An introduction to Skolem's p-adic method for solving Diophantine equations

Josha Box

July 3, 2014

Bachelor thesis

Supervisor: dr. Sander Dahmen

Korteweg-de Vries Instituut voor Wiskunde
Faculteit der Natuurwetenschappen, Wiskunde en Informatica
Universiteit van Amsterdam

Abstract

In this thesis, an introduction to Skolem's p-adic method for solving Diophantine equations is given. The main theorems that are proven give explicit algorithms for computing bounds for the amount of integer solutions of special Diophantine equations of the kind $f(x, y) = 1$, where $f \in \mathbb{Z}[x, y]$ is an irreducible form of degree 3 or 4 such that the ring of integers of the associated number field has one fundamental unit. In the first chapter, an introduction to algebraic number theory is presented, which includes Minkovski's theorem and Dirichlet's unit theorem. An introduction to p-adic numbers is given in the second chapter, ending with the proof of the p-adic Weierstrass preparation theorem. The theory of the first two chapters is then used to apply Skolem's method in Chapter 3.

Title: An introduction to Skolem's p-adic method for solving Diophantine equations
Author: Josha Box, joshabox@msn.com, 10206140
Supervisor: dr. Sander Dahmen
Second grader: Prof. dr. Jan de Boer
Date: July 3, 2014

Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
Science Park 904, 1098 XH Amsterdam
`http://www.science.uva.nl/math`

Contents

Introduction

One of the greatest recent achievements of a single mathematician may well have been Andrew Wiles' proof of Fermat's Last Theorem. In 1995 Wiles published his final paper, after having devoted seven years of his life to the problem. The theorem states that for any integer $n > 2$, there are no non-trivial integer solutions (x, y, z) to the equation

$$x^n + y^n = z^n.$$

Of course, for $n = 2$ solving the Fermat equation is nothing else than finding Pythagorean triples, of which we know there exist infinitely many. How should one prove such a fact? In the case of finding infinitely many Pythagorean triples, it suffices to notice that $(3, 4, 5)$ is a solution, which implies that $(3n, 4n, 5n)$ is also a solution for every integer $n \geq 1$. Wiles, however, had much more difficulty proving the non-existence of non-trivial solutions for $n > 2$. In general, if n is a natural number, $A \in \mathbb{Z}$ and $f \in \mathbb{Z}[x_1, \ldots, x_n]$, then an equation of the kind

$$f(x_1, \ldots, x_n) = A$$

for which integer solutions $(x_1, \ldots, x_n)$ are searched, is called a *Diophantine equation*. In particular, Fermat's equation is Diophantine for every natural number n. The word Diophantine is derived from the Hellenistic mathematician Diophantus, who studied such equations in the third century AD. It was inside the margin of Diophantus' book *Arithmetica* that Pierre de Fermat scribbled his famous words

> *"If an integer n is greater than 2, then $x^n + y^n = z^n$ has no solutions in non-zero integers x, y, and z. I have a truly marvelous proof of this proposition which this margin is too narrow to contain."*

Mathematicians have tried to find Fermat's "marvelous proof" ever since, without any success. Though Wiles did eventually prove the theorem in 1995, his proof uses techniques that could not have been known by Fermat in 1621. Therefore, most mathematicians agree that Fermat had likely made a mistake in his proof. Avoiding the details, one could say that Wiles used a modern number theoretic approach to his class of Diophantine equations. Ever since Diophantus, and probably long before that as well, mathematicians have been occupied by Diophantine equations. In the past, this amounted to solving one such equation at a time. However, in the 20th century, new techniques allowed mathematicians to successfully solve entire classes of Diophantine equations.

In this thesis one such technique, called *Skolem's p-adic method*, is investigated. This is done in Chapter 3, while the required prerequisite knowledge is studied in Chapters

1 and 2. In Chapter 1, an introduction to algebraic number theory is presented, while Chapter 2 is devoted to p-adic numbers. Algebraic number theory can be viewed as a foundation for most modern methods for solving Diophantine equations. Also, many recent methods, including Wiles' proof of Fermat's Last Theorem, use p-adic numbers.

In Chapter 1, the prerequisites and introductory theory are presented in the first two sections. The latter sections focus on proving the unique decomposition of ideals of the ring of integers into prime ideals, Minkowski's theorem and Dirichlet's unit theorem.

Furthermore, in Chapter 2 the p-adic numbers are defined and an algebraically closed complete extension is. The main result of this chapter is the p-adic Weierstrass preparation theorem, of which Strassmann's theorem is found to be an immediate corollary. Together with Dirichlet's unit theorem, one could say that Strassmann's theorem is at the heart of Skolem's method described in Chapter 3.

Motivations

Parts of my own motivations for choosing the subjects of my thesis have been very well described by the German mathematician Richard Dedekind:

> *"The greatest and most fruitful progress in mathematics and other sciences is through the creation and introduction of new concepts; those to which we are impelled by the frequent recurrence of compound phenomena which are only understood with great difficulty in the older view."*

In other words, I wanted to learn many new concepts and ideas. Therefore, I chose not to follow the shortest path towards solving Diophantine equations. Instead, I first dug deep into the algebraic and p-adic number theory, without continuously keeping their applications to Diophantine equations in mind. Section 2.3 is an example of a piece of theory that is not strictly necessary prerequisite knowledge for the methods applied in Chapter 3, while in my opinion the information contributes significantly to the understanding of the p-adic numbers.

The idea of studying Skolem's p-adic method for solving Diophantine equations was proposed by my supervisor, who focuses on Diophantine equations in his own research as well. What fascinated me about Diophantine equations is that they are so accessible that I would be able to explain their meaning to, say, my grandmother, while mathematicians are often only able to say something about them using very advanced mathematics. To me it seemed a challenge to be able to understand such a sophisticated technique. Moreover, I had already enjoyed studying the first three chapters of Algebraic Number Theory and Fermat's Last Theorem by Stewart and Tall [16] in the honours extension of the course Algebra 2 and was therefore eager to learn more algebraic number theory as well. Furthermore, the theory of p-adic numbers was exactly one of those new concepts and ideas that Dedekind spoke of and it fascinated me that such an extraordinary idea had had such far-reaching implications.

1 Number theory

In this chapter we will explore the number theory that is necessary for studying Diophantine equations in Chapter 3. Also, some examples of direct applications of the theory to suitable Diophantine equations are given in this chapter. Number theory is one of the oldest fields of mathematics and studies, in essence, the integers. The language in which the integers and its generalizations are studied is that of algebra. Therefore,the reader should have prerequisite knowledge of ring and field theory, group theory and some Galois theory. The theory as described in [4], [5] and [6] should be sufficient for understanding this chapter.

1.1 Prerequisite knowledge

In this section, the important theory for understanding this chapter that the reader will be least likely to have come across is explained. Most of these facts are related to free abelian groups. We will frequently encounter such groups throughout this chapter.

Definition 1.1. If G is an abelian group such that there exist $g_1, \ldots, g_n \in G$ that generate G and are linearly independent over $\mathbb{Z}$, then G is called *free abelian of rank n.*

The rank of a free abelian group is, similar to the dimension of a vector space in linear algebra, well-defined and any $g \in G$ can be expressed in a unique way as $g = a_1 g_1 + \ldots + a_n g_n$, where $a_i \in \mathbb{Z}$ for each i. A $\mathbb{Z}$- linearly independent set generating G is also called a *basis.*

Lemma 1.2. *If G is free abelian of rank n with basis $\{x_1, \ldots, x_n\}$ and $A = (a_{ij})$ is an $n \times n$ $\mathbb{Z}$-matrix, then the elements $y_i = \sum_j a_{ij} x_j$ form a basis for G if and only if A is* unimodular*, i.e.* $\det A = \pm 1$.

Proof. Let $x = (x_1, \ldots, x_n)^T$ and $y = (y_1, \ldots, y_n)^T$. Suppose that the y_i form a basis. Then there exist matrices B and C such that $x = By$ and $y = Cx$, so $BC = I_n$ and the result follows.

If A is unimodular, we can write $\pm A^{-1} = \det(A) \cdot A^{-1} = \tilde{A}$, the adjoint matrix of A which has integer coefficients. Hence A^{-1} has integer entries and we are done. □

Theorem 1.3. *If H is a subgroup of a free abelian group G of rank n, then H is free abelian of rank $s \leq n$ and there exists a basis $\{v_1, \ldots, v_n\}$ for G and positive integers $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}_{>0}$ such that $\{\alpha_1 v_1, \ldots \alpha_s v_s\}$ is a basis for H.*

A proof by induction on n can be found in [16].

Theorem 1.4. *If G is free abelian of rank r with a subgroup H, then G/H is finite if and only if the rank of H equals r. Moreover, if this is the case and we have $\mathbb{Z}$-bases $\{x_1, \ldots, x_r\}$ for G and $\{y_1, \ldots, y_r\}$ for H such that $y_i = \sum_j a_{ij} x_j$, then $|G/H| = |\det(a_{ij})|$.*

Proof. If the rank of H is s then we can use Theorem 1.3 to find a basis $\{v_1, \ldots, v_n\}$ of G and $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}$ such that the $u_i = \alpha_i v_i$ $(1 \leq i \leq s)$ form a basis for H. Then G/H is the direct product of s cyclic groups of orders α_i and $r - s$ infinite cyclic groups and we have $r = s$ if and only if G/H is finite.

In that case, $|G/H| = \alpha_1 \cdots \alpha_r$. Define $u = (u_1, \ldots, u_r)^T$, $v = (v_1, \ldots, v_r)^T$ and the vectors x and y likewise. By writing the different elements into the different bases, we find matrices A, B, C, D such that $y = Ax$, $u = Bx$, $v = Cu$ and $y = Dv$. By Lemma 1.2, B and D are unimodular. Also, C is diagonal with $c_{ii} = \alpha_i$ and $A = BCD$ by consecutive 'writing out on the basis', hence

$$\det A = \det B \det C \det D = \pm 1 \cdot \alpha_1 \cdots \alpha_r \cdot \pm 1 = \pm |G/H|,$$

which completes the proof. □

This theorem finishes the theory we need to understand free abelian groups. We now focus our attention to symmetric polynomials.

Definition 1.5. Let n be an integer and R a ring. The *k-th symmetric polynomial*

$$\sigma_k := \sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k} \in R[x_1, \ldots, x_n].$$

Symmetric polynomials arise naturally when computing the coefficients of a polynomial in terms of its roots. If $f = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n = (x - \alpha_1) \cdots (x - \alpha_n)$, then $a_{n-i} = (-1)^i \sigma_i(\alpha_1, \ldots, \alpha_n)$.

Theorem 1.6 (Fundamental theorem of symmetric polynomials)**.** *Every symmetric polynomial in $R[x_1, \ldots, x_n]$ can be written as a polynomial over R in the elementary symmetric polynomials. As a corollary, if $K \subset L$ are fields and $f \in K[x]$ has roots $\alpha_1, \ldots \alpha_m$, then for any symmetric polynomial $S \in K[x_1, \ldots, x_m]$ we have $S[\alpha_1, \ldots, \alpha_m] \in K$.*

Very important for studying finite field extensions of $\mathbb{Q}$ is the following theorem.

Theorem 1.7 (Theorem of the primitive element)**.** *Let F be a field of characteristic 0 and $L \supset F$ a finite extension. Then there exists a $\theta \in L$ such that $L = F(\theta)$.*

The element θ is called a *primitive element* for the field extension. Proofs of Theorems 1.6 and 1.7 can be found in [6].

1.2 Algebraic numbers

In this section, we study the basics of algebraic number theory. We start by introducing the language and notation.

Definition 1.8. (i) A finite extension field of $\mathbb{Q}$ is called a *number field*.

(ii) If α is a root of a polynomial $f \in \mathbb{Q}[x]$, then α is called an *algebraic number*.

(iii) If α is a root of a monic polynomial $f \in \mathbb{Z}[x]$, then α is called an *algebraic integer*.

The sets of algebraic numbers and algebraic integers will be denoted as $\mathbb{A}$ and $\mathbb{B}$ respectively.

Lemma 1.9. *The set $\mathbb{A}$ of algebraic numbers is a subfield of $\mathbb{C}$.*

Proof. Remember that α is algebraic if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. So if $\alpha, \beta \in \mathbb{A}$, then $\alpha \pm \beta, \alpha \cdot \beta \in \mathbb{Q}(\alpha, \beta)$ and α is clearly also algebraic over $\mathbb{Q}(\beta)$, so

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] < \infty.$$

Lastly, note that $\mathbb{Q}(\alpha) = \mathbb{Q}(1/\alpha)$. □

Also note that the primitive element of a finite extension is always algebraic, since the extension is finite. Recall the following fact from Galois theory.

Lemma 1.10. *If $K = \mathbb{Q}(\theta)$ is a number field with $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, then there exist precisely n monomorphisms $\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{C}$ and the elements $\sigma_i(\theta)$ are the roots of the minimum polynomial of θ over $\mathbb{Q}$.*

From now on, Let $K = \mathbb{Q}(\theta)$ be a number field of degree n with monomorphisms $\sigma_1, \ldots, \sigma_n$ into $\mathbb{C}$.

Definition 1.11. With the same notation as in the previous lemma, the *field polynomial* of $\alpha \in \mathbb{Q}(\theta)$ is defined as $f_\alpha = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha))$.

