]$ and $i \in \mathbb{Z}_{\geq 0}$ we write $f[X^i]$ for the coefficient of the term X^i of f. That is $f[X^i] = a_i$ for $f = \sum_{n=0}^{\infty} a_n X^n$.

Just as for $R[X]$, it is straightforward to verify that $R[[X]]$ becomes a ring with addition and multiplication defined as

$$\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} (a_n + b_n) X^n.$$

$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_{n-k} b_k\right) X^n.$$

$$= a_0 b_0 + (a_1 b_0 + a_0 b_1) X + (a_2 b_0 + a_1 b_1 + a_0 b_2) X^2 + \cdots.$$

The product is sometimes called the cauchy product.

One can define a topology on $R[[X]]$ such that the formal expression $\sum_{n=0}^{\infty} a_n X^n$ concides with the limit of the finite sums $\sum_{n=0}^{m} a_n X^n$ as $m \to \infty$.

Proposition 1.5.2. *Let R be a ring. Then we have a well-defined topology on $R[[X]]$ by declaring a subset $U \subset R[[X]]$ to be open if and only if for each $x \in U$*

there exists an $n \in \mathbb{Z}_{\geq 0}$ such that $x + X^n R[[X]] \subset U$.
This topology makes $R[[X]]$ into a topological ring, i.e. addition and multiplication are continuous maps.

Proof. It is clear the the topology contains $\emptyset$ and $R[[X]]$ itself and it clearly closed under taking unions. if $U, V \subset R[[X]]$ are open, and $x \in U \cap V$. Then there exist $n, m \in \mathbb{Z}_{\geq 0}$ such that $x + X^n R[[X]] \subset U$ and $x + X^m R[[X]] \subset V$. It follows that $x + X^k \subset U \cap V$ for $k = \max\{n, m\}$ and hence $U \cap V$ is open. This shows that the topology is well-defined.
The proof that addition and multiplication are continuous follows immediatly from the fact that the $X^n R[[X]]$ are ideals of $R[[X]]$, for let $s, m : R[[X]] \times R[[X]] \to R[[X]]$ denote the addition and multiplication respectively.
Let $(f, g) \in R[[X]] \times R[[X]]$ and let $U, U' \subset R[[X]]$ be open neighborhoods of $s(f, g) = f + g$ and $m(f, g) = fg$ respectively. Pick $n \in \mathbb{Z}_{\geq 0}$ such that $f + g + X^n R[[X]] \subset U$ and $gf + X^n R[[X]] \subset U'$. As we have

$$f + g + X^n R[[X]] = (f + X^n R[[X]]) + (g + X^n R[[X]])$$
$$fg + X^n R[[X]] = (f + X^n R[[X]])(g + X^n R[[X]]),$$

it follows immediatly that $s(V) \subset U$ and $m(V) \subset U'$ for the open neighborhood $V = (f + X^n R[[X]]) \times (g + X^n R[[X]])$ of (f, g) in $R[[X]] \times R[[X]]$ and hence s and m are continuous. □

We now summarize some basic properties of $R[[X]]$.

Proposition 1.5.3. *Let R be a ring and consider the ring of formal power series $R[[X]]$. Then*

(i) If R is an integral domain then so is $R[[X]]$.

(ii) If R is Noetherian then so is $R[[X]]$.

(iii) The unit group of $R[[X]]$ is given by

$$(R[[X]])^* = \left\{ \sum_{n=0}^{\infty} a_n X^n \in R[[X]] : a_0 \in R^* \right\}.$$

Proof. To prove (i), assume that R is an integral domain and let $f = \sum_{n=0}^{\infty} a_n X^n$ and $g = \sum_{n=0}^{\infty} b_n X^n$ be non-zero elements of $R[[X]]$. Define

$$m = \min\{n \in \mathbb{Z}_{\geq 0} : a_n \neq 0\}, \quad k = \min\{n \in \mathbb{Z}_{\geq 0} : b_n \neq 0\}.$$

We have $fg = \sum_{n=0}^{\infty} c_n X^n$ for $c_n = \sum_{i=0}^{n} a_{n-i} b_i$ $(n \in \mathbb{Z}_{\geq 0})$. I claim that $c_{m+k} \neq 0$. By the minimality of m and k we have $b_i = 0$ for $i < k$ and for $m + k \geq i > k$ we have $m + k - i < m$ so that $a_{m+k-i} = 0$. It follows that $a_{m+k-i} b_i = 0$ for $i \in \{1, \ldots, m + k\} \setminus \{k\}$ and hence

$$c_{m+k} = \sum_{i=0}^{m+k} a_{m+k-i} b_i = a_{m+k-k} b_k = a_m b_k \neq 0$$

as $a_m, b_k \neq 0$ and R is an integral domain. This shows that $fg \neq 0$ and hence $R[[X]]$ is an integral domain.

To prove (ii), assume that R is Noetherian and let $I \subset R[[X]]$ be an ideal. For $n \in \mathbb{Z}_{\geq 0}$ define

$$I_n := \{r \in R : r = f[X^n] \text{ for some } f \in X^n R[[X]] \cap I\}.$$

Then the I_n are ideals of R as I is an ideal, and we have $I_n \subset I_{n+1}$ as I is closed under multiplication by $X \in R[[X]]$. Thus we have an increasing chain of ideals $I_0 \subset I_1 \subset J_2 \subset \cdots$ so we have $I_m = I_{m+1} = \cdots$ for some $m \in \mathbb{Z}> 0$ as R is Noetherian.
For $i \in \{0, \ldots, m\}$ let $I_i = (r_{i0}, \ldots, r_{iv_i})$ for certain $r_{ij} \in R$ $(1 \leq j \leq v_i)$. For each such r_{ij}, choose some $g_{ij} \in X^i R[[X]] \cap I$ such that $r_{ij} = g_{ij}[X^i]$ and let J be the ideal in $R[[X]]$ generated by

$$\{g_{ij} : 1 \leq i \leq m, 1 \leq j \leq v_i\}.$$

Then clearly J is a finitely generated ideal contained in I and I claim that in fact $J = I$.
To see this, let $f \in I$. Inductively construct $g_0, g_1, \ldots \in J$ as follows. Let $a_0 := f[X^0]$ and note that $a_0 \in I_0 = (r_{01}, \ldots, r_{0v_0})$ so that $a_0 = k_{01}r_{01} + \cdots + k_{0v_0}r_{0v_0}$ for certain $k_{0j} \in R$. Define $g_0 = k_{01}g_{01} + \cdots + k_{0v_0}g_{0v_0}$, so that $g_0 \in J$ and

$$g_0[X^0] = k_{01}r_{01} + \cdots + k_{0v_0}r_{0v_0} = a_0 = f[X^0].$$

It follows that $f - g_0 \in XR[[X]]$.
Now suppose inductively that for some $n \in \mathbb{Z}_{\geq 0}$ we have $g_0, \ldots, g_n \in J$ such that $f - \sum_{i=0}^{n} g_i \in X^{n+1}R[[X]]$. Let $a_{n+1} = \left(f - \sum_{i=0}^{n} g_i\right)[X^{n+1}]$ so that $a_{n+1} \in I_{n+1}$. Now distinguish two cases: $n < m$ and $n \geq m$.
Assume that $n < m$. As $a_{n+1} \in I_{n+1}$ and $n + 1 \leq m$ we have $I_{n+1} = (r_{(n+1)1}, \ldots, r_{(n+1)v_{n+1}})$, so we have

$$a_{n+1} = k_{(n+1)1}r_{(n+1)1} + \cdots + k_{(n+1)v_{n+1}}r_{(n+1)v_{n+1}}$$

for certain $k_{(n+1)j} \in R$ $(1 \leq j \leq v_{n+1})$. Then define

$$g_{n+1} := k_{(n+1)1}g_{(n+1)1} + \cdots + k_{(n+1)v_{n+1}}g_{(n+1)v_{n+1}}.$$

It follows that $g_{n+1} \in X^{n+1}R[[X]]$, and

$$\begin{aligned} g_{n+1}[X^{n+1}] &= k_{(n+1)1}r_{(n+1)1} + \cdots + k_{(n+1)v_{n+1}}r_{(n+1)v_{n+1}} \\ &= a_{n+1} = \left(f - \sum_{i=0}^{n} g_i\right)[X^{n+1}]. \end{aligned}$$

Thus $\left(f - \sum_{i=0}^{n} g_i\right) - g_{n+1} = f - \sum_{i=0}^{n+1} g_i \in X^{n+2}R[[X]]$.
For the second and remaining case, assume that $n \geq m$. Then $a_{n+1} \in I_{n+1} =$

$I_m = (r_{m1}, \ldots, r_{mv_m})$ so for certain $k_{(n+1)j} \in R$ $(1 \leq j \leq v_m)$ we have

$$a_{n+1} = \sum_{j=1}^{v_m} k_{(n+1)j} r_{mj}.$$

Note that the number of j in the sum is independent of n, it just depends on m. Now define $g_{n+1} \in R[[X]]$ as

$$g_{n+1} = \sum_{j=1}^{v_m} k_{(n+1)j} X^{n+1-m} g_{mj}.$$

As we have $g_{mj} \in X^m R[[X]]$ for $1 \leq j \leq v_m$ it follows that $g_{n+1} \in X^{n+1} R[[X]]$, and just as in the case of $n < m$ we have

$$g_{n+1}[X^{n+1}] = \sum_{j=1}^{v_m} k_{(n+1)j} r_{mj} = a_{n+1} = \left(f - \sum_{i=0}^{n} g_i \right) [X^{n+1}].$$

so that also in this case we have $(f - \sum_{i=0}^{n} g_i) - g_{n+1} = f - \sum_{i=0}^{n+1} g_i \in X^{n+2} R[[X]]$.

This concludes both cases and thus we have inductively defined $g_0, g_1, \ldots \in J$ with the following properties:

(a) We have $f - \sum_{i=0}^{n} g_i \in X^{n+1} R[[X]]$ for all $n \in \mathbb{Z}_{\geq 0}$.

(b) For $n \geq m$ we have $g_n = \sum_{j=1}^{v_m} k_{nj} X^{n-m} g_{mj}$.

To finish the argument that $f \in J$, define

$$h_j = \sum_{n=m}^{\infty} k_{nj} X^{n-m} \in R[[X]] \quad (1 \leq j \leq v_m)$$

and let $h = \sum_{j=1}^{v_m} h_j g_{mj} \in J$. To show that $f \in J$ it suffices to show that $f = g_0 + \cdots + g_{m-1} + h$. To see this note that (a) implies that

$$f = \sum_{n=0}^{\infty} g_n = g_0 + g_1 + \cdots + g_{m-1} + \sum_{n=m}^{\infty} g_n.$$

Using continuity of addition and multiplication we see that

$$\sum_{n=m}^{\infty} g_n = \sum_{n=m}^{\infty} \sum_{j=1}^{v_m} k_{nj} X^{n-m} g_{mj} = \sum_{j=1}^{v_m} \sum_{n=m}^{\infty} k_{nj} X^{n-m} g_{mj} = \sum_{j=1}^{v_m} h_j g_{mj} = h.$$

Here continuity of addition was used to interchange the two sums and continuity of the multiplication justifies the fact that the constant g_{mj} can be taken out of the series $\sum_{n=m}^{\infty} k_{nj} X^{n-m} g_{mj}$ for fixed j. This implies that

$f = g_0 + \cdots + g_{m-1} + h$ and hence the proof of (ii) is complete.

To prove (iii), suppose that $f = \sum_{n=0}^{\infty} a_n X^n \in R[[X]]$ is a unit. Then $fg = 1$ for some $g = \sum_{n=0}^{\infty} b_n X^n \in R[[X]]$. We have

$$fg = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + (a_2 b_0 + a_1 b_1 + a_0 b_2)X^2 + \cdots = 1,$$

so that $a_0 b_0 = 1$ and hence $a_0 \in R^*$. Conversely, suppose that $a_0 \neq 0$. Let $b_0 = a_0^{-1}$ and define b_n for $n \in \mathbb{Z}_{>0}$ recursively by

$$b_n = -a_0^{-1} \sum_{k=0}^{n-1} a_{n-k} b_k. \tag{5}$$

It follows that $a_0 b_0 = 1$ and for $n \in \mathbb{Z}_{>0}$ we have $0 = a_0 b_n + \sum_{k=0}^{n-1} a_{n-k} b_k = \sum_{k=0}^{n} a_{n-k} b_k$ and hence $g := \sum_{n=0}^{\infty} b_n X^n$ is the inverse of f:

$$fg = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_{n-k} b_k \right) X^n = 1. \qquad \square$$

Corollary 1.5.4. *In the ring of formal power series $R[[X]]$ over a ring R we have*

$$(1 - X)^{-1} = 1 + X + X^2 + \cdots .$$

Proof. Let $f = \sum_{n=0}^{\infty} a_n X^n = 1 - X$. Then from 1.5.3 we have that f is a unit with inversegiven by $g = \sum_{n=0}^{\infty} b_n X^n$ with $b_0 = a_0^{-1} = 1$ and b_n $(n \geq 1)$ as in (5). As $a_k = 0$ for $k \geq 2$ we get for $n \geq 1$

$$b_n = -a_0^{-1} \sum_{k=0}^{n-1} a_{n-k} b_k = -(a_1 b_{n-1}) = b_{n-1}.$$

As $b_0 = 1$ it follows that $g = 1 + X + X^2 + \cdots$ as desired. $\square$

Corollary 1.5.5. *The ring of formal power series $k[[X]]$ over a field k is a discrete valuation ring with uniformizing parameter X.*

Proof. Proposition 1.5.3 implies that $k[[X]]$ is Noetherian integral domain and that the non-units of $k[[X]]$ are those series $\sum_{n=0}^{\infty} a_n X^n$ for which $a_0 = 0$. It follows that

$$k[[X]] \setminus (k[[X]])^* = X \cdot k[[X]],$$

and hence $k[[X]]$ is a local ring with principal non-zero maximal ideal. It follows that $k[[X]]$ is DVR by 1.4.2. $\square$

Definition 1.5.6. *Let k be a field. Then the field of Laurent series $k((X))$ is defined as the field of fractions of the discrete valuation ring $k[[X]]$.*

Note that by proposition 1.4.2 we have that a non-zero $f \in k((X))$ can be written uniquely as $f = X^k g$ for an integer k and $g = \sum_{n=0}^{\infty} a_n X^n$ a unit of $k[[X]]$. That is

$$f = X^k \sum_{n=0}^{\infty} a_n X^n = \sum_{n=k}^{\infty} a_{n-k} X^n.$$

Thus we see that the field of fractions $k((X))$ of $k[[X]]$ is obtained by allowing a finite number of negative powers of X to occur in a series $\sum_n a_n X^n$.

2 The p-adic numbers

This section is devoted to a construction of the *ring of p-adic integers* $\mathbb{Z}_p$ and the *field of p-adic numbers* $\mathbb{Q}_p$. We will construct $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value and establish some basic properties like compactness of $\mathbb{Z}_p$ and the Laurent series representation of elements of $\mathbb{Q}_p$.