Lemma 1.12. *The field polynomial $f_\alpha \in \mathbb{Q}[x]$.*

Proof. We can write $\alpha = p(\theta)$ for some $p \in \mathbb{Q}[x]$. Then

$$f_\alpha = \prod_{i=1}^{n} (x - p(\sigma_i(\theta)))$$

and by expanding this product we see that the coefficients of f_α are symmetric polynomials in the $\sigma_i(\theta)$. By Theorem 1.6, they are now in $\mathbb{Q}$. □

Lemma 1.13. *The field polynomial f_α is a power of the minimum polynomial p_α of α over $\mathbb{Q}$.*

Proof. Since $p_\alpha(\sigma(\alpha)) = \sigma(p(\alpha)) = 0$, we see that the Galois conjugates $\sigma_i(\alpha)$ are the zeros of p_α. Also, since α is a zero of f_α, p_α divides f_α. Let m be the degree of p_α. If $f_\alpha = p_\alpha^k \cdot h$ for some non-constant $h \in \mathbb{C}[x]$, then some $\sigma_i(\alpha)$ is a root of h. But then all conjugates $\sigma_i(\alpha)$ are roots of h and p_α divides h. We conclude that $h = 1$. □

Corollary 1.14. *An element $\alpha \in \mathbb{Q}(\theta)$ is in $\mathbb{Q}$ if and only if all of its conjugates are equal and $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ if and only if all of its conjugates are distinct.*

Theorem 1.15. *The following statements are equivalent:*

(a) α is an algebraic integer,

(b) α is an eigenvalue of a matrix with integer coefficients and

(c) the additive group generated by $1, \alpha, \alpha^2, \ldots$ is finitely generated.

Proof. Clearly, if α is an eigenvalue of a matrix with integer coefficients, then it is a zero of the characteristic polynomial, which has integer coefficients. For the converse, note that α is a zero of $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ if and only if $\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \ldots - a_1\alpha - a_0$. Hence we see that

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -a_n & -a_{n-1} & \cdots & \cdots & -a_1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \end{pmatrix},$$

where the matrix has integer coefficients. Note that in this way we can prove an analogous statement for algebraic numbers.

Clearly, if α is an algebraic integer, the additive group $G =< 1, \alpha, \alpha^2, \ldots >$ is finitely generated. Now suppose G is finitely generated and let $v_1, \ldots, v_n$ be the generators. Then we can write $\alpha v_i = b_{i1}v_1 + \ldots + b_{in}v_n$ for integers $b_{ij} \in \mathbb{Z}$. With $B = (b_{ij})$ and $v = (v_1, \ldots, v_n)^T$, we then see that $\alpha v = Bv$, so α is an eigenvalue of a matrix with integer coefficients. □

Lemma 1.16. *The set $\mathbb{B}$ of algebraic integers is a ring.*

Proof. Using the previous lemma, we see that $\alpha, \beta \in \mathbb{B}$ means that α is an eigenvalue of some matrix M with eigenvector v and β is an eigenvalue of some matrix N with eigenvector w, both with integer coefficients. But then $\alpha + \beta$ is an eigenvalue of $M \otimes I + I \otimes N$ and $\alpha \cdot \beta$ is an eigenvalue of $M \otimes N$, both with eigenvector $v \otimes w$. Also, both matrices clearly have integer coefficients, so by the previous lemma, we are done. □

The following lemma describes a very useful property of algebraic integers.

Lemma 1.17. *If α is a complex number satisfying a monic polynomial equation with coefficients that are algebraic integers, then α is an algebraic integer as well.*

Proof. Suppose that $\alpha^n + \gamma_{n-1}\alpha^{n-1} + \ldots + \gamma_0 = 0$, with $\gamma_i \in \mathbb{B}$ for each i. Then each γ_i lies in a finitely generated group generated by elements that we call $v_{i1}, \ldots, v_{in_i}$. Thus the group $G =< 1, \alpha, \alpha^2, \ldots >$ lies within the group generated by

$$\{v_{0j_0}, v_{1j_1}\alpha, \ldots, v_{n-1,j_{n-1}}\alpha^{n-1} \mid 1 \leq j_i \leq n_i,\, 0 \leq i \leq n-1,\},$$

which is a finite set. □

Definition 1.18. If K is a number field, we define the *ring of integers* of K to be $\mathcal{O}_K = K \cap \mathbb{B}$.

This is indeed a ring since it is the intersection of two rings. Also, we see that $\mathbb{Z} \subset \mathcal{O}_K \subset K$. The ring of integers of a number field K can be seen as a generalization of the integers $\mathbb{Z} \subset \mathbb{Q}$, as will become clear in Theorem 1.21.

Lemma 1.19. *If $\alpha \in K$, there exists a $k \in \mathbb{Z}$ such that $k\alpha \in \mathcal{O}_K$.*

Proof. Since α satisfies some monic polynomial equation over $\mathbb{Q}$, we can smartly choose a $k \in \mathbb{Z}$ such that $c\alpha$ satisfies a monic polynomial over $\mathbb{Z}$. □

From the previous lemma together with the theorem of the primitive element, we may conclude that we can write any number field K as $K = \mathbb{Q}(\theta)$ for some algebraic *integer* θ. Therefore, from now on we write $K = \mathbb{Q}(\theta)$, where $\theta \in \mathbb{B}$.

The following useful property follows immediately from Gauss' lemma.

Lemma 1.20. *An algebraic number is an algebraic integer if and only if its minimum polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

Theorem 1.21. $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$

Proof. If $\alpha \in \mathbb{B} \cap \mathbb{Q}$, its minimum polynomial is $x - \alpha$, which must be in $\mathbb{Z}[x]$. □

We now define the discriminant, which will turn out to be a very useful invariant later on.

Definition 1.22. The *discriminant* of a basis $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{Q}(\theta)$ is defined as $\Delta(\mathcal{A}) = (\det \sigma_i(\alpha_j))^2$.

Lemma 1.23. *The discriminant of any basis for $\mathbb{Q}(\theta)$ is rational and non-zero.*

Proof. Suppose $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ and $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ are two bases. Then there exists an invertible basis transformation matrix $C = (c_{ik})$ such that for each k $\beta_k = c_{1k}a_1 + \ldots + c_{nk}a_n$ and hence $\sigma_j(\beta_k) = c_{1k}\sigma_j(\alpha_1) + \ldots + c_{nk}\sigma_j(\alpha_n)$. We thus find that for $A = (\sigma_i(\alpha_j))$ and $B = (\sigma_i(\beta_j))$ we have $B = CA$, so in particular

$$\Delta(\mathcal{B}) = (\det(C))^2\Delta(\mathcal{A}),$$

where $\det(C)$ is a rational number. Hence we can reduce the statement to proving that the specific basis $\{1, \theta, \ldots, \theta^{n-1}\}$ has a rational discriminant. But a matrix of the form $(a_i^j)_{ij}$ has a known determinant, which is called the *Vandermonde determinant*. It equals

$$\prod_{i<j}(\alpha_i - \alpha_j),$$

which can be seen by comparison of the roots, the degree and one coefficient. Then we see that $(\det((\sigma_i(\theta))^j))^2$ is a symmetric expression in the $\sigma_i(\theta)$ and hence rational by Theorem 1.6. Any discriminant is non-zero since the $\sigma_i(\theta)$ are non-zero and the basis transformation matrix is invertible. □

Using our knowledge of algebraic integers, we can show more.

Lemma 1.24. *Let $\mathcal{A}$ be a basis for $K = \mathbb{Q}(\theta)$ consisting of algebraic integers. Then the discriminant $\Delta(\mathcal{A}) \in \mathbb{Z}$.*

Proof. By Lemma 1.23, $\Delta(\mathcal{A}) \in \mathbb{Q}$. But since $\mathcal{A}$ consists of algebraic integers, $\Delta(\mathcal{A}) \in \mathbb{B}$ as well, so $\Delta(\mathcal{A}) \in \mathbb{Z}$ by Theorem 1.21. □

We already saw that $\mathcal{O}_K$ is an abelian group under addition. Hence we can define an *integral basis* for $\mathcal{O}_K$ as a basis for the free abelian group $(\mathcal{O}_K, +)$. Sometimes we refer to an integral basis for $\mathcal{O}_K$ as an integral basis *for* K. Despite the fact that this is incorrect, no confusion should arise from this. The first question one might ask is: does every number field have an integral basis? The answer is yes.

Theorem 1.25. *Every number field $K = \mathbb{Q}(\theta)$ has an integral basis consisting of $n = [K : \mathbb{Q}]$ elements.*

Proof. Firstly, from Lemma 1.19, we see that any integral basis is also a $\mathbb{Q}$-basis for K, i.e. a basis for K such that every element is expressible in the basis elements with coefficients in $\mathbb{Q}$. Hence they must consist of n elements. Surely we can find a basis for K consisting of algebraic integers, for example $\{1, \theta, \ldots, \theta^{n-1}\}$. The basis $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ of algebraic integers that minimalizes $|\Delta(\mathcal{A})|$ will be an integral basis. If not, then there exists an $\alpha \in \mathcal{O}_K$ such that $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$, but $a_1 \in \mathbb{Q} \setminus \mathbb{Z}$ (after renumbering). However, if $a_1 = a + r$ with $a \in \mathbb{Z}$ and $0 < r < 1$, then replacing α_1 by $\beta_1 = \alpha - a\alpha_1$ gives a new basis of algebraic integers with determinant $r^2\Delta(\mathcal{A})$, contradicting the minimality of Δ. □

Lemma 1.26. *If $\mathcal{X}$ and $\mathcal{Y}$ are two integral bases for K, then $\Delta(\mathcal{X}) = \Delta(\mathcal{Y})$.*

Proof. By Lemma's 1.25 and 1.2, we can write $\Delta(\mathcal{X}) = (\det C)^2\Delta(\mathcal{Y})$ for some $\mathbb{Z}$-matrix $C = (c_{ij})$ that is unimodular. □

When $\mathcal{X}$ is an integral basis for K, we may now of speak of $\Delta = \Delta(\mathcal{X})$ as *the* discriminant of K. This shows the role of the discriminant as a useful invariant of a number field.

Definition 1.27. If K/F is a finite field extension of degree n and $\alpha \in K$, we define the *norm* $\mathrm{N}_{K/F}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$ and the *trace* $\mathrm{T}_{K/F}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_n(\alpha)$, where the σ_i are the distinct homomorphisms $K \to \mathbb{C}$ that are the identity on F. If $F = \mathbb{Q}$, we just write $\mathrm{N}_{K/\mathbb{Q}} = \mathrm{N}$ and $\mathrm{T}_{K/\mathbb{Q}} = \mathrm{T}$.

The following observations follow immediately from the definitions and will be useful in Chapter 2.

Lemma 1.28. *If K/F is a field extension of degree n and $\alpha \in K$, then*

(i) the norm $\mathrm{N}_{K/F}$ is multiplicative and the trace $\mathrm{T}_{K/F}$ is linear over F;

(ii) $\mathrm{N}_{K/F}(\alpha) = (-1)^n a_0$, where a_0 is the constant coefficient of the minimum polynomial of α over F;

(iii) $\mathrm{N}_{K/F}(\alpha)$ is the determinant of the matrix of multiplication by α and

(iv) if $[K : F(\alpha)] = k$, then $\mathrm{N}_{F(\alpha)/F}(\alpha)^k = \mathrm{N}_{K/F}(\alpha)$.

Lemma 1.29. *If $\alpha \in \mathcal{O}_K$, both the norm $\mathrm{N}(\alpha) \in \mathbb{Z}$ and the trace $\mathrm{T}(\alpha) \in \mathbb{Z}$.*

Proof. The field polynomial is a power of the minimum polynomial and the latter is in $\mathbb{Z}[x]$ if and only if $\alpha \in \mathcal{O}_K$. Hence the field polynomial is in $\mathbb{Z}[x]$ when $\alpha \in \mathcal{O}_K$. But $\mathrm{N}(\alpha)$ is the constant coefficient of the field polynomial and $\mathrm{T}(\alpha)$ is the coefficient of x^{n-1}. □

Example 1.30. In order to get a feeling for the theory, let us study the quadratic number fields. Let θ be an algebraic integer. If $[\mathbb{Q}(\theta) : \mathbb{Q}] = 2$, then θ is a zero of $x^2 + ax + b$ for some $a, b \in \mathbb{Z}$ and hence

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b^2}}{2}.$$

If we divide out the squares of $a^2 - 4b^2$, we conclude that $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$ for a squarefree integer d. Also, for any squarefree $d \in \mathbb{Z}$, $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}]$ clearly equals 2.

We can also compute the set of algebraic integers of $\mathbb{Q}(\sqrt{d})$. Since $\{1, \sqrt{d}\}$ is a basis for $\mathbb{Q}(\theta)$ over $\mathbb{Q}$, any element can be written as $\alpha = (a + b\sqrt{d})/c$ for $a, b, c \in \mathbb{Z}$ and $c > 0$ and a, b, c not all divisible by the same prime. We know that $\alpha \in \mathcal{O}_K$ if and only if the coefficients of its minimum polynomial are in $\mathbb{Z}$. If $\alpha \in \mathbb{Q}$, then we know that $\alpha \in \mathcal{O}_K$ if and only if $\alpha \in \mathbb{Z}$. But if $\alpha \notin \mathbb{Q}$, then we know its minimum polynomial is $(x - \alpha)(x + \alpha)$. If we carefully compute its coefficients in terms of a, b and c, we find that

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] \text{ if } d \not\equiv 1 \pmod 4 \text{ and } \mathcal{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}] \text{ if } d \equiv 1 \pmod 4.$$

1.3 Unique factorization

We already know three ways of generalizing prime numbers in $\mathbb{Z}$: irreducible elements, prime ideals and maximal ideals. Since $\mathbb{Z}$ is a principal ideal ring, we see that p is prime if and only if p is irreducible if and only if (p) is prime if and only if (p) is maximal. However, in other number fields such equivalences do not hold. So what is the best way to generalize prime numbers in a number field?