2.1 Ultrametric spaces

The valuation v_p on $\mathbb{Q}$ as in example 1.4.4 will induce an absolute value on $\mathbb{Q}$ and the absolute value will in turn induce an ultrametric. A few basic results about ultrametric spaces are discussed in this section.

Definition 2.1.1. *A metric d on a set X is called an ultrametric if the following ultrametric inequality holds for $x, y, z \in x$:*

$$d(x, y) \leq \max\{d(x, z), d(y, z)\}. \tag{6}$$

In this case X is called an ultrametric space.

Note that as $d(x, y), d(y, z) \leq d(x, y)+d(y, z)$ we have $\max\{d(x, y), d(y, z)\} \leq d(x, y) + d(y, z)$ so the ultrametric inequality implies the usual triangle inequality.
Principles in ultrametric spaces can be counterintuitive as they don't behave like Euclidean distances: distances in ultrametric spaces don't add up. As an example of this consider the ε-ball $B_\varepsilon(x) = \{y \in X : d(x, y) < \varepsilon\}$ for an $x \in X$. Then for $y, z \in B_\varepsilon(x)$ we have $d(x, y) < \varepsilon$ and $d(x, z) < \varepsilon$, so by the ultrametric inequality we have $d(y, z) \leq \max\{d(y, x), d(z, x)\} < \varepsilon$. It follows that the diameter of $B_\varepsilon(x)$ does not exceed its radius.

Proposition 2.1.2. *The following statements hold in an ultrametric space X.*

(i) If $x, y, z \in X$ are such that $d(x, y) < d(x, z)$ then $d(x, z) = d(y, z)$. That is, if from the three possible distances between the points x, y, z we have that two distances are unequal, then the largest distance equals the remaining distance.

(ii) The open and closed ε-balls

$$B_\varepsilon(x) = \{y \in X : d(x, y) < \varepsilon\}$$
$$\overline{B}_\varepsilon(x) = \{y \in X : d(x, y) \leq \varepsilon\}$$

are both simultaneously open and closed subsets of X.

(iii) If (x_n) is a sequence in X such that $d(x_n, x_{n+1}) \to 0$ as $n \to \infty$ then (x_n) is a cauchy sequence.

Proof. Using the ultrametric inequality twice we obtain

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

The second maximum equals $d(y,z)$ because otherwise we would get $d(x,z) \leq d(x,y)$, contradicting $d(x,y) < d(x,z)$. This proves (i).
To prove (ii) note that $B_\varepsilon(x)$ is open and $\overline{B}_\varepsilon(x)$ is closed as is true in any metric space. To prove that they are closed and open respectively, it suffices to show that the sphere $S_\varepsilon(x) := \{y \in X : d(x,y) = \varepsilon\}$ is open in X as we have

$$B_\varepsilon(x) = \overline{B}_\varepsilon(x) \setminus S_\varepsilon(x) \quad \text{and} \quad \overline{B}_\varepsilon(x) = B_\varepsilon(x) \cup S_\varepsilon(x).$$

To prove that $S_\varepsilon(x)$ is open in X, let $y \in S_\varepsilon(x)$. Then $B_\varepsilon(y) \subset S_\varepsilon(x)$, for let $z \in B_\varepsilon(y)$. Then $d(y,z) < \varepsilon = d(x,y)$ so (i) implies that $d(y,z) = d(x,y) = \varepsilon$ and hence $z \in S_\varepsilon(x)$ as desired.
To prove (iii), let $\varepsilon > 0$ and let $N \in \mathbb{Z}_{\geq 0}$ be such that $d(x_n, x_{n+1}) < \varepsilon$ for $n \geq N$. Let $n > m \geq N$. Using the ultrametric inequality on the points $x_m, x_{m+1}, \ldots, x_n$ to obtain

$$d(x_m, x_n) \leq \max\{d(x_i, x_{i+1}) : m \leq i < n\} < \varepsilon.$$

This shows that (x_n) is cauchy. □

2.2 Valued fields

A discrete valuation on a field K induces an absolute value in a natural way. This gives K the structure of a metric space and allows us to consider topological concepts on fields with a discrete valuation and the corresponding discrete valuation ring.

Definition 2.2.1. *An absolute value on a field K is a map $|\,.\,| : K \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in K$ we have*

(i) $|x| = 0$ *if and only if* $x = 0$.

(ii) $|xy| = |x||y|$.

(iii) $|x + y| \leq |x| + |y|$.

In this case K is called a valued field. If in addition the inequality $|x + y| \leq \max\{|x|, , |y|\}$ holds for $x, y \in K$ then the absolute value is said to be non-archimedian.

Since $|x|, |y| \leq |x| + |y|$ we see that $\max\{|x|, |y|\} \leq |x| + |y|$ so the non-archimedian inequality implies the standard triangle inequalty.
Here are some basic properties of valued fields.

Proposition 2.2.2. *Let K be a valued field, and let $x, y \in K$ and let (x_n) and (y_n) be sequences in K. Then the following statements holds:*

(i) *We have* $|1| = |-1| = 1$, $|x| = |-x|$ *and* $|x^{-1}| = |x|^{-1}$ *if* $x \neq 0$.

(ii) *The function* $d : K \times K \to \mathbb{R}_{\geq 0}$ *given by* $d(x, y) = |x - y|$ *defines a translation invariant metric on* K*, if the absolute value is non-archimedian then* d *satisfies the ultrametric inequality* $d(x, y) \leq \max\{d(x, z), d(z, y)\}$ *for* $x, y, z \in K$.

(iii) $|x - y| \geq ||x| - |y||$.

(iv) *If* $x_n \to x$ *then* $|x_n| \to |x|$.

(v) *If* (x_n) *and* (y_n) *are cauchy then* $(x_n + y_n)$ *and* $(x_n y_n)$ *are cauchy as well.*

(vi) *If* $x_n \to x$ *and* $y_n \to y$ *then* $x_n + y_n \to x + y$ *and* $x_n y_n \to xy$.

If the absolute value is non-archimedean then the following statements hold as well:

(vii) *If* $|x| < |y|$ *then* $|x + y| = |y|$.

(viii) *If* $x_n \to x$ *and* $x \neq 0$*, then* $|x_n| = |x|$ *for* n *sufficiently large.*

(ix) *The series* $\sum_{n=1}^{\infty} x_n$ *converges if* $x_n \to 0$ *and* K *is complete.*

Proof. We have $|1|^2 = |1 \cdot 1| = |1|$ and since $|1| \neq 0$ this gives $|1| = 1$. We then have $|-1|^2 = |1| = 1$ so that $|-1| = 1$. This gives $|-x| = |-1||x| = |x|$. If $x \neq 0$ we have $1 = |1| = |xx^{-1}| = |x||x|^{-1}$ which proves $|x^{-1}| = |x|^{-1}$. This completes (i).
To see that d defines a metric, we clearly have $d(x, y) = 0$ if and only if $x = y$, and

$$d(x, y) = |x - y| = |(-1)(y - x)| = |-1||y - x| = |y - x| = d(y, x).$$

For $x, y, z \in K$ we have $d(x, y) = |x - y| = |x - z + z - y| \leq |x - z| + |z - y| = d(x, z) + d(z, y)$, and clearly this also gives the ultrametric inequality when the absolute value is non-archimedian. This shows that d is a metric on K, and the translation invariance is also immediate.
To prove (iii), note that we have the inequalities

$$|x| \leq |x - y| + |y|, \quad \text{and} \quad |y| \leq |y - x| + |x|.$$

Substracting $|y|$ and $|x|$ respectively from these two inequalities results in $||x| - |y|| \leq |x - y|$ as desired. From this we also obtain (iv) as we have

$$||x_n| - |x|| \leq |x_n - x| \to 0 \text{ as } n \to \infty$$

To prove (v), note that a cauchy sequence is bounded, for if $N \in \mathbb{Z}_{>0}$ is such that $|x_n - x_m| < 1$ for $n, m \geq N$ then for $n \geq N$ we have

$$|x_n| \leq |x_n - x_N| + |x_N| < 1 + |x_N|.$$

Hence the sequence (x_n) is bounded by $M := \max\{|x_1|, \ldots, |x_{N-1}|, 1 + |x_N|\}$. If M is a bound on the cauchy sequences (x_n) and (y_n) then we have

$$\begin{aligned} |(x_n + y_n) - (x_m + y_m)| &\leq |x_n - x_m| + |y_n - y_m| \to 0 \text{ as } n, m \to \infty. \\ |x_n y_n - x_m y_m| &\leq |x_n||y_n - y_m| + |y_m||x_n - x_m| \\ &\leq M|y_n - y_m| + M|x_n - x_m|\} \to 0 \text{ as } n, m \to \infty. \end{aligned}$$

This shows that $(x_n + y_n)$ and $(x_n y_n)$ are cauchy. The above also proves (vi) if we replace x_m with x and y_m with y. Note that M also bounds x and y by (iv).

Now assume that the absolute value is non-archimedean, so that the induced metric is an ultrametric by (ii).
The proof of (vii) is a reformulation of proposition 2.1.2 (i), for we have $d(x, 0) = |x| < |y| = | - y| = d(-y, 0)$ so that

$$|x + y| = d(x, -y) = d(-y, 0) = | - y| = |y|.$$

To prove $(viii)$, let $N \in \mathbb{Z}_{>0}$ such that $|x_n - x| < |x|$ for $n \geq N$. Using (vii) for such n we obtain

$$|x_n| = |(x_n - x) + x| = |x|.$$

To prove (ix), let (s_n) be the sequence of partial sums, i.e. $s_n = x_1 + \cdots + x_n$ for $n \in \mathbb{Z}_{>0}$. Then $d(s_{n+1}, s_n) = |s_{n+1} - s_n| = |x_n| \to 0$ as $n \to \infty$. Thus (s_n) is cauchy by 2.1.2 (iii) and hence converges which means that the series $\sum_{n=1}^{\infty} x_n$ is convergent. □

Note that one can summarize (iv) and (vi) of proposition 2.2.2 by saying that the maps $K \to \mathbb{R}_{\geq 0}$ and $K \times K \to K$ given by the absolute value, addition and multiplication are continuous maps, with the topology induced by the metric in (ii) on K, the corresponding product topology on $K \times K$ and the induced euclidean topology on $\mathbb{R}_{\geq 0}$.

A map between $\varphi : K \to L$ between valued fields is said to be an isometry if φ is a ring homomorphism and preserves the absolute value, that is $|\varphi(x)| = |x|$ for $x \in K$. If φ is bijective then it is said to be an isomorphism and K and L are said to be isomorphic. If φ is an isometry then it is induces an isomorphism between K and $\varphi(K) \subset L$. If one identifies K with $\varphi(K)$ then one can think of K as a subset of L.

Theorem 2.2.3. *Let K be a field with discrete valuation v and let the real number α satisfy $0 < \alpha < 1$. Then $|\,.\,| : K \to \mathbb{R}_{\geq 0}$ given by*

$$|x| = \begin{cases} \alpha^{v(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

defines a non-archimedean absolute value on K.

Proof. It is clear that $|x| = 0$ if and only if $x = 0$. Let $x, y \in K$ then if x or y equals 0 we trivially have $|xy| = |x||y|$. If both are non-zero we have

$$|xy| = \alpha^{v(xy)} = \alpha^{v(x)+v(y)} = \alpha^{v(x)}\alpha^{v(y)} = |x||y|.$$

Lastly, if x, y or $x + y$ equals zero we clearly have $|x + y| \leq \max\{|x|, |y|\}$. If all three are non-zero, we have

$$|x + y| = \alpha^{v(x+y)} \leq \alpha^{\min\{v(x)+v(y)\}} = \max\{\alpha^{v(x)}, \alpha^{v(y)}\} = \max\{|x|, |y|\}. \quad \square$$

Definition 2.2.4. *Let K be a field with discrete valuation v and $\alpha \in \mathbb{R}$ such that $0 < \alpha < 1$. Then the non-archimedian absolute value $K \to \mathbb{R}_{\geq 0}$ obtained from v and α as in theorem 2.2.3 is called the absolute value induced by (v, α).*

Note that for the absolute value $|\,.\,| : K \to \mathbb{R}_{\geq 0}$ induced by (v, α) we have for non-zero $x \in K$ that $v(x) \geq 0$ if and only if $|x| \leq 1$. Thus the discrete valuation ring R of K is the closed unit ball with respect to this norm.
If $\mathfrak{m}$ is the maximal ideal of R then the non-zero ideals are given by

$$\begin{aligned}\mathfrak{m}^k &= \{0\} \cup \{x \in R \setminus \{0\} : v(x) \geq k\} \\ &= \{x \in R : |x| \leq \alpha^k\}.\end{aligned}$$

We also see that the ideals are closed. For $k < 0$ we don't have $\mathfrak{m}^k \subset R$ but $\mathfrak{m}^k$ is still a closed R-submodule of K.

As seen in example 1.4.4 we have the so called p-adic valuation v_p on $\mathbb{Q}$. Taking $\alpha = p^{-1}$ we obtain the p-adic absolute value on $\mathbb{Q}$, denoted by $|\,.\,|_p$. That is we have

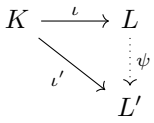
$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-v_p(x)} & \text{if } x \in \mathbb{Q}^*. \end{cases}$$

The real numbers $\mathbb{R}$ are a completion of the rational number $\mathbb{Q}$ with respect to the usual archimedean absolute value on $\mathbb{Q}$. The field of p-adic numbers $\mathbb{Q}_p$ will be constructed as the completion of $\mathbb{Q}$ with respect to the non-archimedian p-adic absolute value, one can think of $\mathbb{Q}_p$ as a non-archimedean analogue of $\mathbb{R}$. This completion process is the subject of the next section.

2.3 Completion of valued fields

A complete valued field is a valued field that is complete as a metric space. If a valued field is not complete, we can always consider its completion. Recall that an isometry of valued fields is a ring homomorphism preserving the absolute value, and that an isomorphism of valued fields is a bijective isomety.

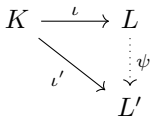
Definition 2.3.1. *Let K be a valued field. We say that a complete valued field L, together with an isometry $\iota : K \to L$ is a completion of K if it satisfies the following universal property:*
if L' is another complete valued field with an isometry $\iota' : K \to L'$ then there exists a unique isometry $\psi : L \to L'$ such that the following diagram commutes.



That is, the map $i' : K \to L'$ factors uniquely through L. In addition, if the absolute value on K is non-archimedian we require that the absolute value on L is also non-archimedian.

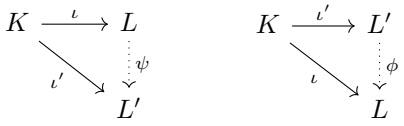
We will show that a completion of a valued field always exists and that it is essentially unique. We first tackle uniqueness.

Lemma 2.3.2. *If (L, ι) and (L', ι') are two completions of the valued field K, then there exists a unique isomorphism $\psi : L \to L'$ compatible with ι and ι'. That is we have a commutative diagram*

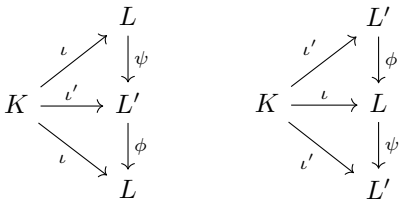


where ψ is now an isomorphism.

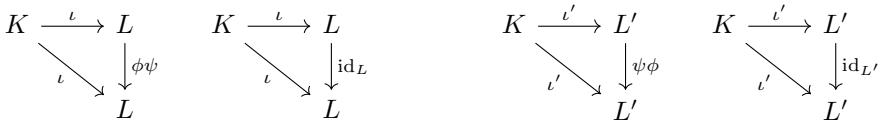
Proof. Since L and L' are completions of K, there exist unique isometry $\psi : L \to L'$ and $\phi : L' \to L$ such that we have commutative diagrams



It suffices to show that ψ is an isomorphism for it is clearly unique by the unique factorisation property in definition 2.3.1.
Combining the above two diagrams we obtain the commutative diagrams



We now have four commutative diagrams:



The uniqueness of the factorisation in definition 2.3.1 now implies that $\phi\psi = \mathrm{id}_L$ and $\psi\phi = \mathrm{id}_{L'}$. Thus ϕ and ψ are mutual inverses which proves that ψ is an isomorphism. □

The following lemma gives a sufficient condition for when the universal property in definition 2.3.1 is satisfied.

Lemma 2.3.3. *Let K be a valued field and let L be a complete valued field with isometry $\iota : K \to L$. Then L is a completion of K if $\iota(K)$ is a dense subset of L.*

Proof. Let L' be a complete valued field with isometry $\iota' : K \to L'$. We need to show that there exists a unique isometry $\psi : L \to L'$ such that $\iota' = \psi\iota$.
Since ι is injective we have an inverse $\iota^{-1} : \iota(K) \to K$, i.e. $\iota\iota^{-1} = \mathrm{id}_{\iota(K)}$ and $\iota^{-1}\iota = \mathrm{id}_K$. The composition $\phi := \iota'\iota^{-1} : i(K) \to L'$ is an isometry. Define the map $\psi : L \to L'$ as follows. For $x \in L$ there exists a sequence (x_n) contained in $\iota(K)$ such that $x = \lim x_n$. Then (x_n) is a cauchy sequence, and since ϕ is an isometry it follows that $\phi(x_n)$ is a cauchy sequence in L. Since L is complete it has a unique limit and we define $\psi(x) = \lim \phi(x_n)$.
Note that ψ is well defined, for if (y_n) is another sequence in $\iota(K)$ converging to x we have

$$|\psi(x_n) - \psi(y_n)| = |\psi(x_n - y_n)| = |x_n - y_n| \to 0 \text{ as } n \to \infty.$$

This implies that $\lim \psi(x_n) = \lim \psi(y_n)$ and hence ψ is well defined.
By taking the sequence $(x, x, \dots)$ for $x \in \iota(K)$ it follows that ψ is an extension of ϕ. The fact that ψ is an isometry is a straightforward consequence of the continuity of addition, multiplication and the absolute value. For example, to show that ψ preserves the absolute value, let $x = \lim x_n$ for $x \in L$ and (x_n) a sequence in $\iota(K)$. We then have

$$|\psi(x)| = \lim_{n\to\infty} |\phi(x_n)| = \lim_{n\to\infty} |x_n| = |x|.$$

It is clear that ψ satisfies $\iota' = \psi\iota$ since $\psi(x) = \iota'\iota^{-1}(x)$ for $x \in \iota(K)$. Thus it remains to show that ψ is unique. Suppose that $\psi' : L \to L'$ is another isometric ring homomorphism satisfying $\iota' = \psi'\iota$. Premultipying with ι^{-1} we see that ψ and ψ' agree on $\iota(K)$. If $x \in L$, then $x = \lim x_n$ for a sequence (x_n) contained in $\iota(K)$. Since ψ and ψ' are isometries they are continuous, so it follows that

$$\psi(x) = \lim_{n\to\infty} \psi(x_n) = \lim_{n\to\infty} \psi'(x_n) = \psi'(x).$$

This shows that $\psi = \psi'$ and hence the proof is complete. □

It remains to prove existence.

Theorem 2.3.4. *Every valued field admits a completion.*

Proof. Let K be a valued field. Let $\mathfrak{R}$ be the set of all Cauchy sequences in K. It is a ring under pointwise addition and multiplication by proposition 2.2.2. Now define

$$\mathfrak{m} = \{(x_n) \in \mathfrak{R} : \lim x_n = 0\}.$$

This is an ideal of $\mathfrak{R}$. It is clearly an additive subgroup of $\mathfrak{R}$ and it is closed under multiplication by members of $\mathfrak{R}$ because Cauchy sequences are bounded.

I claim that $L := \mathfrak{R}/\mathfrak{m}$ is a field. Let $(x_n) \bmod \mathfrak{m} \in \mathfrak{R}/\mathfrak{m}$ be nonzero. This means that $(x_n) \notin \mathfrak{m}$. I claim that there exists an $\varepsilon_0 > 0$ and $N \in \mathbb{Z}_{>0}$ such that $|x_n| \geq \varepsilon_0$ for all $n \geq N$. Suppose for contradiction that this is not true. Then for all $\varepsilon > 0$, and all $N \in \mathbb{Z}_{>0}$ there exists $n \geq N$ such that $|x_n| < \varepsilon$. By taking $\varepsilon = 1/n$ for $n \in \mathbb{Z}_{>0}$ this results in a subsequence of (x_n) converging to 0. Since (x_n) is Cauchy this would imply that $(x_n) \in \mathfrak{m}$ which is not the case.

It follows that there exists $\varepsilon_0 > 0$ and $N \in \mathbb{Z}_{>0}$ such that $|x_n| \geq \varepsilon_0$ for all $n \geq N$.
Define the sequence (y_n) in K by $y_n = 1$ if $n < N$ and $y_n = x_n$ if $n \geq N$. Then (y_n) is cauchy, $(x_n) \bmod \mathfrak{m} = (y_n) \bmod \mathfrak{m}$ and $y_n \neq 0$ for all $n \in \mathbb{Z}_{>0}$. The sequence $(1/y_n)$ is then also cauchy:

$$\left|\frac{1}{y_n} - \frac{1}{y_m}\right| = \frac{|y_m - y_n|}{|y_n y_m|} \leq \varepsilon_0^{-2}|y_n - y_m| \to 0 \text{ as } n, m \to \infty.$$

It follows that $(1/y_n) \bmod \mathfrak{m}$ is the inverse of $(x_n) \bmod \mathfrak{m}$ which implies that $L = \mathfrak{R}/\mathfrak{m}$ is a field. If $(x_n) \bmod \mathfrak{m} \in L$ then $(|x_n|)$ is a cauchy sequence in $\mathbb{R}$ and hence converges. Define $|\,.\,| : L \to \mathbb{R}_{\geq 0}$ as

$$|(x_n) \bmod \mathfrak{m}| = \lim_{n\to\infty} |x_n|.$$

Using proposition 2.2.2 it is straightforward to check that this defines a absolute value on L and that it is non-archimedian if the absolute value on K is. Define $\iota : K \to L$ as the map

$$\iota(x) = (x, x, \dots) \bmod \mathfrak{m}.$$

Then ι is an isometry. The fact that $\iota(K)$ is dense in L is a consequence of

$$\mathbf{x} = \lim_{n\to\infty} \iota(x_n), \quad (\mathbf{x} = (x_n) \bmod \mathfrak{m} \in L). \tag{7}$$

To prove (7), let $\varepsilon > 0$. Since (x_n) is cauchy, there exists $N \in \mathbb{Z}_{>0}$ such that $|x_n - x_m| < \varepsilon/2$ whenever $n, m \geq N$. If $n \geq N$ it follows that

$$|\mathbf{x} - \iota(x_n)| = \lim_{m\to\infty} |x_m - x_n| \leq \frac{\varepsilon}{2} < \varepsilon.$$

This proves (7). Lemma 2.3.3 now implies that in order to show that (L, ι) is a completion of K it suffices to prove that L is complete.

Let $(\mathbf{x}_n)$ be a cauchy sequence in L. For $n \in \mathbb{Z}_{>0}$ there exists $y_n \in K$ such that $|\mathbf{x}_n - \iota(y_n)| < 1/n$ by the density of $\iota(K)$ in L. Then

$$\begin{aligned}|y_n - y_m| = |\iota(y_n) - \iota(y_m)| &\leq |\iota(y_n) - \mathbf{x_n}| + |\mathbf{x}_n - \mathbf{x}_m| + |\mathbf{x}_m - \iota(y_m)| \\ &\leq 1/n + |\mathbf{x}_n - \mathbf{x}_m| + 1/m \to 0 \text{ as } n, m \to \infty,\end{aligned}$$

which implies that (y_n) is a cauchy sequence in K.
To see that $(\mathbf{x}_n)$ converges to $\mathbf{y} := (y_n) \bmod \mathfrak{m} \in L$, note that

$$\mathbf{x}_n = \mathbf{x}_n - \iota(y_n) + \iota(y_n), \qquad (n \in \mathbb{Z}_{>0}).$$

Since $\lim(\mathbf{x}_n - \iota(y_n)) = 0$ and $\lim \iota(y_n) = \mathbf{y}$ by (7) it follows that $\lim \mathbf{x}_n = \mathbf{y}$ and hence L is complete. □

From now on we will speak of the completion L of the valued field K and identifying K with its image under the embedding $K \to L$ and write $K \subset L$. With this identification the absolute value on L extends the absolute value on K.

Theorem 2.3.5. *Suppose that K is field with absolute value induced by (v, α) for a discrete valuation v on K and that α is a real number such that $0 < \alpha < 1$. Then there exists a unique discrete valuation v' on the completion L of K extending v such that the absolute value on L is induced by (v', α).*

Proof. Uniqueness is immediate: if (v', α) induces the absolute value on L then $|x| = \alpha^{v'(x)}$ so that $v'(x) = \log_\alpha |x|$ for $x \in L^*$, which completely determines v'.
For the existence, define $v' : L^* \to \mathbb{Z}$ as $v'(x) = \log_\alpha |x|$. Then $|x| = \alpha^{v'(x)}$ so to complete the proof it suffices to show that v' is well defined (in the sense that $v'(x) \in \mathbb{Z}$ for $x \in L^*$) and that v' is indeed a discrete valuation extending v.
Let $x \in L^*$ and let (x_n) be a sequence in K such that $\lim x_n = x$. As x is non-zero, proposition 2.2.2 gives that $|x| = |x_N|$ for some $N \in \mathbb{Z}_{>0}$. Then $v'(x) = \log_\alpha |x| = \log_\alpha |x_N| = v(x_N) \in \mathbb{Z}$ and hence v' is well defined.
To show that v' is a valuation, let $x, y \in L^*$ and let (x_n) and (y_n) in K such that $x_n \to x$ and $y_n \to y$. As x and y are non-zero, proposition 2.2.2 yields that

$$|x_N| = |x| \text{ and } |y_N| = |y| \text{ for some } N \in \mathbb{Z}_{>0}. \tag{8}$$

Taking the base α logarithm gives $v'(x) = v(x_N)$ and $v'(y) = v(y_N)$. We also have $v'(xy) = v(x_N y_N)$ as $|x_N y_N| = |xy|$, and it follows that $v'(xy) = v'(x) + v'(y)$ since v is a discrete valuation on K.
If in addition we have $x + y \neq 0$, we may assume that N in (8) also satisfies $|x_N + y_N| = |x + y|$ as $x_n + y_n \to x + y$ so that $v'(x + y) = v(x_N + y_N)$. It follows that $v'(x + y) \geq \min\{v'(x), v'(y)\}$ as v is a discrete valuation on K. □

The following theorem tells us that the quotients of discrete valuation rings do not change under completion.

Theorem 2.3.6. *Let K' be the completion of the valued field K and assume that the absolute values on K and K' are induced by (v, α) and (v', α) respectively. Let $(R, \mathfrak{m})$ and $(R', \mathfrak{m}')$ be the corresponding discrete valuation rings of K and K'. We then have*

$$R/\mathfrak{m}^n \cong R'/(\mathfrak{m}')^n \quad \text{for } n \in \mathbb{Z}_{>0}.$$

In particular, the residue fields $k = R/\mathfrak{m}$ and $k' = R'/\mathfrak{m}'$ are isomorphic.

Proof. Note that $R \subset R'$ and $\mathfrak{m}^n \subset (\mathfrak{m}')^n$. We have a homomorphism $\varphi : R' \to R'/(\mathfrak{m}')^n$ given by $r \mapsto r \bmod (\mathfrak{m}')^n$ with kernel $(\mathfrak{m}')^n$. The restriction of φ to R has kernel $R \cap (\mathfrak{m}')^n = \mathfrak{m}^n$ so we obtain an injective ring homomorphism

$$\begin{aligned} \overline{\varphi} : R/\mathfrak{m}^n &\to R'/(\mathfrak{m}')^n \\ r \bmod \mathfrak{m}^n &\mapsto r \bmod (\mathfrak{m}')^n \end{aligned}$$

Thus to complete the proof it suffices to show that $\overline{\varphi}$ is surjective.
Let $r' \bmod (\mathfrak{m}')^n \in R'/(\mathfrak{m}')^n$ be arbitrary. If $r' = 0$ then $r' \bmod \mathfrak{m}'$ clearly lies in the image of $\overline{\varphi}$, so we may assume that $r' \neq 0$. Since K is dense in K' there exists $r \in K$ such that $|r - r'| < \min\{|r'|, \alpha^n\}$.
Using proposition 2.2.2 it follows that $|r| = |(r - r') + r'| = |r'| \leq 1$ so $r \in R$. Since also $|r - r'| \leq \alpha^n$ we see that $r - r' \in (\mathfrak{m}')^n$ and hence $r' \bmod (\mathfrak{m}')^n = r \bmod (\mathfrak{m}')^n = \overline{\varphi}(r \bmod \mathfrak{m}^n)$. Thus $\overline{\varphi}$ is surjective and hence the proof is complete. □

2.4 Construction of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ and some properties

Let p be a fixed prime number. Recall from example 1.4.4 that we have a discrete valuation $v_p : \mathbb{Q}^* \to \mathbb{Z}$ given by $v_p(p^k \cdot a/b) = k$.
We define the p-adic absolute value on $\mathbb{Q}$ to be the absolute value $|\,.\,|_p$ on $\mathbb{Q}$ induced by (v_p, p^{-1}). That is

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-v_p(x)} & \text{if } x \neq 0 \end{cases}$$

Definition 2.4.1. *The field of p-adic numbers $\mathbb{Q}_p$ is defined as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value.*

The p-adic absolute value on $\mathbb{Q}$ extends to an absolute value on $\mathbb{Q}_p$ which we also denote by $|\,.\,|_p$, and according to theorem 2.3.5 this absolute value is induced by an extension of the p-adic valuation v_p on $\mathbb{Q}$ to a discrete valuation on $\mathbb{Q}_p$ which we also denote by v_p.
As v_p is a surjective map to $\mathbb{Z}$, we see that the image of the p-adic absolute value $|\,.\,|_p$ on $\mathbb{Q}_p$ in $\mathbb{R}_{\geq 0}$ equals

$$\{0\} \cup \{p^k : k \in \mathbb{Z}\}.$$

Definition 2.4.2. *The ring of p-adic integers $\mathbb{Z}_p$ is defined as the discrete valuation ring of $\mathbb{Q}_p$. That is*

$$\mathbb{Z}_p = \{0\} \cup \{x \in \mathbb{Q}_p^* : v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

In particular, since $v_p(p) = 1$ we have that p generates the maximal ideal of $\mathbb{Z}_p$.