The most important property we want prime numbers to have is that any number can be uniquely factorized into primes and that is why we defined irreducible elements. In $\mathbb{Z}[\sqrt{-6}]$, the elements $2, 3$ and $\sqrt{-6}$ are all irreducible. However, $6 = 2 \cdot 3 = \sqrt{-6} \cdot \sqrt{-6}$, so unique factorization does not hold in general for irreducible elements. But factorization need not even exist at all. If we consider the ring of algebraic integers $\mathbb{B}$, then $\alpha \in \mathbb{B}$ implies $\sqrt{\alpha} \in \mathbb{B}$, so $\alpha = \sqrt{\alpha}\sqrt{\alpha}$, which implies that $\mathbb{B}$ does not even have irreducible elements. However, $2 \in \mathbb{B}$, but $1/2 \notin \mathbb{B}$, so there do exist non-zero non-units.

In this section we will take a closer look at (unique) factorizations in order to find a satisfactory way of generalizing prime numbers. The following example illustrates how unique factorization in a number field can be used to solve Diophantine equations.

Example 1.31. Consider the Diophantine equation

$$x^2 - 4y^2 = 21.$$

We can write this as $(x-2y)(x+2y) = 21$ and 21 can be factorized only as $21 = 1 \cdot 21 = -1 \cdot -21 = 3 \cdot 7 = -3 \cdot -7$. By the uniqueness of factorization into prime numbers in $\mathbb{Z}$, we conclude that

$$(x-2y, x+2y) \in \{(1,21), (-1,-21), (21,1), (-21,-1), (3,7), (-3,-7), (7,3), (-7,-3)\}.$$

This yields eight solutions, of which all are integers:

$$(x, y) \in \{(11,5), (-11,-5), (11,-5), (-11,5), (5,1), (-5,-1), (5,-1), (-5,1)\}.$$

This example is, of course, very simple. But what if the equation was $x^2 + 3y^2 = 21$? If we want to apply the same idea, we get $(x - \sqrt{-3}y)(x + \sqrt{-3}y) = 21$ and we need to consider the number field $\mathbb{Q}(\sqrt{-3})$. In order to apply arguments similar to those in Example 1.31, we would like to have unique factorization in the ring of integers $\mathbb{Z}[\sqrt{-3}]$.

In this section, we assume that the reader is familiar with the basic notions regarding (unique) factorization into irreducible elements, as described in chapter 6 of [5].

Lemma 1.32. *For $x, y \in \mathcal{O}_K$, we have*

(i) x is a unit if and only if $\mathrm{N}(x) = \pm 1$,

(ii) if x is associate to y, then $\mathrm{N}(x) = \pm\,\mathrm{N}(y)$ and

(iii) if $\mathrm{N}(x)$ is a prime number, then x is irreducible.

The following definition of a Noetherian ring will help us to prove that factorization into irreducibles is possible in $\mathcal{O}_K$.

Definition 1.33. (i) A domain D is called *noetherian* is every ideal in D is finitely generated. This generalizes the idea of principal ideal rings.

(ii) A domain D obeys the *ascending chain condition* if every chain $I_0 \subset I_1 \subset I_2 \ldots$ of ideals stops, i.e. there always exists an N such that $I_n = I_N$ for all $n \geq N$.

(iii) A domain D satisfies the *maximal condition* if every non-empty set of ideals contains a maximal element, i.e. an element which is not contained in any other element.

Lemma 1.34. *The three definitions (i), (ii) and (iii) are equivalent.*

Proof. Suppose (i) holds and consider an ascending chain (I_n). Then $\cup_{n=0}^{\infty} I_n$ is a finitely generated ideal and (b) follows.

Suppose that (ii) holds and consider a non-empty set S of ideals. If S does not have a maximal element, we can pick $I_0 \subset I_1 \subset I_2 \subset \ldots$, giving a chain that does not stop, which contradicts (iii).

Now suppose that (iii) holds and let I be an ideal and M the set of finitely generated ideals contained in I. Since $\{0\} \in M$, it is non-empty and thus it has a maximal element J. If $J \neq I$, then for $x \in I \setminus J$, (J, x) is finitely generated and strictly larger than J, so $J = I$. □

Theorem 1.35. *If K is a number field, then $\mathcal{O}_K$ is noetherian.*

Proof. We already saw that $\mathcal{O}_K$ is free abelian of rank $n = [K : \mathbb{Q}]$. Any ideal $I \subset \mathcal{O}_K$ is a subgroup, so by Theorem 1.3, I is free abelian of rank $s \leq n$ and hence I is generated by $s < \infty$ elements. □

Theorem 1.36. *In a noetherian domain D, factorization into irreducibles is possible.*

Proof. Suppose there existed a non-zero element that could not be factorized into irreducibles. By the previous lemma, we can use the maximal condition to find that there exists an $x \in D$ such that (x) is the maximum of $\{(y) \mid y \text{ cannot be factorized into irreducibles}\}$. This x cannot be irreducible, so say $x = yz$ for non-units y and z. Then $(x) \subset (y)$, but $(x) \neq (y)$ since x and y are not associates. The same goes for z, so since x was maximal, we can factorize y and z into irreducibles giving a factorization of x, a contradiction. □

We conclude that factorization into irreducibles is at least possible in the integers of a number field, so our hope of finding some generalization of the prime numbers remains vivid. We now study the role that prime elements play in this story.

Definition 1.37. Let D be a domain. An element $x \neq 0$ is called *prime* when $x \mid ab$ implies $x \mid a$ of $x \mid b$.

Equivalently, we could say that p is prime whenever (p) is prime. Note that this notion of a prime element is for $D = \mathbb{Z}$ indeed equivalent to the classical notion of a prime number. Moreover, being prime is stronger than irreducibility.

Lemma 1.38. *Any prime in a domain D is irreducible.*

Proof. Suppose $x, a, b \in D$ such that $x = ab$ and x is prime. Then $x \mid ab$, so $x \mid a$ or $x \mid b$. Say wlog that $x \mid a$. We find that b is a unit, since $x = xcb$ for some $c \in D$. □

It is important to realize that this is a one-way street. In the example at the beginning of this section, we saw that 2 and $\sqrt{-6}$ were irreducible in $\mathbb{Z}[\sqrt{-6}]$, the ring of integers of $\mathbb{Q}[\sqrt{-6}]$. But then 2 cannot divide $\sqrt{-6}$, while $2 \mid 6$ and $6 = \sqrt{-6}\sqrt{-6}$. This difference between the definitions of a prime element and an irreducible element turns out to characterize precisely when factorization into irreducibles is unique.

Theorem 1.39. *If D is a domain in which factorization into irreducibles is possible, then this factorization is unique if and only if all irreducible elements are prime.*

Proof. Suppose factorization is unique and let $a, b, p \in D$ with p irreducible such that $p \mid ab$. If we write $pc = ab$ and $a = u \cdot p_1 \cdots p_n$, $b = v \cdot q_1 \cdots q_m$ and $c = w \cdot r_1 \cdots r_k$ for units $u, v, w \in D$ and irreducible elements $p_i, q_j, r_l \in D$ for each i, j and l, then we have

$$w \cdot r_1 \cdots r_k \cdot p = (uv) \cdot p_1 \cdots p_n \cdot q_1 \cdots q_m,$$

and by uniqueness, there either exists an i such that p is associate to p_i or there exists a j such that p is associate to q_j. Hence either $p \mid a$ or $p \mid b$.

Now suppose that all irreducible elements are prime. Write $a = u \cdot p_1 \cdots p_n = v \cdot q_1 \cdots q_m$ with $m \leq n$ into irreducibles in two ways. We will use induction on n. For $n = 0$, a is a unit and the factorization is unique. Suppose that any two factorizations consisting of a maximum of $\leq n - 1$ elements are equal. We see that $p_n \mid a$ and since p_n is prime, there exists a j, say wlog that $j = m$, such that $p_n \mid q_m$. Since both are irreducible, we find that p_n is associate to q_m and since both must be non-zero, we get

$$u \cdot p_1 \cdots p_{n-1} = w \cdot q_1 \cdots q_{m-1}$$

for some unit w. The induction hypothesis now gives that these factorizations are the same, so we are done. □

Remember that any Euclidian ring is a principal ideal ring and that any principal ideal ring is a unique factorization domain (see [5]). Hence we conclude that in Euclidian and in principal ideal rings, the definitions of prime and irreducible elements coincide.

If D is a domain with unique factorization into irreducibles, then many intuitive ideas about division remain true. For example, the greatest common divisor and the smallest common multiple of two elements are well-defined up to units. We can then say that two elements $a, b \in D$ are *relatively prime* or *coprime* whenever $\gcd(a, b)$ is a unit.

For negative square-free d, it is not too difficult to check when $\mathbb{Q}(\sqrt{d})$ is Euclidian.

Theorem 1.40. *For negative square-free d, $\mathbb{Q}(\sqrt{d})$ is Euclidian if and only if $d \in \{-1, -2, -3, -7, -11\}$ and in each case, the Euclidian function is $\phi : \mathbb{Q}(\sqrt{d})^* \to \mathbb{R}_{>0}$, $\alpha \mapsto |\mathbb{N}(\alpha)|$.*

A proof can be found in section 4.7 of [16]. This immediately enables us to solve a new class of Diophantine equations. We can now use the same technique as in Example 1.31 to solve the Diophantine equations like $x^2 + dy^2 = 21$ for $d \in \{-1, -2, -3, -7, -11\}$.

Now that we have seen precisely whenever unique factorization into irreducibles is possible, we will shift our focus towards ideals. Kummer and Dedekind developed the theory of ideals and showed that factorization of *ideals* into prime ideals is always possible and unique in rings of integers of number fields. In fact, factorization of ideals can be seen as a generalization of the factorization of elements, since a factorization of a principal ideal into principal prime ideals corresponds precisely to factorizing the element into irreducibles, as we shall see later on.

As usual, we define the multiplication $I \cdot J$ of two ideals as the set of all finite sums $\sum x_i y_j$, where all $x_i \in I$ and all $y_j \in J$. From now on, we will denote ideals by bold letters. The following important observations follow immediately from the definitions.

Lemma 1.41. *If $a, b \in \mathcal{O}_K$, $u \in \mathcal{O}_K$ is a unit and $\mathbf{p} \subset \mathcal{O}_K$ is an ideal, then*

(i) $(a) \cdot (b) = (ab)$,

(ii) $(a) = (ua)$ *and*

(iii) $\mathbf{p}$ *is prime if and only if* $\mathbf{a} \cdot \mathbf{b} \subset \mathbf{p} \Rightarrow \mathbf{a} \subset \mathbf{p}$ *or* $\mathbf{b} \subset \mathbf{p}$ *for all ideals* $\mathbf{a}$ *and* $\mathbf{b}$.

Definition 1.42. A ring D is called a *Dedekind ring* whenever it is a Noetherian domain satisfying the additional properties that

(i) if $\alpha \in Q(D)$ satisfies a monic polynomial equation over D, then $\alpha \in D$ and

(ii) every non-zero prime ideal of D is maximal.

Dedekind rings generalize the properties of rings of integers of number fields when it comes to factorization of ideals, as we will see later on.

Lemma 1.43. *The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind ring.*

Proof. We already know that $\mathcal{O}_K$ is a Noetherian domain (Lemma 1.35) and property (i) holds by Lemma 1.17, so we need to show (ii). To that end, suppose that $\mathbf{p}$ is a prime ideal and that $0 \neq \alpha \in \mathbf{p}$. Since α is an algebraic integer, $N = \mathrm{N}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha) \in \mathbb{Z}$. Also, all the $\sigma_i(\alpha) \in \mathcal{O}_K$ and one of them equals α, so $(N) \subset \mathbf{p}$. Hence we find that $\mathcal{O}/\mathbf{p} \subset \mathcal{O}/(N)$ with the trivial injection $x + \mathbf{p} \mapsto x + (N)$. We had $N \in \mathbb{Z}$, so every element in $\mathcal{O}/(N)$ has finite order and since $\mathcal{O}$ and thus $\mathcal{O}/(N)$ is finitely generated, we must have that $\mathcal{O}/(N)$ is finite. We conclude that $\mathcal{O}/\mathbf{p}$ is a finite domain and must therefore be a field, making $\mathbf{p}$ maximal. □

Now note that the product between ideals is associative and commutative and that D serves as a unit. However, inverses of ideals are not so easily defined. In fact, the set of ideals is, in general, not a group. Therefore, we extend the set of ideals to a larger set, that we will readily show to indeed be a group.

Definition 1.44. If D is a Dedekind ring with quotient field $Q(D)$, then the set $\mathcal{F}$ of *fractional ideals* of D consists of the sets $\mathbf{a} \subset Q(D)$ such that $\mathbf{a}D \subset \mathbf{a}$ and there exists a $c \in D$ such that $c\mathbf{a} \subset \mathcal{O}$.