Proposition 2.4.3. *The residue field of $\mathbb{Z}_p$ equals $\mathbb{F}_p$.*

Proof. The discrete valuation rings of $\mathbb{Q}$ and $\mathbb{Q}_p$ with respect to the p-adic valuation are $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$ respectively. Theorem 2.3.6 implies $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, and as seen in example 1.4.4 the latter is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. This completes the proof. □

This result allows us to derive the Laurent series expansion for elements of $\mathbb{Q}_p$.

Proposition 2.4.4. *Let $k \in \mathbb{Z}$ and suppose that $\{a_i\}_{i=k}^{\infty}$ is a sequence in $S := \{0, 1, \ldots, p-1\} \subset \mathbb{Z} \subset \mathbb{Z}_p$. Then $\sum_{i=k}^{\infty} a_i p^i$ is a convergent series in $\mathbb{Q}_p$, and $x = \sum_{i=k}^{\infty} a_i p^i \in \mathbb{Q}_p$ is non-zero if $a_k \neq 0$ and we have*

$$v_p(x) = v_p\left(\sum_{i=k}^{\infty} a_i p^i\right) = k. \tag{9}$$

Moreover, every $x \in \mathbb{Q}_p$ can be written as a convergent series $x = \sum_{i=k}^{\infty} a_i p^i$ for $k \in \mathbb{Z}$ and $\{a_i\}_{i=k}^{\infty}$ a sequence in S, and this series expansion is unique for non-zero x if we require that $a_k \neq 0$.

Proof. Let $k \in \mathbb{Z}$ and $\{a_i\}_{i=k}^{\infty}$ a sequence in S. Then $|a_i p^i|_p \leq p^{-i} \to 0$ as $i \to \infty$ so the terms of the series $\sum_{i=k}^{\infty} a_i p^i$ go to 0. It follows that the series converges by proposition 2.2.2.

Valuation of a series.
To prove (9), let $x = \sum_{i=k}^{\infty} a_i p^i \in \mathbb{Q}_p$ be such that $a_k \neq 0$. As $p^k\mathbb{Z}_p$ is a closed $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p$ we have $x \in p^k\mathbb{Z}_p$. Similarly we have $x - a_k p^k = \sum_{i=k+1}^{\infty} a_i p^i \in p^{k+1}\mathbb{Z}_p$. Since $|a_k|_p = 1$ (it is non-zero), we obtain

$$|x - a_k p^k|_p \leq p^{-(k+1)} < p^{-k} = |a_k p^k|_p$$

Using proposition 2.2.2 we get $|x|_p = |(x - a_k p^k) + a_k p^k|_p = |a_k p^k|_p = p^{-k}$. This implies that x is non-zero and $v_p(x) = k$ as desired.
To prove uniqueness of the series expansion for a non-zero $x \in \mathbb{Q}^*$, suppose that we have

$$x = \sum_{i=k}^{\infty} a_i p^i = \sum_{i=l}^{\infty} b_i p^i,$$

for $k, l \in \mathbb{Z}$ and $\{a_i\}_{i=k}^{\infty}$ and $\{b_i\}_{i=l}^{\infty}$ sequences in S such that $a_k \neq 0 \neq b_l$.
Then $k = v_p(x) = l$ by (9).

Uniqueness.
We first prove uniqueness in the case that $k = 0$ and then we show that the

general case follows from this, so assume that$k = 0$. Then for $n \in \mathbb{Z}_{\geq 0}$ we have $x - \sum_{i=0}^{n} a_i p^i = \sum_{i=n+1}^{\infty} a_i p^i \in p^{n+1}\mathbb{Z}_p$, or

$$x \equiv \sum_{i=0}^{n} a_i p^i \bmod p^{n+1}\mathbb{Z}_p \tag{10}$$

We now prove that $a_n = b_n$ for $n \in \mathbb{Z}_{\geq 0}$ using induction on n. Letting $n = 0$ in (10) gives $x \equiv a_0 \bmod p\mathbb{Z}_p$ and $x \equiv b_0 \bmod p\mathbb{Z}_p$. Since $a_0, b_0 \in S$ and S is a system of representatives for $\mathbb{Z}_p/p\mathbb{Z}_p$ it follows that $a_0 = b_0$.
Suppose that for some $n \in \mathbb{Z}_{>0}$ we have $a_i = b_i$ for all $i \in \{0, 1, \ldots, n-1\}$. Then $\sum_{i=0}^{n-1} a_i p^i = \sum_{i=0}^{n-1} b_i p^i$ so that

$$p^n \sum_{i=n}^{\infty} a_i p \sum_{i=n}^{\infty} a_i p^i = x - \sum_{i=0}^{n-1} a_i p^i = x - \sum_{i=0}^{n-1} b_i p^i = \sum_{i=n}^{\infty} b_i p^i.$$

As $p^n \neq 0$ this gives $\sum_{i=n}^{\infty} a_i p^{i-n} = \sum_{i=n}^{\infty} b_i p^{i-n}$. Reducing this equality mod$p\mathbb{Z}_p$ we obtain $a_n \equiv b_n \bmod p\mathbb{Z}_p$, and as $a_n, b_n \in S$ this gives $a_n = b_n$ so by induction the series expansion is unique when $k = 0$.
For the general case of uniqueness, let $k \in \mathbb{Z}$ arbitrary. Then $\sum_{i=0}^{\infty} a_{i+k} p^i$ and $\sum_{i=0}^{\infty} b_{i+k} p^i$ are two series expansions for $p^{-k}x$. Since $v_p(p^{-k}x) = 0$ the series are unique so that $a_{i+k} = b_{i+k}$ for all $i \in \mathbb{Z}_{\geq 0}$, which is the same as $a_i = b_i$ for all $i \in \mathbb{Z}_{\geq k}$. This proves the uniqueness.

Existence.
To prove existence of the series we first prove that every $x \in \mathbb{Z}_p$ admits such a series expansion. Recall that $S = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}_p$ is a system of representatives for $\mathbb{Z}_p/p\mathbb{Z}_p$.
Let $x \in \mathbb{Z}_p$ and inductively construct $a_0, a_1, a_2, \ldots \in S$ as follows: let $a_0 \in S$ be such that $x \equiv a_0 \bmod p\mathbb{Z}_p$, and suppose that for some $k \in \mathbb{Z}_{\geq 0}$ we have $a_0, a_1, \ldots, a_k \in S$ such that $x \equiv a_0 + a_1 p + \cdots + a_k p^k \bmod p^{k+1}\mathbb{Z}_p$. Then $x - \sum_{i=0}^{k} a_i p^i = p^{k+1} x_{k+1}$ for some $x_{k+1} \in \mathbb{Z}_p$. Let $a_{k+1} \in S$ be such that $x_{k+1} \equiv a_{k+1} \bmod p\mathbb{Z}_p$. Then we have $x_{k+1} = a_{k+1} + py$ for some $y \in \mathbb{Z}_p$ and it follows that

$$x = \sum_{i=0}^{k} a_i p^i + p^{k+1} x_{k+1} = \sum_{i=0}^{k} a_i p^i + p^{k+1}(a_{k+1} + py) = \sum_{i=0}^{k+1} a_i p^i + p^{k+2} y.$$

Thus we have $x \equiv a_0 + a_1 p + \cdots + a_{k+1} p^{k+1} \bmod p^{k+2}\mathbb{Z}_p$, so by induction this results in a sequence $\{a_i\}_{i=0}^{\infty}$ in S such that $x \equiv \sum_{i=0}^{n} a_i p^n \bmod p^{n+1}\mathbb{Z}_p$ for all $n \in \mathbb{Z}_{\geq 0}$, or $x - \sum_{i=0}^{n} a_i p^i \in p^{n+1}\mathbb{Z}_p$. This gives

$$\left| x - \sum_{i=0}^{n} a_i p^i \right|_p \leq \frac{1}{p^{n+1}} \to 0 \text{ as } n \to \infty, \tag{11}$$

and this shows that $x = \sum_{i=0}^{\infty} a_i p^i$ as desired.
Let $x \in \mathbb{Q}_p^*$ and pick $k \in \mathbb{Z}$ such that $y = p^k x \in \mathbb{Z}_p$. Then $y = \sum_{i=0}^{\infty} a_i p^i$ for

certain $a_0, a_1, \ldots \in S$ and it follows that

$$x = p^{-k}y = p^{-k}\sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} a_i p^{i-k}.$$

Letting $b_k, b_{k+1}, \ldots \in S$ be defined as $b_i = a_{i-k}$ $(i \in \mathbb{Z}_{\geq k})$ we see that $x = \sum_{i=0}^{\infty} b_{i-k}p^{i-k} = \sum_{i=k}^{\infty} b_i p^i$ as desired. This shows that every $x \in \mathbb{Q}_p$ admits such a series expansion and hence the proof is complete. □

We also obtain the following corollary from (9).

Corollary 2.4.5. *The ring of p-adic integers $\mathbb{Z}_p$ consists precisely of the series*

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots,$$

for $a_i \in \{0, \ldots, p-1\}$. The unit group $\mathbb{Z}_p^*$ consists of the series for which $a_0 \neq 0$.

As $\mathbb{Z}_p$ is a discrete valuation ring with uniformizing parameter p we know that every non-zero $x \in \mathbb{Q}_p$ can be written uniquely as $x = up^k$ for $u \in \mathbb{Z}_p^*$ and $k \in \mathbb{Z}$. But observe that for such x we have $x = \sum_{i=k}^{\infty} a_i p^i$ for $k \in \mathbb{Z}$ and $a_k, a_{k+1}, \ldots \in \{0, \ldots, p-1\}$ such that $a_k \neq 0$. We can write

$$x = \sum_{i=k}^{\infty} a_i p^i = p^k \sum_{i=0}^{\infty} a_{i+k} p^i.$$

And $u = \sum_{i=0}^{\infty} a_{i+k}p^i \in \mathbb{Z}_p^*$ from corollary 2.4.5, so this is the desired expansion $x = up^k$.

The ring of p-adic integers $\mathbb{Z}_p$ is compact. This is usually done by proving $\mathbb{Z}_p$ can be embedded as a closed subset of a countable cartesian product of finite discrete spaces. The product is then compact by Tychonoff's theorem and compactness of $\mathbb{Z}_p$ follows. We take a different approach using a characterisation of compactness in metric spaces.

Proposition 2.4.6. *A metric space X is compact if and only if it is complete and totally bounded.*

Recall that a metric space X is totally bounded if it admits a finite ε-net for all $\varepsilon > 0$. An ε-net is a subset $S \subset X$ such that $X = \bigcup_{s \in S} B_\varepsilon(s)$. Thus a metric space is totally bounded if for all $\varepsilon > 0$, it can be covered by a finite collection of ε-balls.

Proposition 2.4.7. *The ring of integers $\mathbb{Z}_p$ is compact.*

Proof. As $\mathbb{Z}_p$ is a closed subset of $\mathbb{Q}_p$ it is complete. To see that it is totally bounded, note that for $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ we have

$$\left| x - \sum_{i=0}^{n} a_i p^i \right|_p = \left| \sum_{i=n+1}^{\infty} a_i p^i \right|_p \leq \frac{1}{p^{n+1}} \qquad (n \in \mathbb{Z}_{\geq 0}).$$

This implies that for $\varepsilon > 0$, the finite set

$$S_n = \left\{ \sum_{i=0}^{n} a_i p^i : a_0, \ldots, a_n \in \{0, \ldots, p-1\} \right\}$$

is an ε-net for $\mathbb{Z}_p$ if $n \in \mathbb{Z}_{\geq 0}$ is chosen such that $p^{-(n+1)} < \varepsilon$. It follows that $\mathbb{Z}_p$ is totally bounded and hence it is compact by proposition 2.4.6. $\square$

3 p-adic integration

We assume that the reader is familiar with Lebesque integration. For the sake of completeness we briefly state the relevant definitions and theorems sufficient for discussing p-adic integration. We will be integrating continuous functions $\mathbb{Z}_p^n \to \mathbb{C}$ by using Haar's measure for compact topological groups. The existence and uniqueness of a Haar measure on locally compact Hausdorff topological groups is a deep result due to Weil.

3.1 Basic definitions and results from measure theory

The standard context for measure theory and Lebesque integration is a measure space. The definition as a follows.

Definition 3.1.1. *A measure space is a triple $(\Omega, \mathfrak{M}, \mu)$. Here Ω is a set, $\mathfrak{M}$ is a σ-algebra of subsets of Ω (meaning that $\mathfrak{M}$ contains Ω and is closed under taking complement and countable unions), and μ is a measure on $\mathfrak{M}$, i.e. a map $\mu : \mathfrak{M} \to [0, \infty]$ such that $\mu(\emptyset) = 0$ and which is countably additive on disjoint sets:*

$$\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n), \quad \text{for all } A_1, A_2, \ldots \in \mathfrak{M} \text{ pairwise disjoint.}$$

The members of $\mathfrak{M}$ are called the measurable sets. A set of measure zero is a measurable set A with $\mu(A) = 0$. If one has a σ-algebra $\mathfrak{M}$ on a set Ω one calls the pair $(\Omega, \mathfrak{M})$ a measurable space.
When X is a topological space, one can consider the Borel-algebra $\mathfrak{B}$ on X. This is the σ-algebra generated by all open subsets of X.
If $(\Omega, \mathfrak{M})$ and $(\Omega', \mathfrak{M}')$ are measure spaces and $f : \Omega \to \Omega'$ is a map, we say that f is measurable if $f^{-1}(A) \in \mathfrak{M}$ whenever $A \in \mathfrak{M}'$. In particular, any continuous map between topological spaces X and Y is measurable with respect to the Borel-algebras on X and Y. A measure on the Borel-algebra of a topological space is called a Borel measure.