We notice that if $\mathbf{a}$ is a fractional ideal and $c\mathbf{a} \subset D$, then $c\mathbf{a} \subset D$ is an ideal in D. Hence, $\mathbf{a}$ is a fractional ideal if and only if there exists a $c \in D$ and an ideal $\mathbf{b} \subset \mathcal{O}$ such that $\mathbf{a} = c^{-1}\mathbf{b}$. Also, every ideal is a fractional ideal and we have the same associative multiplication on $\mathcal{F}$. An example of a fractional ideal in $\mathbb{Q}$ is $\frac{1}{2}\mathbb{Z}$, which we will soon show to be the inverse $2\mathbb{Z} = (2)$.

Definition 1.45. If $\mathbf{a} \subset D$ is an ideal, then we define $\mathbf{a}^{-1} = \{x \in Q(D) \mid x\mathbf{a} \subset D\}$.

We will show in Theorem 1.49 that $\mathbf{a}^{-1}$ indeed serves as the inverse of $\mathbf{a}$. From the definition, we see that $D\mathbf{a}^{-1} \subset \mathbf{a}^{-1}$ and any $c \in \mathbf{a}$ gives $c\mathbf{a}^{-1} \subset D$, so $\mathbf{a}^{-1} \in \mathcal{F}$. Also, we notice that $\mathbf{a}\mathbf{a}^{-1} \subset D$ and that for any ideal $\mathbf{b}$ we have $\mathbf{b} \subset \mathbf{a}$ implies $\mathbf{a}^{-1} \subset \mathbf{b}^{-1}$. Before we are able to prove theorem 1.49, we need some additional lemma's.

Lemma 1.46. *For each non-zero ideal $\mathbf{a} \subset D$, there exist prime ideals $\mathbf{p}_1, \ldots, \mathbf{p}_r$ such that $\mathbf{p}_1 \cdots \mathbf{p}_r \subset \mathbf{a}$.*

Proof. Suppose not. By the noetherianity of D, we can choose a maximal ideal $\mathbf{a}$ such that those prime ideals do not exist. In particular, $\mathbf{a}$ is not prime, so we can find ideals $\mathbf{b}$ and $\mathbf{c}$ such that $\mathbf{bc} \subset \mathbf{a}$, but $\mathbf{b} \not\subset \mathbf{a}$ and $\mathbf{c} \not\subset \mathbf{a}$. If we define $\mathbf{b}' = \mathbf{a} + \mathbf{b}$ and $\mathbf{c}' = \mathbf{a} + \mathbf{c}$, then we find that $\mathbf{b}'\mathbf{c}' \subset \mathbf{a}$ and $\mathbf{a} \subsetneq \mathbf{b}'$, $\mathbf{a} \subsetneq \mathbf{c}'$. Now we can use the maximality of $\mathbf{a}$ to find products of prime ideals in $\mathbf{b}'$ and in $\mathbf{c}'$. The product of all these prime ideals must then be in $\mathbf{a}$, a contradiction. □

Lemma 1.47. *If $\mathbf{a} \subset D$ is a proper ideal, then $D \subsetneq \mathbf{a}^{-1}$.*

Proof. We will show that $\mathbf{p}^{-1} \neq D$ for any maximal ideal $\mathbf{p}$. This is sufficient since there exists a maximal ideal $\mathbf{p}$ such that $\mathbf{a} \subset \mathbf{p}$, which means $\mathbf{p}^{-1} \subset \mathbf{a}^{-1}$. Now take $0 \neq x \in \mathbf{p}$ and let r be smallest such that there exist prime ideals $\mathbf{p}_i$ with $\mathbf{p}_1 \cdots \mathbf{p}_r \subset (r) \subset \mathbf{p}$. Since $\mathbf{p}$ is prime, we have $\mathbf{p}_i \subset \mathbf{p}$ for some i, say wlog that $\mathbf{p}_1 \subset \mathbf{p}$. By maximality of $\mathbf{p}_1$, we have $\mathbf{p}_1 = \mathbf{p}$. Also, the minimality of r implies that we can find $b \in \mathbf{p}_2 \cdots \mathbf{p}_r \setminus (a)$. It follows that $b\mathbf{p} \subset (a)$ and hence $ba^{-1} \in \mathbf{p}^{-1}$. However, $b \notin (a)$ implies $ba^{-1} \notin D$, so we are done. □

Lemma 1.48. *If $\mathbf{a} \subset D$ is a non-zero ideal and $S \subset K$ a set such that $\mathbf{a}S \subset \mathbf{a}$, then $S \subset D$.*

Proof. Suppose that $s \in S$. We can write $\mathbf{a} = (a_1, \ldots, a_n)$ since D is noetherian. Since $\mathbf{a}s \subset \mathbf{a}$, we can express $a_i s$ in terms of the a_j as

$$a_i s = \sum_{j=1}^{n} b_{ij} a_j \iff b_{i1}a_1 + \ldots + b_{i,i-1}a_{i-1} + (b_{ii} - s)a_i + b_{i,i+1}a_{i+1} + \ldots + b_{in}a_n = 0.$$

The last set of equations can be viewed as $Ca = 0$, where $C = (c_{ij})$ is a matrix and $a = (a_1, \ldots, a_n)^T$ a vector. Thus B has a zero eigenvalue and hence $\det B = 0$. This gives a monic equation in s with coefficients in D. By Definition 1.42 (i), we find $s \in D$, as desired. □

Theorem 1.49. *The set $\mathcal{F}$ of fractional ideals of D with the usual multiplication is an abelian group.*

Proof. We only need to show that every fractional ideal has an inverse, since the other group properties are clear. We will prove this in steps. First suppose that $\mathbf{p}$ is a maximal ideal. We already saw that $\mathbf{p} \subset \mathbf{p}\mathbf{p}^{-1} \subset D$ and $\mathbf{p}\mathbf{p}^{-1}$ is an ideal. So by maximality, $\mathbf{p}\mathbf{p}^{-1} = \mathbf{p}$ or $\mathbf{p}\mathbf{p}^{-1} = D$. But if $\mathbf{p}\mathbf{p}^{-1} = \mathbf{p}$, then $\mathbf{p}^{-1} \subset D$ by the previous lemma, which contradicts Lemma 1.47.

Suppose towards a contradiction that there exists an ideal $\mathbf{b}$ such that $\mathbf{b}\mathbf{b}^{-1} \neq D$ and let $\{0\} \neq \mathbf{a}$ be the maximal ideal such that the inequality holds. We can find a maximal ideal $\mathbf{p}$ such that $\mathbf{a} \subset \mathbf{p}$. Then $\mathbf{p}^{-1} \subset \mathbf{a}^{-1}$ and hence $\mathbf{a} \subset \mathbf{a}\mathbf{p}^{-1} \subset \mathbf{a}\mathbf{a}^{-1} \subset D$, so $\mathbf{a}\mathbf{p}^{-1}$ is an ideal. But $\mathbf{a} = \mathbf{a}\mathbf{p}^{-1}$ would contradict the previous two lemmas like before, so $\mathbf{a}\mathbf{p}^{-1}$ is a strictly larger ideal. The maximality condition now yields $\mathbf{a}\mathbf{p}^{-1}(\mathbf{a}\mathbf{p}^{-1})^{-1} = D$, from which it follows from the definition of $\mathbf{a}^{-1}$ that $D = \mathbf{a}\mathbf{p}^{-1}(\mathbf{a}\mathbf{p}^{-1})^{-1} \subset \mathbf{a}\mathbf{a}^{-1} \subset D$.

Lastly, we turn to fractional ideals. If $\mathbf{a}$ is fractional, we can write $\mathbf{a} = c^{-1}\mathbf{b}$ for $c \in D$ and $\mathbf{b}$ an ideal in D. Then we see that $c^{-1}\mathbf{b} \cdot c\mathbf{b}^{-1} = D$, finishing the proof. □

The following definition helps to highlight our new view of fractional ideals as a group under multiplication.

Definition 1.50. If $\mathbf{a}$ and $\mathbf{b}$ are prime ideals in D, we say that $\mathbf{a}$ divides $\mathbf{b}$, written as $\mathbf{a} \mid \mathbf{b}$, when there exists an ideal $\mathbf{c}$ such that $\mathbf{b} = \mathbf{a}\mathbf{c}$. This is now equivalent to $\mathbf{b} \subset \mathbf{a}$, since we can take $\mathbf{c} = \mathbf{a}^{-1}\mathbf{b} \subset D$.

The group structure of $\mathcal{F}$ now allows us to prove the following fundamental theorem.

Theorem 1.51. *Every non-zero ideal of D can be uniquely, up to order, written as a product of prime ideals.*

Proof. We first prove the existence of this factorization. Like always, we assume that not every non-zero ideal can be factorized into prime ideals and we take $\mathbf{a}$ to be the maximal ideal that cannot be factorized. In particular, $\mathbf{a}$ is not prime, hence not maximal, so we can find a maximal ideal $\mathbf{p}$ such that $\mathbf{a} \subsetneq \mathbf{p}$ and hence we find that $\mathbf{a} \subsetneq \mathbf{a}\mathbf{p}^{-1} \subset \mathbf{a}\mathbf{a}^{-1} \subset D$. Since $\mathbf{a}\mathbf{p}^{-1}$ is a strictly larger ideal than $\mathbf{a}$, it can be factorized. Multiplication by $\mathbf{p}$ then gives a factorization for $\mathbf{a}$, a contradiction.

We now prove the uniqueness by induction. Suppose $\mathbf{p}_1 \cdots \mathbf{p}_r = \mathbf{q}_1 \cdots \mathbf{q}_s$, where all $\mathbf{p}_i$'s and $\mathbf{q}_j$'s are prime ideals. Then $\mathbf{p}_r \mid \mathbf{q}_i$ for some i since $\mathbf{p}_r$ is prime, say w.l.o.g. that $i = s$. Since $\mathbf{p}_r$ is maximal, this implies that $\mathbf{p}_r = \mathbf{q}_s$ and multiplication by $\mathbf{p}_r^{-1}$ now yields $\mathbf{p}_1 \cdots \mathbf{p}_{r-1} = \mathbf{q}_1 \cdots \mathbf{q}_{s-1}$. By the induction hypothesis, $r - 1 = s - 1$ and the factors are the same. □

Corollary 1.52. *If we allow negative powers in the expansion, then any fractional ideal* $\mathbf{a}$ *can also uniquely be written as a product of powers of prime ideals.*

Proof. We already know that $\mathbf{a}$ is fractional if and only if there exists an ideal $\mathbf{b} \subset D$ and a $c \in D$ such that $(c)\mathbf{a} = c\mathbf{a} = \mathbf{b}$. If $\mathbf{b} = \mathbf{p}_1 \cdots \mathbf{p}_r$ and $(c) = \mathbf{q}_1 \cdots \mathbf{q}_s$, then $\mathbf{a} = \mathbf{p}_1 \cdots \mathbf{p}_r \mathbf{q}_1^{-1} \cdots \mathbf{q}_s^{-1}$. The factorization of $\mathbf{a}$ is unique since the factorizations of $\mathbf{b}$ and (c) are. □

One immediate consequence is that we can again define the greatest common divisor and the least common multiple of two ideals.

At this point, we leave the abstract Dedekind ring D and go back to considering the Dedeking ring $\mathcal{O}_K$, the ring of integers of a number field K.

Definition 1.53. If $\mathbf{a} \subset \mathcal{O}_K$ is an ideal, then we define its *norm* $\mathrm{N}(\mathbf{a}) = |\mathcal{O}/\mathbf{a}|$.

This norm is always finite by the proof of Lemma 1.43. The following lemma illustrates that there should be no confusion between the norm of an element and that of an ideal.

Lemma 1.54. *If* $\mathbf{a} = (a) \subset \mathcal{O}_K$ *is a principal ideal, then* $\mathrm{N}(\mathbf{a}) = |\,\mathrm{N}(a)|$.

Proof. Since $\mathcal{O}_K/\mathbf{a}$ is finite, we conclude from Theorems 1.3 and 1.4 that $\mathbf{a}$ is a free abelian group of rank n. So if $\mathcal{V} = \{v_1, \ldots, v_n\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ and $\mathcal{U} = \{u_1, \ldots, u_n\}$ for $\mathbf{a}$, then we can write $u_i = \sum_j \alpha_{ij} v_j$ with $\alpha_{ij} \in \mathbb{Z}$ for each i, j. By Theorem 1.4, we then find that $\mathrm{N}(\mathbf{a}) = |\mathcal{O}_K/\mathbf{a}| = \det c_{ij}$. As we saw in the proof of Lemma 1.23, we also have $\Delta\mathcal{U} = (\det c_{ij})^2 \Delta\mathcal{V}$. Since $\mathrm{N}(\mathbf{a})$ is positive, we find

$$\mathrm{N}(\mathbf{a}) = \left| \frac{\Delta\mathcal{U}}{\Delta\mathcal{V}} \right|^{1/2}.$$

Now since $\mathbf{a} = (a)$ is principal, we can take $u_i = av_i$ for each i. They are all in $\mathbf{a}$ and clearly still linearly independent over $\mathbb{Z}$. We also see from the definitions that $\Delta(\{av_1, \ldots, av_n\}) = (\mathrm{N}(a))^2 \Delta(\{v_1, \ldots, v_n\})$, which proves the statement. □

The norm is indeed multiplicative, as we would like a 'norm' to be.