We now define integrals of functions $\Omega \to \mathbb{C}$ for a measure space $(\Omega, \mathfrak{M}, \mu)$. We take the Borel-algebra on $\mathbb{C}$ and its topological subspaces.
A simple function on Ω is a measurable map $\varphi : \Omega \to [0, \infty)$ with finite range, say $\{\alpha_1, \ldots, \alpha_n\}$. Let $A_i = \varphi^{-1}(\alpha_i) = \{\omega \in \Omega : \varphi(\omega) = \alpha_i\}$. The integral of φ over $E \in \mathfrak{M}$ is then defined as

$$\int_E \varphi \, d\mu = \sum_{i=1}^{n} \alpha_i \mu(A_i \cap E).$$

For example, if χ_E is the characteristic function on E, i.e. $\chi_E(x) = 1$ if $x \in E$ and $\chi_E(x) = 0$ otherwise, we have $\int_E \chi_E \, d\mu = \mu(E)$.
For a measurable map $f : \Omega \to [0, \infty)$ and $E \in \mathfrak{M}$ the integral of f over E is

then defined as

$$\int_E f\,d\mu = \sup\left\{\int_E \varphi\,d\mu : 0 \le \varphi \le f, \varphi \text{ simple}\right\}.$$

For a map $f : \Omega \to \mathbb{R}$ we have $f = f^+ - f^-$ where $f^+ = \max\{f, 0\}$ and $f^- = \min\{f, 0\}$ are the positive and negative parts of f. They are measurable if f is measurable. If $f : \Omega \to \mathbb{C}$ is measurable, then $|f| : \Omega \to [0, \infty)$ is also measurable. If the integral $\int_\Omega |f|\,d\mu$ is finite we say that f is integrable.
Write $f = u + iv$ for $u, v : \Omega \to \mathbb{R}$ the real and imaginary parts of f. Then $|u^+| \le |f|$ and $|-u^-| \le |f|$ and so u^+ and $-u^-$ are integrable and they define functions $\Omega \to [0, \infty)$. Similarly for v^+ and v^-. Then for $E \in \mathfrak{M}$ we define

$$\int_E f\,d\mu = \int_E u^+\,d\mu + \int_E -u^-\,d\mu + i\left(\int_E v^+\,d\mu + \int_E -v^-\,d\mu\right).$$

We now state some properties of the Lebesque integral of integrable functions $\Omega \to \mathbb{C}$. The proofs can be found in Rudin [8].

Theorem 3.1.2. *Let $(\Omega, \mathfrak{M}, \mu)$ be measure space. Let $\alpha, \beta \in \mathbb{C}$ and $f, g : \Omega \to \mathbb{C}$ be integrable functions. Then the following statements hold.*

1. *The function $\alpha f + \beta g$ is integrable and for $E \in \mathfrak{M}$ we have*

$$\int_E \alpha f + \beta g\,d\mu = \alpha \int_E f\,d\mu + \beta \int_E g\,d\mu.$$

2. *For $E \in \mathfrak{M}$ we have*

$$\left|\int_E f\,d\mu\right| \le \int_E |f|\,d\mu.$$

An important tool for using the Lebesque integral is the Dominated Convergence theorem.

Theorem 3.1.3. *Let $(\Omega, \mathfrak{M}, \mu)$ be measure space and suppose that (f_n) is a sequence of functions $\Omega \to \mathbb{C}$ such that*

$$f(\omega) := \lim_{n\to\infty} f_n(\omega)$$

exists for all $\omega \in \Omega$. If there exists an integrable function $g : \Omega \to \mathbb{C}$ such that $|f_n(\omega)| \le |g(\omega)|$ for all $\omega \in \Omega$ then f is integrable and for all $E \in \mathfrak{M}$ we have

$$\lim_{n\to\infty} \int_E f_n\,d\mu = \int_E f\,d\mu.$$

3.2 Igusa's local Zeta function

On locally compact Hausdorff groups one can define a translation invariant measure on the Borel subsets, for a proof of existence and uniqueness, see [**?**].

Theorem 3.2.1. *Let G be a compact Hausdorff group and let $\mathfrak{B}$ be the Borel-algebra on G. Then there exists a unique regular Borel measure $\mu : \mathcal{B} \to [0, \infty]$, called the Haar measure that satisfies the following properties:*

1. *The measure is translation invariant, i.e. $\mu(gS) = \mu(S) = \mu(Sg)$ for all $g \in G$ and $S \in \mathfrak{B}$.*
2. *$\mu(G) = 1$.*

As $\mathbb{Z}_p$ is compact and Hausdorff (it is metrizable), so is $\mathbb{Z}_p^n$ for $n \in \mathbb{Z}_{>0}$ and hence we have a Haar measure on $\mathbb{Z}_p^n$.

Proposition 3.2.2. *Let μ be the Haar measure on $\mathbb{Z}_p^n$. Then for $m \in \mathbb{Z}_{\geq 0}$ we have $\mu((p^m\mathbb{Z}_p)^n) = \frac{1}{p^{mn}}$.*

Proof. We have a disjoint union $\mathbb{Z}_p = \bigcup_{i=0}^{p^m-1} i + p^m\mathbb{Z}_p$ as $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^m\mathbb{Z}$, and this gives a disjoint union of $\mathbb{Z}_p^n$ as follows:

$$\mathbb{Z}_p^n = \left(\bigcup_{i=0}^{p^m-1} i + p\mathbb{Z}_p \right)^n = \bigcup_{0 \leq i_1, \ldots, i_n < p^m} \left[(i_1 + p^m\mathbb{Z}_p) \times \cdots \times (i_n + p^m\mathbb{Z}_p) \right].$$

Since the union is disjoint and the Haar measure is translation invariant we have

$$\mu(\mathbb{Z}_p^n) = \sum_{0 \leq i_1, \ldots, i_n < p^m} \mu\left((i_1 + p^m\mathbb{Z}_p) \times \cdots \times (i_n + p^m\mathbb{Z}_p) \right) = \sum_{0 \leq i_1, \ldots, i_n < p^m} \mu((p^m\mathbb{Z}_p)^n).$$

As the sum consists of p^{mn} terms it follows that $1 = \mu(\mathbb{Z}_p^n) = p^{mn}\mu((p\mathbb{Z}_p)^n)$ as desired. □

Definition 3.2.3. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and $s \in \mathbb{C}$ with positive real part. Then the (local) zeta function of f is defined as*

$$Z_p(f, s) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, d\mu(x).$$

We need to verify that the integrand is integrable. Write $g : \mathbb{Z}_p^n \to \mathbb{C}$ for the integrand, and observe that it is continuous for it is the composition of continuous functions.

$$\mathbb{Z}_p^n \xrightarrow{f} \mathbb{Z}_p \xrightarrow{|\cdot|_p} \mathbb{R}_{\geq 0} \xrightarrow{(.)^s} \mathbb{C}$$

Since $\mathbb{Z}_p^n$ is compact it follows that g is bounded. Since also $\mu(\mathbb{Z}_p^n) = 1 < \infty$ it follows that g is in fact integrable as we have

$$\int_{\mathbb{Z}_p^n} |g(x)| \, d\mu(x) \leq \mu(\mathbb{Z}_p^n) \cdot \sup_{x \in \mathbb{Z}_p^n} |g(x)| = \sup_{x \in \mathbb{Z}_p^n} |g(x)| < \infty,$$

Note that the image $g(\mathbb{Z}_p^n)$ of the integrand $g : \mathbb{Z}_p^n \to \mathbb{C}$ is contained in

$$\{0\} \cup \{p^{-ks} : k \in \mathbb{Z}_{\geq 0}\} \subset \mathbb{C}$$

which is a countable set. Thus g has an at most countable image. The integrals of measurable functions with a finite image (simple functions) are easy to evaluate: the integral is a linear combination of the measures of the inverse images. Using Lebesque's dominated convergence theorem we obtain an analogous result for $Z_p(f,s) = \int_{\mathbb{Z}_p^n} g\, d\mu$ using an infinite sum.

Proposition 3.2.4. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and $s \in \mathbb{C}$ with positive real part. For $k \in \mathbb{Z}_{\geq 0}$ define*

$$E_k = \{x \in \mathbb{Z}_p^n : |f(x)|_p = p^{-k}\}. \tag{12}$$

Then the sets E_k are measurable and

$$Z(f,s) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, d\mu(x) = \sum_{k=0}^{\infty} p^{-ks} \mu(E_k).$$

Proof. Let $g : \mathbb{Z}_p \to \mathbb{C}$ be the integrand, that is $g(x) = |f(x)|_p^s$. For $m \in \mathbb{Z}_{\geq 0}$ define $g_m : \mathbb{Z}_p \to \mathbb{C}$ by

$$g_m(x) = \begin{cases} g(x) & \text{if } x \in E_0 \cup \cdots \cup E_m \\ 0 & \text{otherwise} \end{cases}$$

Then g_m is a simple function with range contained in $\{0, 1, p^{-s}, \ldots, p^{-ms}\}$ and $g_m^{-1}(p^{-ks}) = E_k$. Thus we have

$$\int_{\mathbb{Z}_p^n} g_m(x)\, d\mu(x) = \sum_{k=0}^{m} p^{-ks} \mu(E_k).$$

Now g is integrable as we have seen, we have $g_m \to g$ pointwise and $|g_m(x)| \leq |g(x)|$ for all $x \in \mathbb{Z}_p$ and $m \in \mathbb{Z}_{\geq 0}$. The dominated convergence theorem now implies that

$$Z(f,s) = \int_{\mathbb{Z}_p^n} g(x)\, d\mu(x) = \lim_{m\to\infty} \int_{\mathbb{Z}_p^n} g_m(x)\, d\mu(x) = \sum_{k=0}^{\infty} p^{-ks} \mu(E_k). \qquad \square$$

Example 3.2.5.

Let $n = 1$ and $f = X^d \in \mathbb{Z}_p[X]$ for $d \in \mathbb{Z}_{>0}$. Let $E_0, E_1, \ldots$ be as in (12). For $k \in \mathbb{Z}_{\geq 0}$ and $x \in \mathbb{Z}_p$ we have $|f(x)|_p = |x|_p^d = p^{-k}$ if and only if $x \neq 0$ and $dv(x) = k$. So in particular we see that $E_k = \emptyset$ and $\mu(E_k) = 0$ when d does not divide k.
If d does divide k we have $k = md$ for some $m \in \mathbb{Z}_{\geq 0}$ so that $dv(x) = k$ if and only if $m = v(x)$. Thus we have $E_k = E_{md} = p^m\mathbb{Z}_p \setminus p^{m+1}\mathbb{Z}_p$ and $\mu(E_{md}) = p^{-m} - p^{-(m+1)}$ by proposition 3.2.2. Thus we have

$$\begin{aligned} Z_p(f,s) &= \sum_{k=0}^{\infty} p^{-ks}\mu(E_k) = \sum_{m=0}^{\infty} p^{-mds}\mu(E_{md}) = \sum_{m=0}^{\infty} \frac{1}{p^{mds}} \left(\frac{1}{p^m} - \frac{1}{p^{m+1}}\right) \\ &= \sum_{m=0}^{\infty} \frac{p-1}{p^{mds}p^{m+1}} = \sum_{m=0}^{\infty} \frac{p-1}{p} \left(p^{-ds-1}\right)^m = \frac{p-1}{p(1-p^{-ds-1})} = \frac{p-1}{p-p^{-ds}}. \end{aligned}$$

3.3 The power series

Let p be a prime number. Then for a polynomial $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ one defines the power series of f to be the following formal power series:

$$Q_p(f,t) := \sum_{m=0}^{\infty} N_m t^m \in \mathbb{Z}[[t]],$$

where $N_0 = 1$ and

$$N_m = |\{x \in (\mathbb{Z}/p^m\mathbb{Z})^n : (f \bmod p^m)(x) = 0\}| \qquad (m \in \mathbb{Z}_{>0}).$$

Here $f \bmod p^m$ is the polynomial of which the coefficients are reduced $\bmod\ p^m$. That is, it is the image of f under the ring homomorphism

$$\mathbb{Z}_p[X_1, \ldots, X_n] \to (\mathbb{Z}/p^m\mathbb{Z})[X_1, \ldots, X_n]$$

induced by the composite ring homomorphism $\mathbb{Z}_p \to \mathbb{Z}_p/p^m\mathbb{Z}_p \to \mathbb{Z}/p^m\mathbb{Z}$.

Example 3.3.1.

Consider the case of $f = X^d \in \mathbb{Z}_p[X]$ for $d \in \mathbb{Z}_{>0}$. For $m \in \mathbb{Z}_{>0}$ and $x \in \mathbb{Z}_p$ we have $f(x) = x^d \equiv 0 \bmod p^m$ if and only if $p^m | x^d$.
To proceed we write $m = qd + r$ for $q \in \mathbb{Z}_{\geq 0}$ and $r \in \{1, \ldots, d\}$ (!), and $x = up^k$ for $u \in \mathbb{Z}_p^*$ and $k \in \mathbb{Z}_{\geq 0}$. Then $x^d = u^d p^{kd}$ so that

$$p^{qd+r} = p^m | x^d = u^d p^{kd} \quad \Leftrightarrow \quad qd + r \leq kd \quad \Leftrightarrow \quad q + \frac{r}{d} \leq k.$$

As $0 < r/d \leq 1$ we see that $q + r/d \leq k$ if and only if $q+1 \leq k$, which holds if and only if $p^{q+1} | up^k = x$, or $x \equiv 0 \bmod p^{q+1}$. We conclude that $f(x) \equiv 0 \bmod p^m$ if and only if $x \equiv 0 \bmod p^{q+1}$.
As $m \geq q + 1$ we have a well-defined ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}/p^m\mathbb{Z} &\to \mathbb{Z}/p^{q+1}\mathbb{Z}. \\ x \bmod p^m &\mapsto x \bmod p^{q+1} \end{aligned}$$

The kernel equals $\{x \bmod p^m : x \bmod p^{q+1} = 0 \bmod p^{q+1}\}$, so as $f(x) \equiv 0 \bmod p^m$ if and only if $x \equiv 0 \bmod p^{q+1}$ it follows that $N_m = |\ker(\varphi)|$. Since φ is surjective we get

$$p^{q+1} = |\mathbb{Z}/p^{q+1}\mathbb{Z}| = \frac{|\mathbb{Z}/p^m\mathbb{Z}|}{|\ker(\varphi)|} = \frac{p^m}{N_m}.$$

Thus we have $N_m = p^m/p^{q+1} = p^{m-q-1} = p^{qd+r-q-1} = p^{q(d-1)+r-1}$. We now calculate $Q_p(f,t)$:

$$Q_p(f,t) = \sum_{m=0}^{\infty} N_m t^m = 1 + \sum_{r=1}^{d} \sum_{q=0}^{\infty} N_{qd+r} t^{qd+r}$$

For $r \in \{1, \ldots, d\}$ we have

$$\sum_{q=0}^{\infty} N_{qd+r} t^{qd+r} = \sum_{q=0}^{\infty} p^{q(d-1)+r-1} t^{qd+r} = p^{r-1} t^r \sum_{q=0}^{\infty} p^{q(d-1)} t^{qd}$$
$$= p^{r-1} t^r \sum_{q=0}^{\infty} (p^{d-1} t^d)^q = \frac{p^{r-1} t^r}{1 - p^{d-1} t^d}.$$

It follows that

$$Q_p(f,t) = 1 + \sum_{r=1}^{d} \frac{p^{r-1} t^r}{1 - p^{d-1} t^d} = \frac{1 - p^{d-1} t^d + \sum_{r=1}^{d} p^{r-1} t^r}{1 - p^{d-1} t^d}$$
$$= \frac{1 + t + pt^2 + \cdots + p^{d-2} t^{d-1}}{1 - p^{d-1} t^d}.$$

3.4 Relation between the power series and the zeta function

For a prime p, $n \in \mathbb{Z}_{>0}$, $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and $s \in \mathbb{C}$ with $\Re(s) > 0$, we have defined

$$Q_p(f,t) = \sum_{m=0}^{\infty} N_m \cdot t^m \in \mathbb{Z}[[t]]$$
$$Z_p(f,s) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s \, d\mu(x) \in \mathbb{C}.$$

With $N_0 = 1$, $N_m = |\{x \in (\mathbb{Z}/p^m\mathbb{Z})^n : (f \bmod p^m)(x) = 0\}|$ for $m \in \mathbb{Z}_{>0}$ and μ the Haar measure on $\mathbb{Z}_p^n$ such that $\mu(\mathbb{Z}_p^n) = 1$. In this section we will prove that

$$Z_p(f,s) = Q_p\left(f, \frac{1}{p^{n+s}}\right)(1 - p^s) + p^s. \tag{13}$$

We have only defined $Q_p(f,t)$ as a formal power series. The following lemma justifies the evaluation of complex t as in (13).