Lemma 1.55. *If* $\mathbf{a}$ *and* $\mathbf{b}$ *are ideals in* $\mathcal{O}_K$*, then* $\mathrm{N}(\mathbf{ab}) = \mathrm{N}(\mathbf{a})\,\mathrm{N}(\mathbf{b})$.

Proof. Fist note that, by the uniqueness of factorization, it is sufficient to prove $\mathrm{N}(\mathbf{ap}) = \mathrm{N}(\mathbf{a})\,\mathrm{N}(\mathbf{p})$, where $\mathbf{p}$ is a prime ideal. Towards that end, notice that the surjection $\pi : \mathcal{O}_K/\mathbf{ap} \to \mathcal{O}_K/\mathbf{a}$ with $\pi(\mathbf{ap}+x) = \mathbf{a}+x$ is a homomorphism with kernel $\mathbf{a}/\mathbf{ap}$, which implies that $|\mathcal{O}_K/\mathbf{ap}| = |\mathcal{O}_K/\mathbf{a}| \cdot |\mathbf{a}/\mathbf{ap}|$. Thus it remains to show that $|\mathbf{a}/\mathbf{ap}| = |\mathcal{O}_K/\mathbf{p}|$.

Consider then $\phi : \mathcal{O}_K \to \mathbf{a}/\mathbf{ap}$ with $\phi(x) = \mathbf{ap} + yx$, where $y \in \mathbf{a} \setminus \mathbf{ap}$. By the unique prime factorization, $\mathbf{ap} \not\subset \mathbf{a}$, so such a y exists. Also, note that the kernel of ϕ is an ideal unequal to $\mathcal{O}_K$ that contains $\mathbf{p}$. So since $\mathbf{p}$ is maximal, $\mathbf{p} = \ker \phi$. For surjectivity, suppose that $\mathbf{ap} \subset \mathbf{b} \subset \mathbf{a}$ for some ideal $\mathbf{b}$. Multiplying by $\mathbf{a}^{-1}$ then yields $\mathbf{p} \subset \mathbf{a}^{-1}\mathbf{p} \subset \mathcal{O}_K$ and by maximality of $\mathbf{p}$ we find that $\mathbf{b} = \mathbf{a}$ or $\mathbf{b} = \mathbf{ap}$. Since $y \notin \mathbf{ap}$, we conclude that $\mathbf{ap} + (y) = \mathbf{a}$. Thus ϕ is surjective and $\mathbf{a}/\mathbf{ap} \simeq \mathcal{O}_K/\mathbf{p}$ as groups. □

Our definition of the norm also allows us to prove a generalization of Fermat's Little Theorem, which will be useful in Chapter 3.

Lemma 1.56. *Let p be a prime number and K a number field of degree n with ring of integers $\mathcal{O}_K$. Then for each $a \in \mathcal{O}_K$, we have that $a^{p^n} \equiv 1 \pmod{(p)}$.*

Proof. We defined the norm of the ideal (p) as $\mathrm{N}((p)) = |\mathcal{O}_K/(p)| < \infty$ and by Lemma 1.54, $\mathrm{N}((p)) = |\mathrm{N}(p)| = p^n$. □

Using unique factorization and Lemma 1.55, many interesting properties of the norm are easily deduced. For example, if $\mathbf{a}$ is an ideal and $\mathrm{N}(\mathbf{a})$ is prime, then $\mathbf{a}$ is prime. Also, from the definition, we see that $\mathrm{N}(\mathbf{a}) \cdot 1 = \mathrm{N}(\mathbf{a}) \in \mathbf{a}$. Hence, if $\mathbf{p}$ is prime, then some prime divisor p of $\mathrm{N}(\mathbf{p})$ is in $\mathbf{p}$. But if there were two different primes $p, q \in \mathbf{p}$, then $1 = ap + bq \in \mathbf{p}$ for some $a, b \in \mathbb{Z}$ and $\mathcal{O}_K = \mathbf{p}$, which is not true. Also, $(p) \subset \mathbf{p}$ and $\mathrm{N}(\mathbf{p})$ divides $\mathrm{N}((p)) = p^n$, where $n = [K : \mathbb{Q}]$. We have thus found for any prime ideal $\mathbf{p}$ that $\mathrm{N}(\mathbf{p}) = p^m$, where $m \leq n$ and p is a unique prime number. We are now ready to prove an important theorem.

Theorem 1.57. *Factorization of elements into irreducibles is unique in $\mathcal{O}_K$ if and only if $\mathcal{O}_K$ is a principal ideal ring.*

Proof. We already know that this factorization is unique in any principal ideal ring. For the converse, suppose the factorization is unique and let $0 \neq \mathbf{p} \subset \mathcal{O}_K$ be a prime ideal. Then there exists a prime number $p \in \mathbb{Z} \cap \mathbf{p}$. In $\mathcal{O}_K$, we can uniquely write $p = p_1 \cdots p_m$ into irreducibles. Since $\mathbf{p}$ is a prime ideal, there exists an i such that $p_i \in \mathbf{p}$. By theorem 1.39, p_i is then prime and hence $(p_i) \subset \mathbf{p}$ is a prime ideal. But any non-zero prime ideal is maximal and since $\mathbf{p} \neq \mathcal{O}_K$, we find that $\mathbf{p} = (p_i)$ is principal. Lastly, the unique factorization of ideals into prime ideals shows that any ideal is principal. □

This finishes the theory of unique factorization in $\mathcal{O}_K$, for now. We may conclude that unique factorization is possible when $\mathcal{O}_K$ is a principal ideal domain or, equivalently, when every irreducible element is prime and that in that case, the factorization of $\pi \in \mathcal{O}_K$ corresponds to the factorization of (π) into (principal) prime ideals. If factorization is not unique, there exists an irreducible element $y \in \mathcal{O}_K$ that is not prime. Hence (y) is not prime and (y) factorizes into prime ideals that are all not principal.

At this point, it would be a shame not to mention the following definition.

Definition 1.58. If $\mathcal{P}$ is the set of principal fractional ideals in $\mathcal{O}$, the *class group* is defined as the set $\mathcal{H} = \mathcal{F}/\mathcal{P}$. Its order $h = |\mathcal{H}|$ is called the *class number*.

The class group 'measures' in some way how non-unique the factorization into irreducibles is in a number field. It can be shown that the class group is always finite (see [16]). Also, note that the class number $h = 1$ if and only if factorization into irreducibles is unique in $\mathcal{O}_K$.

1.4 A geometrical approach to number theory

We begin this section by studying some geometry, which shall accumulate into Minkowski's theorem. Then, we shall translate a number field K into a geometrical setting which will allow us to apply the strength of Minkowski's theorem. The final result we obtain is Dirichlet's unit theorem, a detailed description of the group of units in the ring of integers $\mathcal{O}_K$ of a number field. This is an essential tool for our study of Diophantine equations in Chapter 3. At first, we need to develop the geometrical formalisms.

Definition 1.59. If $\{e_1, \ldots, e_n\}$ is a linearly independent set in $\mathbb{R}^m$, then the additive group generated by $\{e_1, \ldots, e_n\}$ is called a *lattice*. A subset of $\mathbb{R}^n$ is called *discrete* when its intersection with $B(r^+) := \{x \in \mathbb{R}^n \mid |x| \leq r\}$ is finite for every $r \geq 0$.

Note that any lattice is a free abelian group. The following theorem connects the new definitions.

Theorem 1.60. *An additive subgroup of $\mathbb{R}^n$ is a lattice if and only if it is discrete.*

Proof. Firstly, suppose that L is a lattice generated by $\{e_1, \ldots, e_n\}$. Since the e_i form a basis for $\mathbb{R}^n$, we have a trivial automorphism f of $\mathbb{R}^n$ as a vector space by $f(a_1e_1 + \ldots + a_ne_n) = (a_1, \ldots, a_n)$. By Heine-Borel, $f(B(r^+))$ is bounded, say by M. Then, if $v = a_1e_1 + \ldots + a_ne_n \in B(r^+)$, we find that $|a_i| \leq ||f(v)|| \leq M$ for each i. But for each i there are only finitely many integer values of a_i that obey this inequality, which implies that L is discrete.

For the converse, let G be a discrete additive subgroup of $\mathbb{R}^n$. We shall use induction on n. The case $n = 0$ is trivial. Since $G \subset \mathbb{R}^n$, we may take a maximal linearly independent set $\{g_1, \ldots, g_m\}$ in G. If V is the span of the $\{g_1, \ldots, g_{m-1}\}$, define $H = G \cap V$. Then H is a discrete subgroup, so by the hypothesis we can find a linearly independent set $\{h_1, \ldots, h_k\}$ that generates H. As $g_1, \ldots, g_{m-1} \in H$, we have $k \geq m - 1$ and because $g_m \notin H$, the set $\{h_1, \ldots, h_k, g_m\}$ is linearly independent in G, so $k \leq m - 1$ as well. Thus $k = m - 1$ and we define A as the set of all $x \in G$ such that $x = a_1h_1 + \ldots + a_{m-1}h_{m-1} + a_mg_m$, $0 \leq a_i < 1$ for each $i \neq m$ and $0 \leq a_m \leq 1$. Since A is a bounded subset of the discrete set G, it must be finite, so we may define $x' \in A$ with minimal coefficient a of g_m. Clearly, for any $g \in G$ we can find integers c_i such that

$$g' := g - c_mx' - c_1h_1 - \ldots - c_{m-1}h_{m-1}$$

is in A and has a coefficient for g_m that is strictly smaller than a, but non-negative. It follows that this coefficient equals 0 and $g' \in H$. Hence $\{x', h_1, \ldots, h_{m-1}\}$ generates G and since the set is clearly linearly independent, G must be a lattice. □

Definition 1.61. If $L \subset \mathbb{R}^n$ is lattice generated by $\{e_1, \ldots, e_n\}$, the *fundamental domain* T is the set of elements $\sum a_i e_i$ such that $0 \leq a_i < 1$.

The fundamental domain of a lattice can be seen as one of the 'boxes' of the roster. For example, for the lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$ generated by $(1,0)$ and $(0,1)$, we see that $T = [0,1) \times [0,1)$. Also, by considering the integer parts of the coefficients, we see that for any n-dimensional lattice $L \subset \mathbb{R}^n$ and any $x \in \mathbb{R}^n$, there is a unique $l \in L$ such that $x \in T + l$.

Next, we shall study the the quotient group $\mathbb{R}^n/L$ for lattices L. We denote the direct product of n copies of the (multiplicative) circle group of $S^1 = \{e^{2\pi i x} \mid x \in [0,1)\}$ as $\mathbb{T}^n = S^1 \times \ldots \times S^1$ and will call this the *n-dimensional torus.*

Theorem 1.62. *Suppose that $m \geq n$ are integers and that L is an m-dimensional lattice in $\mathbb{R}^n$. Then $\mathbb{R}^n/L \simeq \mathbb{T}^m \times \mathbb{R}^{n-m}$ as groups.*

Proof. Let V be the m-dimensional span of the generators of L and take a complement space W such that $\mathbb{R}^n = V \oplus W$. Then as groups, $\mathbb{R}^n \simeq V \times W$. We see that $W \simeq \mathbb{R}^{n-m}$ and the map

$$\pi : V \longrightarrow \mathbb{T}^m, \sum_{i=1}^{m} a_i e_i \mapsto (e^{2\pi i a_1}, \ldots, e^{2\pi i a_m})$$

is a surjective group homomorphism with kernel L. □

Corollary 1.63. *If L is an n-dimensional lattice in $\mathbb{R}^n$, the previously defined map π gives a bijection $T \to \mathbb{T}^n$.*

Definition 1.64. For a subset $X \subset \mathbb{R}^n$, we define its *volume* $v(X)$ as the (Lebesgue) integral of 1 over X. This volume exists only if the integral does. Also, if L is an n-dimensional lattice, we use the bijection $\phi := \pi|_T : T \to \mathbb{T}^n$ to define for any subset $Y \subset \mathbb{T}^n$ its volume as $v(Y) = v(\phi^{-1}(Y))$.

Theorem 1.65. *If $X \subset \mathbb{R}^n$ is bounded, $v(X)$ exists and $\pi|_X$ is injective, then $v(\pi(X)) = v(X)$.*

Proof. The idea is to split X into parts using the lattice, bring those parts to the fundamental domain T and then use the bijection ϕ. Firstly, the boundedness of X implies that X intersects only finitely many sets $T + l$ for $l \in L$. Since $\mathbb{R}^n = \cup_{l \in L} T + l$, we can write $X = X_{l_1} \cup \ldots \cup X_{l_m}$, where $X_{l_i} = X \cap (T + l_i)$. We translate this to the fundamental domain by defining $Y_{l_i} = X_{l_i} - l_i \subset T$ (this is a real minus, not a setminus). Since $\pi(x) = \pi(x - l_i)$, the injectivity of $\pi|_X$ implies that the Y_{l_i} are disjoint. Also clearly, $v(X_{l_i}) = v(Y_{l_i})$ since we just applied a translation. Putting this all together gives

$$v(\pi(X)) = v(\pi(\cup X_{l_i})) = v(\pi(\cup Y_{l_i})) = v(\phi(\cup Y_{l_i})) = v(\cup Y_{l_i}) = \sum v(Y_{l_i}) = \sum v(X_{l_i}),$$

which equals $v(X)$, as desired. □

We say that a subset $X \subset \mathbb{R}^n$ is *symmetric* when $x \in X$ implies $-x \in X$.

Theorem 1.66 (Minkowski)**.** *Let L be an n-dimensional lattice in $\mathbb{R}^n$ and X a bounded, convex and symmetric subset of $\mathbb{R}^n$. If $v(X) > 2^n v(T)$, then X contains a non-zero point of L.*

Proof. If L is generated by $\{e_1, \ldots, e_n\}$, let $2L$ be the lattice generated by $\{2e_1, \ldots, 2e_n\}$. It has a fundamental domain $2T$ with volume $v(2T) = 2^n v(T)$. If $\pi : \mathbb{R}^n \to \mathbb{T}^n$ induces the isomorphism $\mathbb{R}^n/2L \simeq \mathbb{T}^n$, then we find that

$$v(\pi(X)) \leq v(\mathbb{T}^n) = v(2T) = 2^n v(T) < v(X),$$

by the assumption. Thus, by Theorem 1.65 there must exist two points $x \neq y \in X$ such that $\pi(x) = \pi(y)$, which means that $x - y \in 2L$ and $\frac{1}{2}(x-y) \in L$. Since X is symmetric, also $-y \in X$ and by convexity $\frac{1}{2}x - \frac{1}{2}y \in X$ as well. □

The crucial idea of the proof is that X needs to overlap itself when you try to squeeze it into the fundamental domain T or, equivalently, in the torus $\mathbb{T}^n$. This theorem might seem trivial at first sight, but the implications it has are enormous. For example, the *four squares theorem*, which states that every positive integer can be written as a sum of four squares, can be proven quite easily using Minkowski's theorem. See [16] page 143 for a proof. But more importantly for us, Minkowski's theorem also has led to many new insights in number theory. In order to use Minkowski's theorem, we need to translate the story of number fields, rings of integers and ideals into that of lattices and vector spaces over $\mathbb{R}$.

Since most information about an element $\alpha \in K = \mathbb{Q}(\theta)$ is captured by its Galois conjugates, we look at them a little closer. Note that if $\tau : K \to \mathbb{C}$ is a homomorphism, then so is $\overline{\tau} : K \to \mathbb{C}$ given by $\overline{\tau}(x) = \overline{\tau(x)}$. We say τ is *real*, when $\tau = \overline{\tau}$ and *complex* when it is not real. So the Galois homomorphisms come in pairs and we may write $n = s + 2t$, where s is the number of real Galois homomorphisms and t the number of complex ones. In the rest of this section, let K, n, s and t be given.

Definition 1.67. The map

$$\sigma : K \longrightarrow \mathbb{C}^n, \quad \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$$

will be referred to as the *geometric representation* of K.

We consider $\mathbb{C}^n$ here as a vector space over $\mathbb{R}$. Notice that σ is a homomorphism since the σ_i are homomorphisms and that is injective since K is a field and σ is non-trivial.

Definition 1.68. If $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$, we define its *norm* $\mathrm{N}(x) = x_1 \cdots x_n$.

This notation should not cause any confusion, since for $\alpha \in K$, we have $\mathrm{N}(\alpha) = \mathrm{N}(\sigma(\alpha))$. Also, we see that $\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$ for any $x, y \in \mathbb{C}^n$.

Theorem 1.69. *If $I \subset (K, +)$ is a finitely generated subgroup generated by $\mathcal{A} = \{\alpha_1, \ldots, \alpha_m\}$, then $\sigma(I)$ is a lattice with generators $\sigma(\alpha_1), \ldots, \sigma(\alpha_m)$. In particular, ideals of $\mathcal{O}_K$ are mapped to lattices.*

The proof amounts to calculating the determinant of a matrix and can be found in [16].

We now focus on proving Dirichlet's unit theorem. Let U be the group of units of $\mathcal{O}$. We would like to use the geometric interpretation of K we just introduced. However, U is a multiplicative group and is hence not mapped to a lattice. Luckily for us, there exists such a thing as the logarithm.

Definition 1.70. The map

$$\ell : \ K^* \longrightarrow \mathbb{R}^n, \ \ x \mapsto (\log|\sigma_1(x)|, \ldots, \log|\sigma_n(x)|)$$

where $|\cdot|$ denotes the usual absolute value on $\mathbb{C}$, is called the *logarithmic representation* of K. Also, we write $\ell_i(x) = \log|\sigma_i(x)|$.

This map is well-defined since for each i, $|\sigma_i(x)| = 0$ if and only if $x = 0$. Notice that $\ell = l \circ \sigma$, where l maps $(x_1, \ldots, x_n)$ to $(\log|x_1|, \ldots, \log|x_n|)$. Moreover, ℓ is clearly a homomorphism between $(K^*, \cdot)$ and $(\mathbb{R}^n, +)$ and

$$\sum_{i=1}^{n} \ell_i(\alpha) = \log|\,\mathrm{N}(\alpha)|.$$

Before we can characterize the 'finite part' of U, we need a lemma.

Lemma 1.71. *If $f \in \mathbb{Z}[x]$ is a monic polynomial such that all roots in $\mathbb{C}$ have absolute value 1, then all roots of f are roots of unity.*

A proof that relies on symmetric polynomials can be found in [16].

Theorem 1.72. *The kernel of $\ell|_U : \ U \to \mathbb{R}^n$ is the set W of roots of unity in $\mathcal{O}_K$, which is a finite group of even order.*

Proof. For each $\alpha \in K$, note that $\ell(\alpha) = 0$ if and only if $|\sigma_i(\alpha)| = 1$ for each i. Suppose that $\ell(\alpha) = 0$. By Lemma 1.20, the field polynomials of α is in $\mathbb{Z}[x]$. So by the previous lemma, α is a root of unity. Conversely, if α is a root of unity, then so are its conjugates, so $|\sigma_i(\alpha)| = 1$ for each i.

Again since all Galois conjugates of a root of unity are roots of unity as well, a root of unity is mapped by σ within a bounded area of $\mathbb{C}^n$. Also, $\sigma(\mathcal{O}_K)$ is a lattice (after identifying $\mathbb{C}^n$ with $\mathbb{R}^{2n}$) by Theorem 1.69 and hence discrete by Theorem 1.60. We conclude that $\mathcal{O}_K$ contains finitely many roots of unity, so in particular W is finite. The order of W is even, since $-1 \in W$. □

Now that we have characterized the kernel of ℓ, we continue by investigating its image.

Lemma 1.73. *The image $E = \ell(U) \subset \mathbb{R}^n$ is a lattice of dimension $\leq s + t - 1$.*

Proof. We first show that E is a lattice. By Theorem 1.60, it is sufficient to show that E is discrete. Consider $r > 0$ and $\epsilon \in U$ such that $||\ell(\epsilon)|| < r$, where $||\cdot||$ denotes the Euclidian norm in $\mathbb{R}^n$. In particular, we find that $|\ell_k(\epsilon)| \leq ||\ell(\epsilon)|| < r$ and hence $|\sigma_k(\epsilon)| < e^r$ for each k. Since $U \subset \mathcal{O}_K$ and $\mathcal{O}_K$ is a finitely generated abelian group, $\sigma(\mathcal{O}_K)$ is a lattice by Theorem 1.69 and hence discrete. We thus find just finitely many $\epsilon \in U$ such that $|\sigma_k(\epsilon)| < e^r$, so in particular finitely many $\epsilon \in U$ such that $||\ell(\epsilon)|| < r$. This proves that E is discrete.

For the dimension, note that

$$|\sigma_i(x)| = |\overline{\sigma_i(x)}| = |\overline{\sigma_i}(x)| \text{ for each } x \in U,$$

which means that the the coordinates of $\ell(x)$ always have t pairs of identical entries. Hence E has dimension $\leq s + 2t - t = s + t$. Also, we know that for any $\epsilon \in U$, we have

$$\sum_{i=1}^{n} \ell_i(\epsilon) = \log |\operatorname{N}(\epsilon)| = \log 1 = 0.$$

We can interpret this as a sum over the $s + t$ not necessarily identical entries with the entries corresponding to a complex σ_i counted twice. From these $s + t$ entries, we can choose $s+t-1$ randomly, after which the last one is fixed. This means that the dimension of E must be $\leq s + t - 1$. □

The last thing about E that we need to find out is its exact dimension. This will turn out to be $s + t - 1$. Before we shall be able to prove this, we need two lemma's. Firstly, we need a more topological description of the dimension of a lattice.

Lemma 1.74. *A lattice L in $\mathbb{R}^m$ has dimension m if and only if there exists a bounded $B \subset \mathbb{R}^m$ such that*

$$\mathbb{R}^m = \cup_{x \in L} x + B.$$

Proof. If L has dimension m, the fundamental domain will serve as the bounded set, as explained below Definition 1.61.

For the converse, suppose that such a B exists and that the dimension of L is strictly smaller than m. If V is the space spanned by L, then we can find a complement W of V and we see that $\mathbb{R}^m = \cup_{x \in V} x + B$. Hence the projection $\pi : \mathbb{R}^m \to W$ has $\pi(B) = W$ as image. However, writing out the distance on $\mathbb{R}^m$ in the bases of V and W, we see that $|\pi(u) - \pi(v)| \leq |u - v|$ for each $u, v \in \mathbb{R}^m$. Therefore, W must be bounded as well, a contradiction when $\dim W \geq 1$. □

Next, we would like to be able to compute the volume of the fundamental domain.

Lemma 1.75. *If L is an m-dimensional lattice in $\mathbb{R}^m$ generated by $\{e_1, \ldots, e_m\}$, then $v(T) = |\det(a_{ij})|$, where T is the fundamental domain of L and $e_i = (a_{1i}, \ldots, a_{ni})$ for each i.*

Proof. This follows from the substitution rule for integrals, using the substitution $x_i = \sum_j a_{ij} y_j$. □

We are now ready to make a crucial step in the proof of Dirichlet's unit theorem. It involves, as was already spoiled, Minkowski's theorem. However, before we do that, we need to be a little more precise about our geometrical representation. So far, we have not specified the order of the homomorphisms σ_i. We shall write them as

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+1}}, \ldots, \overline{\sigma_{s+t}},$$

where the first s are real and the others complex. If we consider $\mathbb{C}$ as a vector space over $\mathbb{R}$, then for $x \in \mathcal{O}_K$, $\sigma_{s+i}(x) = a + bi = (a, b)$ for some $a, b \in \mathbb{R}$ and $\overline{\sigma_{s+i}}(x) = a - bi = (a, -b)$ for each $1 \leq i \leq t$. Moreover, for each $j \leq s$, $\sigma_j(x) = c = (c, 0)$ for some $c \in \mathbb{R}$, so in fact, the image of σ is contained in an $(s+2t)$-dimensional vector space over $\mathbb{R}$ and it is captured fully by the first $s+t$ coordinates of σ (the last t being complex, hence counted twice). Thus, we view σ as $\sigma : K \to \mathbb{L}^{st}$, where $\mathbb{L}^{st} = \mathbb{R}^s \times \mathbb{C}^t$. In this perspective, the definition of the norm slightly changes into $\mathrm{N}(x_1, \ldots, x_{s+t}) = x_1 \cdots x_s \cdot |x_{s+1}|^2 \cdots |x_{s+t}|^2$ for $(x_1, \ldots, x_{s+t}) \in \mathbb{L}^{st}$. We highlight the use of Minkowski's theorem in the following lemma, before we prove the final theorem.

Lemma 1.76. *Suppose that L is an $(s+2t)$-dimensional lattice in $\mathbb{L}^{st}$ with a fundamental domain of volume v and $c_1, \ldots, c_{s+t} \in \mathbb{R}_{>0}$ such that*

$$c_1 \cdots c_s \cdot c_{s+1}^2 \cdots c_{s+t}^2 > \left(\frac{4}{\pi}\right)^t v.$$

Then there exists a non-zero $x \in L \cap X$, where

$$X = \{(x_1, \ldots, x_{s+t}) \in \mathbb{L}^{st} \mid |x_i| < c_i \text{ for each } 1 \leq i \leq s+t\}.$$

Proof. In order to use Minkowski's theorem, we compute $v(X)$. It is a product of s real integrals over $(-c_j, c_j)$ for $1 \leq j \leq s$ and t complex integrals over $\{z \in \mathbb{C} \mid |z| < c_{s+k}\}$ for $1 \leq k \leq t$. Thus, the volume equals

$$v(X) = 2c_1 \cdots 2c_s \pi c_{s+1}^2 \cdots \pi c_{s+t}^2 = 2^s \pi^t c_1 \cdots c_s c_{s+1}^2 \cdots c_{s+t}^2 > 2^{s+2t} v.$$

Since X is clearly bounded, convex and symmetric, Minkowski's theorem now yields the desired result. □

Theorem 1.77. *The image E of U is a lattice of dimension $s + t - 1$.*

Proof. Let $S = \{x \in \mathbb{L}^{st} \mid |\mathrm{N}(x)| = 1\}$. Then we see that S is mapped to the set $V = \{(x_1, \ldots, x_{s+t}) \in \mathbb{R}^{s+t} \mid x_1 + \ldots + x_{s+t} = 0\}$ by coordinate-wise applying $\log|\cdot|$. If we call this map l, then $\ell|_U = (l \circ \sigma)|_U$. By the well-known properties of the logarithm, we can use Lemma 1.74 to conclude that we are done when we can find a bounded $B \subset S$ such that $S = \cup_{\epsilon \in U} \sigma(\epsilon) B$.