Lemma 3.4.1. *With the notation as above, the series of complex numbers*

$$\sum_{m=0}^{\infty} N_m t^m$$

converges for complex t in the open disk $\mathfrak{D} = \{z : |z| < p^{-n}\} \subset \mathbb{C}$ and hence the series defines a holomorphic function $\mathfrak{D} \to \mathbb{C}$.
In particular, for complex s with $\Re(s) > 0$ we have $p^{-n-s} \in \mathfrak{D}$ and the mapping $s \mapsto Q_p(f, p^{-n-s})$ defines a holomorphic map from the open right-half plane to $\mathbb{C}$.

Proof. Let $m \in \mathbb{Z}_{\geq 0}$ and $t \in \mathfrak{D}$. Then $N_m \leq |(\mathbb{Z}/p^m\mathbb{Z})^n| = p^{mn}$ so that

$$|N_m t^m| = N_m |t|^m \leq p^{nm}|t|^m = |p^n t|^m.$$

As $t \in \mathfrak{D}$ we have $|p^n t| < 1$ so the series $\sum_{m=0}^{\infty} N_m t^m$ converges by comparison with the geometric series $\sum_{m=0}^{\infty} |p^n t|^m$.
If s is such that $\Re(s) > 0$ we have $|p^{-n-s}| = p^{\Re(-n-s)} = p^{-n-\Re(s)} < p^{-n}$ so that indeed $p^{-n-s} \in \mathfrak{D}$. The map $s \mapsto Q_p(f, p^{-n-s})$ is then analytic by composition of two analytic functions, as the map $s \mapsto p^{-n-s}$ from the open right-half plane to $\mathfrak{D}$ is also analytic. □

The proof of (13) is based on the following lemma.

Lemma 3.4.2. *For $m \in \mathbb{Z}_{>0}$ consider $V_m := \{x \in \mathbb{Z}_p^n : |f(x)|_p \leq p^{-m}\}$. Then*

$$\mu(V_m) = \frac{N_m}{p^{nm}}.$$

Proof. Using the notation $x \bmod p^m := (x_1 \bmod p^m, \ldots, x_n \bmod p^m)$ for $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and $m \in \mathbb{Z}_{\geq 0}$ we have

$$\begin{aligned} V_m &= \{x \in \mathbb{Z}_p^n : |f(x)|_p \leq p^{-m}\} \\ &= \{x \in \mathbb{Z}_p^n : f(x) \equiv 0 \bmod p^m\} \\ &= \{x \in \mathbb{Z}_p^n : (f \bmod p^m)(x \bmod p^m) = 0 \bmod p^m\}. \end{aligned}$$

From this we see that for $x \in V_m$ we have $x \bmod p^m \subset V_m$. Note that $\mathbb{Z}_p^n$ is the disjoint union of cosets $s + (p^m\mathbb{Z}_p)^n$ for $s \in S$, with S a set of representatives for $(\mathbb{Z}_p/p^m\mathbb{Z}_p)^n$, for example $S = \{0, 1, \ldots, p^m - 1\}^n$. As $x + (p^m\mathbb{Z}_p)^n \subset V_m \subset \mathbb{Z}_p^n$ for any $x \in V_m$ we have a disjoint union

$$V_m = \bigcup_{s \in S'} s + (p^m\mathbb{Z}_p)^n,$$

where S' is some subset of S that has cardinality N_m. Using lemma 3.2.2 and translation invariance we see that

$$\mu(V_m) = \sum_{s \in S'} \mu(s + (p^m\mathbb{Z}_p)^n) = N_m \mu((p^m\mathbb{Z}_p)^n) = \frac{N_m}{p^{nm}}.$$ □

Proposition 3.4.3. *Let p be a prime number, $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and $s \in \mathbb{C}$ such that $\Re(s) > 0$. Then for the power series $Q_p(f, t) \in \mathbb{Q}[[t]]$ and Igusa's local zeta function $Z_p(f, s)$ we have*

$$Z_p(f, s) = Q_p\left(f, \frac{1}{p^{n+s}}\right)(1 - p^s) + p^s.$$

Here the evaluation of $Q_p(f, t)$ for complex t is as in lemma 3.4.1.

Proof. Letting $E_0, E_1, \ldots$ as in proposition 3.2.4 we see that $E_m = V_m \setminus V_{m+1}$ for $m \in \mathbb{Z}_{\geq 0}$. Using lemma 3.4.2 it follows that

$$\begin{aligned}
Z_p(f,s) &= \sum_{m=0}^{\infty} p^{-ms}\mu(E_m) = \sum_{k=0}^{\infty} \frac{1}{p^{ms}} \left(\frac{N_m}{p^{nm}} - \frac{N_{m+1}}{p^{n(m+1)}} \right) \\
&= \sum_{m=0}^{\infty} \frac{N_m}{p^{(n+s)m}} - \sum_{m=0}^{\infty} \frac{N_{m+1}}{p^{n(m+1)+ms}} \\
&= \sum_{m=0}^{\infty} N_m \left(\frac{1}{p^{n+s}} \right)^m - p^s \sum_{m=0}^{\infty} N_{m+1} \left(\frac{1}{p^{n+s}} \right)^{m+1} \\
&= Q_p\left(f, \frac{1}{p^{n+s}} \right) - p^s \left(Q_p\left(f, \frac{1}{p^{n+s}} \right) - 1 \right) \\
&= Q_p\left(f, \frac{1}{p^{n+s}} \right)(1-p^s) + p^s.
\end{aligned}$$

□

We have computed $Q_p(f,t)$ and $Z_p(f,s)$ for $f = X^d \in \mathbb{Z}_p[X]$ in examples 3.3.1 and 3.2.5. We verify proposition 3.4.3 for this f. We first rewrite $Q_p(f,t)$. From example 3.3.1 we have

$$\begin{aligned}
Q_p(f,t) &= \frac{1 + t + pt^2 + \cdots + p^{d-2}t^{d-1}}{1 - p^{d-1}t^d} = \frac{1 + t(1 + pt + \cdots + (pt)^{d-2})}{p - p^d t^d} \\
&= \frac{1 + t \cdot \frac{(pt)^{d-1}-1}{pt-1}}{1 - p^{d-1}t^d} = \frac{pt - t - 1 + p^{d-1}t^d}{(pt-1)(1-p^{d-1}t^d)}.
\end{aligned}$$

Letting $t = p^{-1-s}$ we have $pt = p^{-s}$, $p^{d-1}t^d = p^{d-1}p^{-d-ds} = p^{-1-sd}$ and $p^s = 1/pt$. Also note that $1 - p^s = (p^{-s} - 1)p^s$. From proposition 3.4.3 we then have

$$\begin{aligned}
Z_p(f,s) &= Q_p\left(f, \frac{1}{p^{1+s}} \right)(1-p^s) + p^s \\
&= \frac{p^{-s} - p^{-1-s} - 1 + p^{-1-sd}}{(p^{-s}-1)(1-p^{-1-sd})} \cdot (1-p^s) + p^s \\
&= \frac{1 - p^{-1} - p^s + p^{-1-sd+s} + p^s - p^{-1-sd+s}}{1 - p^{-1-sd}} \\
&= \frac{p-1}{p - p^{-sd}},
\end{aligned}$$

which checks with 3.2.5.

4 Rationality of the zeta function

4.1 Rationality and the Zeta function

For a prime number p and $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ we have defined $Q_p(f,t)$ as a formal power series in $\mathbb{Q}[[t]]$. The following theorem was first proven by Igusa [3].

Theorem 4.1.1. *The power series $Q_p(f,t)$ is a rational function in t.*

To be precise about this, note that we have the following diagram of inclusions.

$$\begin{array}{ccc} \mathbb{Q}[t] & \longrightarrow & \mathbb{Q}[[t]] \\ \downarrow & & \downarrow \\ \mathbb{Q}(t) & \longrightarrow & \mathbb{Q}((t)) \end{array} \tag{14}$$

The statement of theorem 4.1.1 means that $Q_p(f,t) \in \mathbb{Q}(t)$ as interpreted in diagram (14). An example of a power series being a rational function is the formal power series $1 + X + X^2 + \cdots = \frac{1}{1-X}$ as seen in corollary 1.5.4.

The proof of 4.1.1 is beyond the scope of this thesis. The roots of the polynomial $f \in \mathbb{Z}_p[X_1, \ldots, x_n]$ reduced mod p defines a variety in $\mathbb{A}^n$ over the field $\mathbb{F}_p$, and we will see that the rationality is easily shown if the hypersurface determined by $(f = 0 \bmod p)$ has no singularity. The general proof uses resolution of singularities to bypass the singularities and for this the relation with the local zeta function is useful: this resolution of singularities corresponds with a pullback and this operation behaves well with integrals through a change of variables substitution. See Popa [5] for the details.

We will in stead prove the rationality in the special case where there is no singularity and compute an example an example where there is a singularity. We also have the following result.

Theorem 4.1.2. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$. Then $Q_p(f,t) \in \mathbb{Q}(t)$ if and only if $Z_p(f,s)$ is a rational function of p^{-s} with coefficients in $\mathbb{Q}$.*

Proof. Let $s \in \mathbb{C}$ with $\Re(s) > 0$ and let $t := p^{-s}$. Then using proposition 3.4.3 we have

$$Z_p(f,s) - \frac{1}{t} = Q_p(f, p^{-n}t)\left(1 - \frac{1}{t}\right).$$

This yields

$$Q(f, p^{-n}t) = \frac{t}{t-1}\left(Z_p(f,s) - \frac{1}{t}\right) = \frac{tZ_p(f,s) - 1}{t-1}.$$

Thus, if $Z_p(f,s)$ is a rational function of $t = p^{-s}$ then so is $Q_p(f, p^{-n}t)$, say $Q_p(f, p^{-n}t) = \frac{q(t)}{q'(t)}$ for polynomial functions $q, q' : \mathbb{C} \to \mathbb{C}$ with rational coeffi-

cients. Then

$$Q_p(f,t) = \frac{q(p^n t)}{q'(p^n t)}$$

and hence $Q_p(f,t) \in \mathbb{Q}(t)$. The converse follows immediatly from 3.4.3. □

4.2 Rationality in the non-singular case

A straightforward method to compute $Q_p(f,t)$ and verify its rationality, is to first compute N_1 using the fact that $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field, and then to lift (improve) solutions mod p to solutions mod p^2, then to lift these solutions mod p^3 and so on.
This first step, the computation of N_1, is usually done through parametrisations. The second step of improving the solutions can be done in the following manner.

Note that if $x_1, \ldots, x_n \in \mathbb{Z}_p$ are such that $(x_1, \ldots, x_n) \bmod p^m$ is a root of $f \bmod p^m$, then we have

$$(f \bmod p^m)(x_1 \bmod p^m, \ldots, x_n \bmod p^m) = f(x_1, \ldots, x_n) \bmod p^m = 0 \bmod p^m.$$

This implies that $(x_1, \ldots, x_n) \bmod p^k$ is a root of $f \bmod p^k$ for any positive integer $k < m$. We can formalize this as follows.
Let $k \in \mathbb{Z}_{>0}$. As p^{k+1} is contained in the kernel of the natural map $\pi_k : \mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ we have a well defined map $\mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ given by $a \bmod p^{k+1} \mapsto a \bmod p^k$. Let $\varepsilon_k : (\mathbb{Z}/p^{k+1}\mathbb{Z})^n \to (\mathbb{Z}/p^k\mathbb{Z})^n$ be this map copied n times. If we let

$$E_m := \{x \in (\mathbb{Z}/p^m\mathbb{Z})^n : (f \bmod p^m)(x) = 0 \bmod p^m\}$$

then $N_m = |E_m|$, and the observation that a root $\bmod p^m$ is still a root $\bmod\ p^k$ for $k < m$ can be stated as $E_{m+1} \subset \varepsilon_m^{-1}(E_m)$.
We can use this to inductively find E_m. So if E_m is given for some $m \in \mathbb{Z}_{>0}$, we can subdivide E_{m+1} according to their image under ε_m. That is we have a disjoint union

$$E_{m+1} = \bigcup_{x \in E_m} (\varepsilon_m^{-1}(x) \cap E_{m+1}), \tag{15}$$

and hence

$$N_{m+1} = |E_{m+1}| = \sum_{x \in E_m} |\varepsilon_m^{-1}(x) \cap E_{m+1}|. \tag{16}$$

For $m \in \mathbb{Z}_{>0}$ we have that

$$\left\{ \sum_{i=0}^{m-1} a_i p^i : a_0, \ldots, a_{m-1} \in \{0, \ldots, p-1\} \right\}.$$

is a set of representatives for $\mathbb{Z}/p^m\mathbb{Z}$. Thus if $x \bmod p^m = \sum_{i=0}^{m-1} a_i p^i \bmod p^m \in \mathbb{Z}/p^m\mathbb{Z}$ is given, then for $y \bmod p^{m+1} = \sum_{i=0}^{m} b_i p^i \bmod p^{m+1} \in \mathbb{Z}/p^{m+1}\mathbb{Z}$ we

have $y \bmod p^m = x \bmod p^m$ if any only if $a_i = b_i$ for all $i \in \{0, 1, \ldots, m-1\}$. It follows that for

$$x = (x_1, \ldots, x_n) \bmod p^m = \left(\sum_{i=0}^{m-1} a_{1,i} p^i, \ldots, \sum_{i=0}^{m-1} a_{n,i} p^i \right) \bmod p^m \in E_m$$

we have

$$\varepsilon_m^{-1}(x) = \left\{ \left(\sum_{i=0}^{m} a_{1,i} p^i, \ldots, \sum_{i=0}^{m} a_{n,i} p^i \right) \bmod p^{m+1} : a_{1,m}, \ldots, a_{n,m} \in \{0, \ldots, p-1\} \right\}.$$

Thus for such fixed x we have that $|\varepsilon_m^{-1}(x) \cap E_{m+1}|$ equals the number of n-tuples $(a_{1,m}, \ldots, a_{n,m})$ in $\{0, \ldots, p-1\}^n$ for which

$$\left(\sum_{i=0}^{m} a_{1,i} p^i, \ldots, \sum_{i=0}^{m} a_{n,i} p^i \right) \bmod p^{m+1}$$

is a root of $f \bmod p^{m+1}$.