In order to find a suitable B, we define $M = \sigma(\mathcal{O}_K)$, which is an $(s+2t)$-dimensional lattice by Theorem 1.25 and Corollary 1.69. Let v be the volume of the fundamental domain of M. Consider $y \in S$ and define the linear map $\lambda_y : \mathbb{L}^{st} \to \mathbb{L}^{st}$ with $\lambda_y(x) = yx$. Then λ_y has determinant $\mathrm{N}(y) = \pm 1$, which is easily seen when considering $\mathbb{L}^{st}$ as a

subset of $\mathbb{C}^{s+2t}$. Hence the bases for the lattices M and yM are related by a unimodular map, which by Lemma 1.75 implies that their fundamental domains have the same volume v. Now choose $c_1, \ldots, c_{s+t} \in \mathbb{R}_{>0}$, such that

$$\delta = c_1 \cdots c_s \cdot c_{s+1}^2 \cdots c_{s+t}^2 > \left(\frac{4}{\pi}\right)^t v.$$

If again $X = \{(x_1, \ldots, x_{s+t}) \in \mathbb{L}^{st} \mid |x_i| < c_i \text{ for each } 1 \leq i \leq s+t\}$, then Lemma 1.76 tells us that we can find a non-zero $x \in yM \cap X$. So for some non-zero $\alpha \in \mathcal{O}_K$, we have $x = y\sigma(\alpha)$. Now $|\,\mathrm{N}(x)| = |\,\mathrm{N}(\alpha)|$, which implies that $|\,\mathrm{N}(\alpha)| < \delta$.

An important fact to realize now is that due to the unique factorization of ideals of $\mathcal{O}_K$ into prime ideals, any ideal has finitely many divisors. In particular, any $m \in \mathbb{Z}$ can be contained in at most finitely many ideals and since $\mathrm{N}(\mathbf{a}) \in \mathbf{a}$ for any ideal $\mathbf{a}$ of $\mathcal{O}_K$, we conclude that there are finitely many ideals with norm m, so also finitely many with norm $< \delta$. Since $|\,\mathrm{N}(a)| = \mathrm{N}((a))$ for each $a \in K$, we find only finitely many pairwise non-associate elements $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K$ with $|\,\mathrm{N}(\alpha_i)| < \delta$ for each i. Then for some $\epsilon \in U$ and some i we have $\alpha_i = \epsilon\alpha$. Finally, we define

$$B = S \cap (\cup_{i=1}^N \sigma(\alpha_i^{-1})X).$$

Note that B is bounded because X is bounded and that B is independent of y since δ and v are. But we now have

$$y = \sigma(\alpha^{-1})x = \sigma(\epsilon)\sigma(\alpha_i^{-1}) \in \sigma(\epsilon)B,$$

as $|\,\mathrm{N}(\sigma(\epsilon))| = 1$. Since y was arbitrary, this completes the proof. □

At last, we can now unify everything we have learned about the unit group U of $\mathcal{O}_K$.

Theorem 1.78 (Dirichlet's unit theorem)**.** *The group of units U of $\mathcal{O}$ is isomorphic to $W \times \mathbb{Z}^{s+t-1}$, where W is the set of roots of unity in $\mathcal{O}_K$ and a finite group of even order.*

Dirichlet's unit theorem can be generalized to special subrings of $\mathcal{O}_K$, which we call orders.

Definition 1.79. Suppose that K is a number field of degree n. An *order* of K is a subring $\mathcal{O} \subset \mathcal{O}_K$ of the ring of integers of K such that $\mathcal{O}$ has an integral basis of size n. The ring of integers $\mathcal{O}_K$ is called the *maximal order*.

Suppose that $\mathcal{O}$ is an order in K with integral basis $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$, so $\mathcal{O} = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Then $\mathcal{A}$ is also a $\mathbb{Q}$-basis for K, so $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Conversely, suppose that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$, where the α_i are algebraic integers. Then $\mathcal{O} = \mathbb{Z}[\alpha_1, \ldots, \alpha_r]$ is a subring of $\mathcal{O}_K$. Since any integral basis for $\mathcal{O}$ is also a $\mathbb{Q}$-basis for K, $\mathcal{O}$ must be an order. Thus, all orders are of the form

$$\mathcal{O} = \mathbb{Z}[\alpha_1, \ldots, \alpha_r],$$

where the α_i are algebraic integers such that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$.

For a subring $R \subset \mathcal{O}_K$, we define its *rank* as the power of $\mathbb{Z}$ in the decomposition of the group of units in R into cyclic groups. The following theorem allows us to use Dirichlet's unit theorem for any order.

Theorem 1.80. *If $\mathcal{O}$ is an order in K, then the rank of $\mathcal{O}$ is equal to the rank of $\mathcal{O}_K$.*

A proof can be found in [15]. We will not go any further into the theory of orders in this thesis. More information on orders can also be found in [15].

Suppose that U is the group of units of an order $\mathcal{O}$.

Definition 1.81. Dirichlet's unit theorem tells us that there exist $s+t-1$ *fundamental units*, which are the units $\eta_1, \ldots, \eta_{s+t-1}$ such that every $\epsilon \in U$ can be written uniquely as

$$\epsilon = \zeta \epsilon_1^{k_1} \cdots \epsilon_{s+t-1}^{k_{s+t-1}},$$

where $\zeta \in U$ is a root of unity.

Dirichlet's unit theorem gives us a lot of information, but it fails to present a way to actually *find* these fundamental units. In general, this question is rather difficult to answer. For specific cubic number fields we can give a criterion for deciding whether an element is a fundamental unit. The following theorem is such an example.

Theorem 1.82. *Let $K = \mathbb{Q}(\theta)$ be a a cubic number field such that the discriminant of θ is negative, where we may choose θ to be real. If ϵ is a unit in the ring of integers of K such that*

$$1 < \epsilon < \left(\frac{d - 32 + \sqrt{d^2 - 64d + 960}}{8} \right)^{\frac{2}{3}},$$

where d is the absolute value of the discriminant of K, then ϵ is a fundamental unit.

Proof. Since the discriminant of θ is negative, we have two complex and one real Galois homomorphism, so $s = t = 1$ and Dirichlet's unit theorem gives us one fundamental unit. If ϵ is such a fundamental unit, so are $-\epsilon, 1/\epsilon, -1/\epsilon$, so we may assume that $\epsilon > 1$. Since the only roots of unity in a real field are ± 1, we can write any unit as $\pm\epsilon^n$ for some $n \in \mathbb{Z}$. The idea is to find a lower bound for ϵ^2. The Galois conjugates of ϵ are complex and they are each others complex conjugates, so let $re^{i\phi}$ be such a conjugate in polar coordinates. Then $\pm 1 = \mathrm{N}_{K/\mathbb{Q}}(\epsilon) = \epsilon \cdot re^{i\phi} \cdot re^{-i\phi} = \epsilon r^2$, so we find that $\epsilon = \frac{1}{r^2}$. Computing the discriminant of the minimum polynomial of ϵ yields

$$\Delta(\epsilon) = -4\sin^2(\phi)\left(r^3 + \frac{1}{r^2} - 2\cos(\phi)\right).$$

Now one can check that the function $f(x, \phi) = -4\sin^2(\phi)\,(x - 2\cos\phi) - 4x^2$ is bounded from above by 16. Hence we get that $|\Delta(\epsilon)| \leq 4(r^3 + r^{-3})^2 + 16 = 4(\epsilon^2 + \epsilon^{-2} + 8)$. We defined the discriminant Δ of K as the determinant of a matrix defined by an integral basis $\mathcal{A}$ for $\mathcal{O}_K$. Note that $\mathbb{Z}[\epsilon] \subset \mathcal{O}_K$ is an additive subgroup with $\mathbb{Z}$-basis $\mathcal{E} = \{1, \epsilon, \epsilon^2\}$ (since $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = 3$). By Theorem 1.4, the index $|\mathcal{O}_K/\mathbb{Z}[\epsilon]|$ is finite and equals the determinant of A, where $A = (a_{ij})$ is the $\mathbb{Z}$-matrix that converts from the basis of $\mathcal{O}_K$ to the basis of $\mathbb{Z}[u]$. As in the proof of Lemma 1.23, we then find that

$\Delta(\mathcal{E}) = (\det A)^2\Delta(\mathcal{A})$. If we compute $\Delta(\mathcal{E})$ using the Vandermonde determinant, we find that $\Delta(\mathcal{E}) = \Delta(\epsilon)$, which shows that

$$d = |\Delta(\mathcal{A})| \leq |\Delta(\epsilon)| \leq 4\left(\epsilon^3 + \frac{1}{\epsilon^3} + 8\right).$$

The above equation is quadratic in ϵ^3 and can hence be solved for ϵ^3. Taking the $\frac{2}{3}$-rd power shows that ϵ^2 is larger than the right hand side of the desired upper bound for ϵ, which equals the expression given in the theorem. □

Remark 1.83. The theorem can be formulated even a little stronger than presented here. Namely, if ϵ is a unit in the ring of integers of a number field K, then for any $k \in \mathbb{Z}_{>1}$, we have that

$$1 < \epsilon < \left(\frac{d - 32 + \sqrt{d^2 - 64d + 960}}{8}\right)^{\frac{k}{3}}$$

implies that ϵ is at most a $(k-1)$-th power of the fundamental unit. In practice, if we wanted to prove that a unit ϵ is fundamental and the criterium of Theorem 1.82 fails, we can at least find this k and try to check explicitly that ϵ cannot be a $1, 2, \ldots, (k-1)$-th power of the fundamental unit.

Dirichlet's unit theorem has lots of applications in the theory of Diophantine equations. We will see some of these in Chapter 3, but Pell's equation is also a nice example.

Theorem 1.84. Pell's equation $x^2 - dy^2 = 1$ *has infinitely many integer solutions* (x, y) *for any square-free* $d \in \mathbb{Z}_{>0}$.

Proof. We can rewrite the equation as $\mathrm{N}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = 1$. Thus, we consider $\mathbb{Q}(\sqrt{d})$. Since $d > 0$, both monomorphisms $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ are real, so $s = 2$ and $t = 0$. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ by Example 1.30. Dirichlet's unit theorem now says that the unit group contains precisely one factor of $\mathbb{Z}$. So if the ring of integers equals $\mathbb{Z}[\sqrt{d}]$, then all infinitely many units are of the form $x + \sqrt{d}y$ for $x, y \in \mathbb{Z}$ and they have norm 1, which means that (x, y) are all integer solutions to Pell's equation. If the ring of integers equals $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$, then $\mathbb{Z}[\sqrt{d}]$ is an order, so by Theorem 1.80 we find infinitely many solutions as well. We can also show this explicitly.

Suppose $d \equiv 1 \pmod 4$. Then we have infinitely many half- integer solutions of $x^2 - dy^2 = 1$. In particular, we can find solutions $z_1 = x_1 + y_1\sqrt{d}$ and $z_2 = x_2 + y_2\sqrt{d}$ such that $z_2 \neq \pm z_1$, $x_1 \equiv x_2 \pmod 4$ and $y_1 \equiv y_2 \pmod 4$. But then $z_1 z_2^{-1}$ is a solution to Pell's equation and we see that

$$z_1 z_2^{-1} = (x_1 + y_1\sqrt{d})\frac{1}{4}(x_2 - y_2\sqrt{d}) = \frac{x_1x_2 - dy_1y_2}{4} + \frac{x_2y_1 - x_1y_2}{4}\sqrt{d}$$

and the latter is in $\mathbb{Z}[\sqrt{d}]$. Since $z_1 \neq \pm z_2$, we see that $z_1 z_2^{-1} \neq \pm 1$ and hence all its infinitely many powers are solutions to Pell's equation as well. □

The question of finding the integer solutions to Pell's equation has thus been reduced to finding the fundamental unit of $\mathbb{Q}(\sqrt{d})$.

2 p-Adic numbers

In this chapter we study the p-adic numbers, which form a key tool for solving many Diophantine equations. Throughout this entire chapter, p is a prime number. The first mathematician to introduce the p-adic numbers was the German Kurt Hensel in 1897. He was inspired by earlier work on power series by Weierstrass, who was one of Hensel's teachers. Hensel realized that he needed some kind of p-adic theory when he became interested in the exact power of a prime p that divides the discriminant of a number field.

Nowadays, one of the most important applications of p-adic numbers is in Diophantine equations. The p-adic numbers can give 'local' information about the solutions of Diophantine equations, where 'local' refers to the information contained in the prime number p. Therefore, the study of p-adic numbers is often referred to as 'local number theory', whereas the content of Chapter 1 is called 'global number theory'. The results of this chapter are fundamental for the approach to Diophantine equations described in Chapter 3.

2.1 The construction of the p-adic numbers

In this section, we will construct the p-adic numbers as the completion of the rational numbers $\mathbb{Q}$ with respect to the p-adic norm. The p-adic norm is a norm we can define on $\mathbb{Q}$ such that two elements $a, b \in \mathbb{Q}$ are close whenever their difference is divisible by a high power of the prime number p. We begin with the definition of a norm on a field.