Example 4.2.1. *Suppose that $p \neq 2$ and consider $f = X^2 + Y^2 - 1 \in \mathbb{Z}_p[X, Y]$.*

Step 1. Determine N_1.
To do this we consider points $(x, y) \in \mathbb{F}_p^2$ on the line $y = tx + 1$ for $t \in \mathbb{F}_p$ and check which pairs (x, y) are a root of $f \bmod p$. For $x, y, t \in \mathbb{F}_p$ we have

$$x^2 + y^2 - 1 = x^2 + (tx + 1)^2 - 1 = (1 + t^2)x^2 + 2tx = [(1 + t^2)x + 2t]x = 0.$$

This has solution $x = \frac{-2t}{1+t^2}$ provided that $1 + t^2 \neq 0$. If this is the case we obtain $y = tx + 1 = \frac{-2t^2}{1+t^2} + 1 = \frac{1-t^2}{1+t^2}$, so we have the following map:

$$\varphi : \{t \in \mathbb{F}_p : 1 + t^2 \neq 0\} \to E_1 = \{(x, y) \in \mathbb{F}_p : x^2 + y^2 = 1\}$$
$$t \mapsto \left(\frac{-2t}{1 + t^2}, \frac{1 - t^2}{1 + t^2} \right).$$

I claim that this map is injective and that its image equals $E_1 \setminus \{(0, -1)\}$. Suppose that $\varphi(t) = \varphi(s) = (x, y)$ for certain $t, s \in \mathbb{F}_p$ such that $1 + t^2, 1 + s^2$ are non-zero. Then $y = tx + 1 = sx + 1$ so that $tx = sx$. For non-zero x this gives $t = s$ and for $x = 0$ we have

$$\frac{-2t}{1 + t^2} = \frac{-2s}{1 + s^2} = 0.$$

This gives $-2t = -2s$ so that $t = s$ as $p \neq 2$.
To determine the image of φ, note that we clearly have $\mathrm{Im}(\varphi) \subset E_1 \setminus \{(0, -1)\}$. For the converse, let $(x, y) \in E_1 \setminus \{(0, -1)\}$. If $x = 0$ then $y^2 = 1$. As $y \neq -1$ this gives $y = 1$ and it follows that $(x, y) = (0, 1) = \varphi(0)$. If $x \neq 0$ define

$t := (y-1)/x$. We need to show that $t^2+1 \neq 0$ and that $\varphi(t) = (x,y)$. As $x^2+y^2 = 1$ we have

$$t^2+1 = \frac{(y-1)^2}{x^2} + 1 = \frac{y^2-2y+1+x^2}{x^2} = \frac{2-2y}{x^2}.$$

If we would have $t^2+1=0$ then this gives $y=1$. As $x^2+y^2=1$ this implies $x^2=0$ which is a contradiction as $x \neq 0$. It follows that $1+t^2 \neq 0$. It remains to verify that $\varphi(t) = (x,y)$ and this follows by a routine calculation:

$$\begin{aligned}\varphi(t) &= \left(\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right) \\ &= \left(\frac{-2(y-1)/x}{(2-2y)/x^2}, \frac{(x^2-y^2+2y-1)/x^2}{(2-2y)/x^2}\right) \\ &= \left(\frac{(2-2y)x}{2-2y}, \frac{-2y^2+2y}{2-2y}\right) = (x,y).\end{aligned}$$

This proves that the image of φ equals $E_1 \setminus \{(0,-1)\}$.
We have $N_1 = |E_1| = 1 + |\{t \in \mathbb{F}_p : 1+t^2 \neq 0\}|$, so to determine N_1 we need to determine how many $t \in \mathbb{F}_p$ exist such that $t^2+1=0$. Note that there can be at most 2 as the polynomial $X^2+1 \in \mathbb{F}_p[X]$ can have at most 2 zero's, and if $t \in \mathbb{F}_p$ is a zero then $-t$ is the other zero (note that $t \neq -t$ as $p \neq 2$). Thus either there exists no such t or there exist 2.
I claim that such a t exists, i.e. -1 is a square in $\mathbb{F}_p^*$, if and only if $p \equiv 1 \bmod 4$. If such a t exists then t has order 4 in the group $\mathbb{F}_p^*$ so 4 divides $|\mathbb{F}_p^*| = p-1$, that is $p \equiv 1 \bmod 4$.
Conversely, suppose that $p \equiv 1 \bmod 4$. Write $p-1 = 4k$ for $k \in \mathbb{Z}_{>0}$ and let $g \in \mathbb{F}_p^*$ be a generator for the cyclic group $\mathbb{F}_p^*$, i.e. g has order $p-1=4k$. Then $t := g^k$ has order 4 so that $0 = t^4-1 = (t^2-1)(t^2+1)$. As $t^2-1 \neq 0$ this implies that $t^2+1=0$ as desired. It follows that

$$N_1 = 1 + |\{t \in \mathbb{F}_p : 1+t^2 \neq 0\}| = \begin{cases} p-1 & \text{if } p \equiv 1 \bmod 4 \\ p+1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

Step 2. Lift solutions.
Suppose that for some $m \in \mathbb{Z}_{>0}$ we have that N_m is given. Let $(x,y) \bmod p^m = (\sum_{n=0}^{m-1} a_n p^n, \sum_{n=0}^{m-1} b_n p^n) \bmod p^m$ be a root of $f \bmod p^m$, i.e. $(x,y) \bmod p^m \in E_m$. Then according to the above, the number of roots of $f \bmod p^{m+1}$ that reduce to $(x,y) \bmod p^m$, i.e. $|\varepsilon_m^{-1}((x,y) \bmod p^m) \cap E_{m+1}|$, equals the number of pairs $(a_m, b_m) \in \{0,\ldots,p-1\}^2$ such that $(\sum_{n=0}^{m} a_n p^n, \sum_{n=0}^{m} b_n p^n) \bmod p^m$ is a root of $f \bmod p^{m+1}$.
Let $(a_m, b_m) \in \{0,\ldots,p-1\}$ and write $x_k = \sum_{n=0}^{k} a_n p^n$ and $y_k = \sum_{n=0}^{k} b_n p^n$ for $k = 0,1,\ldots,m$. Then as $(x,y) \bmod p^m = (x_{m-1}, y_{m-1}) \bmod p^m$ is a root of $f \bmod p^m$ we have $x_{m-1}^2 + y_{m-1}^2 - 1 = kp^m$ for some $k \in \mathbb{Z}$. Calculating

mod p^{m+1} we have

$$\begin{aligned} x_m^2 + y_m^2 - 1 &= (x_{m-1} + a_m p^m)^2 + (y_{m-1} + b_m p^m)^2 - 1 \\ &= x_{m-1}^2 + y_{m-1}^2 - 1 + 2a_m x_{m-1} p^m + 2b_m y_{m-1} p^m + (a_m^2 + b_m^2) p^{2m} \\ &= (k + 2a_m a_0 + 2b_m b_0) p^m \pmod{p^{m+1}}. \end{aligned}$$

Thus we have $x_m^2 + y_m^2 - 1 \equiv 0 \bmod p^{m+1}$ if and only if $k + 2a_m a_0 + 2b_m b_0 \equiv 0 \bmod p$.
Assume that $a_0 \neq 0 \bmod p$. Then for b_m arbitrary we can solve $\overline{k + 2a_m a_0 + 2b_m b_0} = \overline{0}$ in $\mathbb{F}_p$ for $\overline{a_m}$:

$$\overline{a_m} = \frac{\overline{-k - 2b_m b_0}}{\overline{2a_0}}.$$

Thus we have p possible choices for (a_m, b_m) in this case. If $a_0 \equiv 0 \bmod p$ then $b_0 \not\equiv 0 \bmod p$ so that for a_m arbitrary, we can solve $\overline{k + 2a_m a_0 + 2b_m b_0} = \overline{0}$ for $\overline{b_m}$:

$$\overline{b_m} = \frac{\overline{-k - 2a_m a_0}}{\overline{2b_0}}.$$

And hence in this case we also have p possibilities for (a_m, b_m). Thus we have $N_{k+1} = pN_k$ and hence inductively we find $N_{k+1} = p^k N_1$ for $k \in \mathbb{Z}_{>0}$.

Step 3. Compute $Q_p(f, t)$.

$$\begin{aligned} Q_p(f,t) &= 1 + N_1 t + N_2 t^2 + N_3 t^3 + \cdots \\ &= 1 + N_1 t + p N_1 t^2 + p^2 N_1 t^3 + \cdots \\ &= 1 + N_1 t (1 + pt + (pt)^2 + \cdots) = 1 + \frac{N_1 t}{1 - pt} = \frac{1 - pt + N_1 t}{1 - pt}. \end{aligned}$$

We have $1 - pt + (p \pm 1)t = 1 \pm t$ so that

$$Q_p(f,t) = \begin{cases} \frac{1-t}{1-pt} & \text{if } p \equiv 1 \bmod 4 \\ \frac{1+t}{1-pt} & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

The lifting of the solutions in this example is very well behaved and this is due to the fact that each point on the circle over $\mathbb{F}_p$ has a well defined tangent line.

Lemma 4.2.2. *Let $f \in R[X_1, \ldots, X_n]$ and let $a = (a_1, \ldots, a_n) \in R^n$ for a ring R. Then there exists $g \in (X_1 - a_1, \ldots, X_n - a_n)^2$ such that*

$$f = f(a) + \frac{\partial f}{\partial X_1}(a)(X_1 - a_1) + \cdots + \frac{\partial f}{\partial X_n}(a)(X_n - a_n) + g.$$

Proof. We have a ring isomorphism $\Phi : R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n]$ determined by $X_i \mapsto X_i - a_i$, so there exists $g \in R[X_1, \ldots, X_n]$ such that $f = \Phi(g)$. This just means that we can write f as a polynomial in the variables $X_i - a_i$:

$$f = \sum_{i_1, \ldots, i_n} r_{i_1, \ldots, i_n} (X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$$

for certain $r_{i_1,\ldots,i_n} \in R$, and $(i_1,\ldots,i_n)$ running through a finite subset of $\mathbb{Z}^n_{\geq 0}$. Define

$$g := \sum_{\substack{i_1,\ldots,i_n:\\ i_1+\cdots+i_n\geq 2}} r_{i_1,\ldots,i_n}(X_1-a_1)^{i_1}\cdots(X_n-a_n)^{i_n}.$$

Then $g \in (X_1-a_1,\ldots,X_n-a_n)^2$ and we have

$$f = r_{0,\ldots,0} + r_{1,\ldots,0}(X_1-a_1) + \cdots + r_{0,\ldots,1}(X_n-a_1) + g.$$

Evaluating $a=(a_1,\ldots,a_n)$ results in $f(a) = r_{0,\ldots,0}$, and evaluating a in

$$\frac{\partial f}{\partial X_i} = r_{0,\ldots,i,\ldots,0} + \frac{\partial g}{\partial X_i}$$

results in $r_{0,\ldots,i,\ldots,0} = \frac{\partial f}{\partial X_i}(a)$. This completes the proof. □

Proposition 4.2.3. *Let $f \in \mathbb{Z}_p[X_1,\ldots,X_n]$ and let $a \bmod p = (a_1,\ldots,a_n) \bmod p$ be a root of $f \bmod p$ for which*

$$\nabla f(a) = \left(\frac{\partial f}{\partial X_1}(a),\ldots,\frac{\partial f}{\partial X_n}(a)\right) \neq (0,\ldots,0) \bmod p.$$

That is the gradient is non-zero. Then if $x \bmod p^m$ is a root of $f \bmod p^m$ that lies over $a \bmod p$, i.e. $x \bmod p = a \bmod p$, then there are precisely p^{n-1} roots of $f \bmod p^{m+1}$ that lie over $x \bmod p^m$.

Proof. As $x \bmod p^m$ is a roof of $f \bmod p^m$ we can assume that $x=(x_1,\ldots,x_n)$ for $x_i \in \{0,\ldots,p^m-1\}$. Using lemma 4.2.2 we can write

$$f = f(x) + \frac{\partial f}{\partial X_1}(x)(X_1-x_1) + \cdots + \frac{\partial f}{\partial X_n}(x)(X_n-x_n) + g. \tag{17}$$

for some $g \in (X_1-x_1,\ldots,X_n-x_n)^2$. A lift of $x \bmod p^m$ to $(\mathbb{Z}/p^{m+1}\mathbb{Z})^n$ is of the form

$$y \bmod p^{m+1} = (x_1+p^m y_1,\ldots,x_n+p^m y_n) \bmod p^{m+1}$$

for certain $y_i \in \{0,\ldots,p-1\}$. We need to show that number of n-tuples $(y_1,\ldots,y_n)$ for which $y \bmod p^{m+1}$ is a root of $f \bmod p^{m+1}$ is equal to p^{n-1}. Note that g is linear combination of polynomials of the form $(X_i-x_i)(X_j-x_j)$. Evaluating y in such a polynomial gives

$$(x_i+p^m y_i - x_i)(x_j+p^m y_j - x_j) = y_i y_j p^{2m} \equiv 0 \bmod p^{m+1}.$$

It follows that $g(y) \equiv 0 \bmod p^{m+1}$. Let $k \in \mathbb{Z}$ be such that $f(x) = kp^m$. We then have

$$\begin{aligned} f(y) \bmod p^{m+1} &= kp^m + \frac{\partial f}{\partial X_1}(x)p^m y_1 + \cdots + \frac{\partial f}{\partial X_n}(x)p^m y_n \bmod p^{m+1} \\ &= \left(k + \frac{\partial f}{\partial X_1}(x)y_1 + \cdots + \frac{\partial f}{\partial X_n}(x)y_n\right)p^m \bmod p^{m+1} \end{aligned}$$

It follows that y is a root of $f \bmod p^{m+1}$ if and only if

$$k + \frac{\partial f}{\partial X_1}(x)y_1 + \cdots + \frac{\partial f}{\partial X_n}(x)y_n \equiv 0 \bmod p. \tag{18}$$

Note that $x \bmod p = a \bmod p$ so that $\frac{\partial f}{\partial X_1}(x) \bmod p = \frac{\partial f}{\partial X_1}(a) \bmod p$. By assumption we have $\frac{\partial f}{\partial X_i}(a) \not\equiv 0 \bmod p$ for some $i \in \{1, \ldots, n\}$. Without loss of generatity assume that $i = 1$ (the argument is the same for $i \neq 1$). We can then rewrite (18) as

$$y_1 \bmod p = \frac{-k - \frac{\partial f}{\partial X_2}(a)y_2 - \cdots - \frac{\partial f}{\partial X_n}(a)y_n \bmod p}{\frac{\partial f}{\partial X_1}(a) \bmod p}.$$

And this completely determines y_1 for arbitary $(y_2, \ldots, y_n)$. As there are p^{n-1} possibilities for $(y_2, \ldots, y_n)$ this completes the proof. □

Corollary 4.2.4. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and suppose $N_1 \neq 0$ and that $\nabla f(a) \bmod p$ is non-zero for all roots $a \bmod p$ of $f \bmod p$.*
Then $Q_p(f, t)$ is a rational function; it is given by

$$Q_p(f, t) = \frac{1 + N_1 t - p^{n-1}t}{1 - p^{n-1}t}.$$

Proof. Suppose inductively that N_m is given for some $m \in \mathbb{Z}_{>0}$. Then for each root $x \bmod p^m$ of $f \bmod p^m$ there are p^{n-1} roots of $f \bmod p^{m+1}$ that reduce to $x \bmod p^m$ as $\nabla f(x) \bmod p \neq 0 \bmod p$. Because there are N_m such roots we obtain $N_{m+1} = p^{n-1}N_m$. Inductively we find that $N_{m+1} = p^{m(n-1)}N_1$ for $m \in \mathbb{Z}_{\geq 0}$ and hence

$$\begin{aligned} Q_p(f, t) &= 1 + N_1 t + p^{n-1}N_1 t^2 + p^{2(n-1)}N_1 t^3 + \cdots \\ &= 1 + N_1 t \left(1 + p^{n-1}t + (p^{n-1}t)^2 + \cdots\right) \\ &= 1 + \frac{N_1 t}{1 - p^{n-1}t} = \frac{1 + N_1 t - p^{n-1}t}{1 - p^{n-1}t}. \end{aligned}$$

□

The proof of proposition 4.2.3 also gives useful information when the hypothesis of the gradient are not satisfied, i.e. if one does have $\nabla f(a) \equiv (0, \ldots, 0) \bmod p$. Equation (18) is valid regardless, and (with the notation of the proposition) one sees that $y \bmod p^{m+1}$ is a root of $f \bmod p^{m+1}$ if and only $k \equiv 0 \bmod p$, i.e. $f(x) \equiv 0 \bmod p^{m+1}$. In this case any lift is a root $\bmod\ p^{m+1}$ and if it is not the case then $f \bmod p^{m+1}$ has no root that reduces to $x \bmod p^m$. We summarize this in the following corollary.

Corollary 4.2.5. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ and let $a \bmod p = (a_1, \ldots, a_n) \bmod p$ be a root of $f \bmod p$ for which*

$$\nabla f(a) = \left(\frac{\partial f}{\partial X_1}(a), \ldots, \frac{\partial f}{\partial X_n}(a)\right) \equiv (0, \ldots, 0) \bmod p.$$

Then if $x \bmod p^m$ is a root of $f \bmod p^m$ such that $x \bmod p = a \bmod p$, then there are p^n roots of $f \bmod p^{m+1}$ that lie over $x \bmod p^m$ provided that $f(x) \equiv 0 \bmod p^{m+1}$. If $f(x) \not\equiv 0 \bmod p^{m+1}$ then there are no roots of $f \bmod p^{m+1}$ lying over $x \bmod p^m$.

4.3 An example with a singularity over $\mathbb{F}_p$

We now consider the polynomial $f = Y^2 - X^3 \in \mathbb{Z}_p[X, Y]$. We first determine N_1, i.e. the number of roots of $f \bmod p$.

Step 1. Determine N_1.
Let $E_1 := \{(x, y) \in \mathbb{F}_p^2 : y^2 - x^3 = 0\}$ and consider the map $\varphi : \mathbb{F}_p \to E_1$ given by $t \mapsto (t^2, t^3)$. This is well defined as $(t^2)^3 = (t^3)^2$ for $t \in \mathbb{F}_p$. I claim that φ is a bijection so that $N_1 = |E_1| = p$.
Suppose that $t, s \in \mathbb{F}_p$ are such that $(x, y) = \varphi(t) = \varphi(s)$. From $t^2 = s^2$ we see that $(t, s) = (0, 0)$ if either t or s equals 0 so in this case we clearly have $t = s$. If t and s are both non-zero, let $x = t/s \in \mathbb{F}_p^*$. Then $x^2 = t^2/s^2 = 1$ and $x^3 = t^3/s^3 = 1$. It follows that $\mathrm{ord}(x)|2$ and $\mathrm{ord}(x)|3$ so that $\mathrm{ord}(x) = 1$, i.e $x = 1$, or $t = s$. This shows that φ is injective.

To prove that it is surjective let $(x, y) \in E_1$ be arbitary. If $x = 0$ then $y^2 = 0$ so that $y = 0$ and hence $(x, y) = (0, 0) = \varphi(0)$.
If $x \neq 0$ let$t = y/x$. Then

$$t^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x \quad \text{and} \quad t^3 = \frac{y^3}{x^3} = \frac{y^3}{y^2} = y.$$

Thus we have $(x, y) = (t^2, t^3) = \varphi(t)$ and hence φ is surjective. It follows $N_1 = p$.

Step 2. Lift solutions.
We have $\frac{\partial f}{\partial X} = -3X^2$ and $\frac{\partial f}{Y} = 2Y$. Thus for $a \bmod p$ we have $\left(\frac{\partial f}{\partial X}(a), \frac{\partial f}{\partial Y}(a)\right) \equiv (0, 0) \bmod p$ if and only if $a \bmod p = (0, 0) \bmod p$.
To compute N_m for $m > 1$ we subdivide the roots of $f \bmod p^m$ according to wether they reduce to $(0, 0) \bmod p$ or not.
We have $p - 1$ roots of $f \bmod p$ unequal to $(0, 0) \bmod p$. For each of these there are p lifts to roots of $f \bmod p^2$ by proposition 4.2.3 so there are $p(p - 1)$ roots of $f \bmod p^2$ that do not lie over $(0, 0) \bmod p$. Again each of these has p lifts to roots of $f \bmod p^3$, and so on. Inductively we find that for $m \geq 1$ there are $p^{m-1}(p - 1)$ roots of $f \bmod p^m$ that do not reduce to $(0, 0) \bmod p$.

It remains to determine the number of roots of $f \bmod p^m$ over $(0, 0) \bmod p$. To ease the notation, let R_m denote the number of roots of $f \bmod p^m$ over $(0, 0) \bmod p$, so that $N_m = R_m + p^{m-1}(p - 1)$ for $m \in \mathbb{Z}_{>0}$.
We have that $(0, 0) \bmod p^2$ is a root of $f \bmod p^2$ so using corollary 4.2.5 we see that all p^2 lifts $(a_1 p, b_1 p) \bmod p^2$ of $(0, 0) \bmod p$ are roots of $f \bmod p^2$. It follows that $N_2 = p^2 + p(p - 1) = 2p^2 - p$.

To determine N_3 we need to find the roots of $f \bmod p^2$ that produce roots of $f \bmod p^3$ as in corollary 4.2.5. These roots are of the form $(a_1 p, b_1 p) \bmod p^2$. We then have

$$(b_1 p)^2 - (a_1 p)^3 \bmod p^3 = b_1^2 p^2 \bmod p^3.$$

This equals $0 \bmod p^3$ if and only if $b_1 = 0$. Thus there are p such roots (as we have p possibilities for a_1), and each of these roots gives p^2 lifts so we have p^3 roots of $f \bmod p^3$ over $(0,0) \bmod p$ and hence $R_3 = p^3$.
For N_4 we determine which of the roots $(a_1 p + a_2 p^2, b_2 p^2) \bmod p^3$ produce roots of $f \bmod p^4$:

$$(b_2 p^2)^2 - (a_1 p + a_2 p^2)^3 \bmod p^4 = -a_1^3 p^3 \bmod p^4.$$

This equals $0 \bmod p^4$ if and only if $a_1 = 0$ and hence we have p^2 such roots, and hence p^4 roots of $f \bmod p^4$ over $(0,0) \bmod p$. Thus we have $R_4 = p^4$. Continuing, we take a root $(a_2 p^2 + a_3 p^3, b_2 p^2 + b_3 p^3) \bmod p^4$ of $f \bmod p^4$:

$$(b_2 p^2 + b_3 p^3)^2 - (a_2 p^2 + a_3 p^3)^3 \bmod p^5 = b_2^2 p^4 \bmod p^5.$$

So we have the condition $b_2 = 0$ and we find $R_5 = p^5$. Continuing we have

$$(b_3 p^3 + b_4 p^4)^2 - (a_2 p^2 + a_3 p^3 + a_4 p^4)^3 \bmod p^6 = 0 \bmod p^6.$$

So this time we dont get a condition like $a_i = 0$ or $b_i = 0$, and all the lifts produce roots of $f \bmod p^6$, and we obtain $R_6 = p^7$. For N_7 we have

$$(b_3 p^3 + b_4 p^4 + b_5 p^5)^2 - (a_2 p^2 + a_3 p^3 + a_4 p^4 + a_5 p^5)^3 \bmod p^7 = (b_3^2 - a_2^3) p^6 \bmod p^7.$$

Hence in this case we get the condition $(a_2, b_3) = (0,0)$. So of the p^7 roots, only p^5 provide roots of $f \bmod p^7$, each providing p^2 so we get $R_7 = p^7$. Continuing we get no condition on the coefficients and hence $R_8 = p^9$. Note that one obtains a condition on the b_i every two steps due to the exponent 2 and a condition on the a_i every three steps due to the exponent 3. Specifically, one finds with induction that

$$\begin{aligned} R_{6q} &= p^{7q} \\ R_{1+6q} &= p^{7q} \\ R_{2+6q} &= p^{2+7q} \\ R_{3+6q} &= p^{3+7q} \\ R_{4+6q} &= p^{4+7q} \\ R_{5+6q} &= p^{5+7q} \end{aligned}$$

Here $q \in \mathbb{Z}_{\geq 0}$ except for R_{6q} where we have $q \neq 0$.

Step 3. Compute $Q_p(f,t)$.

$$Q_p(f,t) = 1 + pt + \sum_{q=1}^{\infty} N_{6q} t^{6q} + \sum_{q=1}^{\infty} N_{6q+1} t^{6q+1} + \sum_{r=2}^{5} \sum_{q=0}^{\infty} N_{6q+r} t^{6q+r}$$

We have

$$\sum_{q=1}^{\infty} N_{6q}t^{6q} = \sum_{q=1}^{\infty}(p^{7q} + p^{6q-1}(p-1))t^{6q} = \sum_{q=1}^{\infty}(p^7t^6)^q + \frac{p-1}{p}\sum_{q=1}^{\infty}(p^6t^6)^q$$
$$= \frac{p^7t^6}{1-p^7t^6} + \frac{(p-1)p^6t^6}{p-p^7t^6} = \frac{(p^7+p^6-p^5)t^6}{1-p^6t^6}.$$

$$\sum_{q=1}^{\infty} N_{6q+1}t^{6q+1} = \sum_{q=1}^{\infty}(p^{7q} + p^{6q}(p-1))t^{6q+1} = t\sum_{q=1}^{\infty}(p^7t^6)^q + (p-1)t\sum_{q=1}^{\infty}(p^6t^6)^q$$
$$= \frac{p^7t^7}{1-p^7t^6} + \frac{(p-1)p^6t^7}{1-p^6t^6} = \frac{(2p^7-p^6)t^7}{1-p^7t^6}.$$

For $r \in \{2,3,4,5\}$ we have

$$\sum_{q=0}^{\infty} N_{6q+r}t^{6q+r} = \sum_{q=0}^{\infty}(p^{7q+r} + p^{6q+r}(p-1))t^{6q+r} = p^rt^t\sum_{q=0}^{\infty}(p^7t^6)^q + (p^6t^6)^q$$
$$= \frac{p^rt^r}{1-p^7t^6} + \frac{p^rt^r}{1-p^6t^6}.$$

Combining this we obtain

$$Q_p(f,t) = 1 + pt + \frac{p^7+p^6+p^5)t^6}{1-p^6t^6} + \frac{2p^7-p^6)t^7}{1-p^7t^6}$$
$$+ \frac{p^2t^2+p^3t^3+p^4t^4+p^5t^5}{1-p^7t^6} + \frac{p^2t^2+p^3t^3+p^4t^4+p^5t^5}{1-p^6t^6}.$$

And thus for this f we also see that $Q_p(f,t)$ is a rational function.

4.4 Conclusion

In the first two chapters we have constructed the field of p-adic numbers $\mathbb{Q}_p$ and the ring of p-adic integers $\mathbb{Z}_p$. We then defined Igusa's local Zeta function $Z_p(f,s)$ using a p-adic integral and linked this function to the power series $Q_p(f,t)$. We saw that rationality of $Q_p(f,t)$ is equivalent to the rationality of $Z_p(f,s)$ in p^{-s} and that in the absence of singularities the rationality follows in a straightforward manner through lifting of the roots.

References

[1] J. Denef, *Report on Igusa's local Zeta function*. Séminaire Bourbaki Astérsique 201 − 203 (1991) p.359-386.

[2] J. Denef, *On the degree of Igusa's local Zeta function*. American Journal of Mathematics 109 (1987), p.991-1008.

[3] J. Igusa, *Introduction to the theory of local zeta functions*. Studies in Advanced Mathematics 14, 2000.

[4] J. Gleason, *Existence and Uniqueness of Haar measure*. Paper found at http://www.math.uchicago.edu/∼may/VIGRE/VIGRE2010/REUPapers/Gleason.pdf

[5] M. Popa, *Chapter 3: p-adic integration*. Online course notes found at http://www.math.northwestern.edu/∼mpopa/571/index.html, 2011.

[6] M. Reid, *Undergraduate Commutative Algebra*. Cambridge University-Press, 1995.

[7] A. M. Robert, *A Course in p-adic Analysis*. Springer, 2007.

[8] W. Rudin, *Real and Complex Analysis*. McGraw-Hill Book Company, 1970.

[9] P. Stevenhagen, *Voortgezette Getaltheorie*. Thomas Stieltjes Instituut, 2002.