Definition 2.1. A *norm* or *absolute value* on a field F is a map $|\cdot| : F \longrightarrow \mathbb{R}_{\geq 0}$ such that for each $x, y \in F$

(i) $|x| = 0$ if and only if $x = 0$,

(ii) $|x \cdot y| = |x| \cdot |y|$ and

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

Definition 2.2. The *p-adic valuation* $\mathrm{ord_p}$ is defined for $n \in \mathbb{Z} \setminus \{0\}$ as $\mathrm{ord_p}(n) = \max\{m \in \mathbb{Z} \mid p^m \mid n\}$. Then for$a, b \in \mathbb{Z} \setminus \{0\}$, we define $\mathrm{ord_p}(a/b) = \mathrm{ord_p}(a) - \mathrm{ord_p}(b))$. The *p-adic norm* $|\cdot|_p$ on $\mathbb{Q}$ is defined as $|0|_p = 0$ and for $y \in \mathbb{Q}^*$ as

$$|y|_p = p^{-\mathrm{ord_p}(y)}.$$

The standard absolute value $x \mapsto \max(x, -x)$ on $\mathbb{Q}$ will be denoted as $|\cdot|_\infty$ and the trivial norm that maps $\mathbb{Q}^*$ to $\{1\}$ and 0 to 0 will be denoted by $|\cdot|_1$.

Notice that if you would somehow define a "1-adic valuation" on $\mathbb{Q}$, then the trivial norm would equal the "1-adic norm".

It is not difficult to prove that $\mathrm{ord_p}(x+y) \leq \min(\mathrm{ord_p}(x), \mathrm{ord_p}(y))$ for each $x, y \in \mathbb{Q}^*$, which is equivalent to the following crucial lemma.

Lemma 2.3. *For any $x, y \in \mathbb{Q}$ we have*

$$|x+y|_p \leq \max(|x|_p, |y|_p).$$

Using this lemma, it can easily be shown that $|\cdot|_p$ indeed defines a norm on $\mathbb{Q}$. The reader might notice that for a prime ideal $\mathbf{p}$, we can likewise define a $\mathbf{p}$-adic valuation on any number field K, using the unique factorization of ideals. This is true and in Section 2.5 we will show that such '$\mathbf{p}$-adic norms' can be completely described by p-adic norms. Therefore, we shall study the p-adic case.

Definition 2.4. Any norm $|\cdot|$ on a field F satisfying $|x+y| \leq \max(|x|, |y|)$ for each $x, y \in \mathbb{Q}$ is called *non-archimedian*. A norm that is not non-archimedian is called *archimedian*.

The non-archimedian property of a norm immediately gives rise to some interesting results.

Lemma 2.5. *If F is a field with a non-archimedian norm, then*

$$\sum_{n=1}^{\infty} a_n \text{ converges } \iff a_n \longrightarrow 0.$$

Lemma 2.6. *For any non-archimedian norm $|\cdot|$ on a field F and for each $x, y \in F$, the equality $|x \pm y| = \max(|x|, |y|)$ holds whenever $|x| \neq |y|$.*

Proof. Say wlog that $|x| < |y|$. Then we find that $|x-y| = |y-x| \leq |y|$. However, we also see that

$$|y| = |x-(x-y)| \leq \max(|x|, |x-y|) = |x-y|.$$

Replacing y by $-y$ will do the rest. □

The following examples show how counterintuitive non-Archimedian norms can be. In both examples, consider a field F together with a non-archimedian norm $|\cdot|$ on F.

Example 2.7. As an interesting consequence of Lemma 2.6, consider a triangle with points x, y and z in F. We may assume $z = 0$. Then we see from the above lemma that either $|x| = |y|$ or the length of one of the two is equal to $|x-y|$, the third side. Hence every triangle is isosceles!

Example 2.8. Another nice result is that any element of a sphere is a center. Consider the sphere $B_a(r) = \{x \in F \mid |x-a| < r\}$ around a with radius r and take $b \in F$ such that $|b-a| = r$. Then for $y \in B(a, r)$, we have $|y-a| < r$ and hence

$$|y-b| = |y-a-(b-a)| = \max(|y-a|, |b-a|) = r.$$

In order to see that the p-adic and q-adic norms are really different when p and q are distinct primes, we would like to be able to compare norms to each other. The most intuitive way of defining two norms $|\cdot|_1$ and $|\cdot|_2$ on a field F to be equivalent is when their induced metrics induce the same topologies. Clearly, this is the case when there exists a positive $\alpha \in \mathbb{R}$ such that $|x|_1 = |x|_2^\alpha$ for each $x \in F$, since only the radii of the open balls differ. It is also true, but less trivial, that for any two equivalent norms there exists such an α. A proof of this fact can be found in [7]. The following Theorem by Ostrowski motivates the study of p-adic norms.

Theorem 2.9 (Ostrowski)**.** *Every norm $|\cdot|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$, where p is either ∞, 1 or a prime.*

For a proof, see [9]. In other words, Theorem 2.9 says that, up to equivalence, the p-adic norms constitute all norms on $\mathbb{Q}$, except for the standard and trivial norms. However, we still need to see that all these norms are indeed inequivalent. If $p \neq q$ are primes, then $|p^n|_p = p^{-n}$, while $|q^n|_p = 1$ and vice versa, which shows that $|\cdot|_p$ and $|\cdot|_q$ are not equivalent. Futhermore, the standard and trivial norm are clearly not equivalent to any p-adic norm or each other.

The following theorem allows us to define the p-adic numbes.

Definition/theorem 2.10. *If $(F, |\cdot|)$ is a normed field, then there exists a unique (up to isomorphisms) smallest complete normed extension field K of F such that the norm on K also extends the norm on F. Moreover, $K = \mathcal{C}/\sim$, where $\mathcal{C}$ is the set of Cauchy sequences in F and for $x = (x_n)$ and $y = (y_n)$ in $\mathcal{C}$, we have $x \sim y$ when $\lim_{n\to\infty}(x_n - y_n) = 0$. The inclusion is given by the injection*

$$\iota : F \longrightarrow K, \quad x \mapsto [x, x, x, \ldots],$$

which has a dense image. Also, the norm $|\cdot|$ on K is defined for $x = [(x_n)] \in K$ as $|x| = \lim_{n\to\infty} |x_n|$ (and this is well-defined). The field K is complete and is called the completion of F *with respect to $|\cdot|$.*

The proof of this theorem is very similar to the standard proof that $\mathbb{R}$ is the completion of $\mathbb{Q}$ and has therefore been omitted. We are now able to define the *p-adic numbers* $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic norm. Also, we define the *p-adic integers* $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \,|\, |x|_p \leq 1\}$. By the non-archimedianity of $|\cdot|_p$, this is a subring of $\mathbb{Q}_p$ under addition. A first observation is that the image of the p-adic norm does not change.

Lemma 2.11. *The image of $|\cdot|_p$ of remains $\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}$ after extending its domain to $\mathbb{Q}_p$.*

Proof. If (x_n) is a Cauchy sequence in $\mathbb{Q}$, note that either $0 = x = [(x_n)] \in \mathbb{Q}_p$ or there exist $\epsilon, N > 0$ such that $|x_i|_p > \epsilon$ for each $i \geq N$. By the Cauchy property, there exists an $M > 0$ such that for any $i, j > M$ we also have $|x_i - x_j|_p < \epsilon$. Thus, for $i, j > \max(N, M)$ Lemma 2.6 implies that $|x_i|_p = |x_j|_p$. Therefore, $|x_n|_p$ is constant when n is large enough and $|x|_p = |x_k|_p$ for each $k > \max(N, M)$, so the image of $|\cdot|_p$ does not change. □

The following two lemma's prepare for Theorem 2.14, which will shed new light on the p-adic numbers.

Lemma 2.12. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any $i \in \mathbb{Z}_{\geq 0}$ there exists an integer $\alpha \in \mathbb{Z}$ such that $|\alpha - x|_p \leq p^{-i}$. This integer α can be chosen smaller than p^i.*

Proof. If we write $x = a/b$ 'in lowest terms', then $|x|_p \leq 1$ means that p^i and b are relatively prime. Hence there exist integers m, n such that $mb + np^i = 1$. We can then take $\alpha = am + kp^i$ for $k \in \mathbb{Z}$ such that $\alpha < p^i$. □

In particular, this lemma says that $\mathbb{Z} \subset \mathbb{Z}_p$ is dense.

Lemma 2.13. *Every element $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$ has a unique representative Cauchy sequence of the form (a_i) for which:*

(1) $a_i \in \{0, 1, \ldots, p^i - 1\}$ and

(2) $a_i \equiv a_{i+1} \pmod{p^i}$ for all $i \geq 1$.

Proof. For uniqueness, suppose we have two such representations (a_i) and (b_i) that are unequal, so for some j we have $a_j \neq b_j$. By (1), also $a_j \not\equiv b_j \pmod{p^j}$. It follows by (2) that for all $i > j$ we have $a_i \not\equiv b_i \pmod{p^j}$ and hence $|a_i - b_i|_p > p^{-j}$, which clearly implies $a \not\sim b$.
For existence, take a representation (b_i) for a. We can define $N(j)$ such that $N(j) \geq j$ and $i, i' \geq N(j)$ implies $|b_i - b_{i'}|_p \leq p^{-j}$. Then for any $i \geq N(1)$ it follows from the non-archimedian property that $|b_i|_p \leq 1$. We may then apply the previous lemma to $b_{N(j)}$ for each j and the resulting sequence (α_j) will suffice. □

Theorem 2.14. *We have*

$$\mathbb{Q}_p = \left\{ \sum_{i=-m}^{\infty} \iota(a_i p^i) \mid 0 \leq a_i < p^i,\ a_{-m} \neq 0,\ m \in \mathbb{Z} \right\},$$

where $\iota : \mathbb{Q} \to \mathbb{Q}_p$ is the inclusion of the completion.

Proof. If $a \in \mathbb{Q}_p$ we can find an m such that for $a' = ap^m$, we have $|a'|_p \leq 1$. Let (a'_i) be a representation for a' satisfying (1) and (2) from Lemma 2.13. Also, define $a_i = p^{-m} a'_i$. When we write a'_i in base p, we see that condition (1) implies that the highest occurring power of p is $i-1$ and that (2) means that $a'_{i+1} = a'_i + b_i p^i$ for some non-negative integer $b_i < p^i$. We conclude that a_{i+1} is a partial sum of the form $a_{i+1} = \sum_{k=-m}^{i} b_k p^k$. Clearly these partial sums are Cauchy, hence there exists a limit in $\mathbb{Q}_p$, which we denote by $\sum_{k=-m}^{\infty} \iota(b_k p^k)$. This limit is clearly equivalent to a. On the other hand, any such limit represents an element of $\mathbb{Q}_p$ by definition. □

If $x = \sum_{i=-m}^{\infty} \iota(a_i p^i) \in \mathbb{Q}_p$, this sum is called the *p-adic expansion* of x. Theorem 2.14 allows us to view $\mathbb{Q}_p$ as the set of p-adic expansions. This emphasizes the way we can think of the p-adic numbers as a way of looking modulo all powers of the prime number

p at the same time. Note that $\mathbb{Z}_p$ is the set of elements with no negative powers of p in its p-adic expansion.

In the rest of this chapter, we will just write x when we actually mean the constant sequence $\iota(x)$.

We finish this section with an important property of the p-adic numbers. It says that we can 'lift' factorizations modulo p to $\mathbb{Q}_p$.

Theorem 2.15 (Hensel's Lemma)**.** *Suppose that $f \in \mathbb{Z}_p[x]$ has modulo p a factorization $\overline{f} = \tilde{g}\tilde{h} \in \mathbb{F}_p[x]$, where $\overline{f} := f \pmod p$ and $\tilde{g}, \tilde{h} \in \mathbb{F}_p[x]$ relatively prime and $\tilde{g}$ monic. Then there exist $g, h \in \mathbb{Z}_p[x]$ such that g is monic, $\overline{g} = \tilde{g} \in \mathbb{F}_p[x]$, $\overline{h} = \tilde{h} \in \mathbb{F}_p[x]$ and $f = gh$.*

For a proof, see page 74 of [7].

2.2 From $\mathbb{Q}_p$ to $\mathbb{C}_p$

In this section, we study more algebraic properties of $\mathbb{Q}_p$. This will result in the conclusion that $\mathbb{Q}_p$ is not algebraically closed and hence we construct its algebraic closure $\overline{\mathbb{Q}_p}$. It turns out that $\overline{\mathbb{Q}_p}$ is not complete anymore, but its completion $\mathbb{C}_p$ will be shown to be algebraically closed. We need to construct $\mathbb{C}_p$ in order to be able to do analysis on the p-adic numbers in the coming sections. This section will be of a more algebraic kind and therefore requires the prerequisite knowledge of the theory of field extensions and some Galois theory. We start by investigating the local compactness of $\mathbb{Q}_p$ and its finite extensions.

Definition 2.16. If F is a field with a non-archimedian norm $|\cdot|$, then the *valuation ring* of F is $V_F = \{x \in F \mid |x| \leq 1\}$ and its unique maximal ideal will be denoted by $\mathbf{p}_F = \{x \in F \mid |x| < 1\}$. The *residue field* of F is the quotient $V_F/\mathbf{p}_F =: V_F/\mathbf{p}$.

Theorem 2.17. *If K is a field with a non-archimedian norm $|\cdot|$ that is complete such that the maximal ideal of the valuation ring $\mathbf{p}_K = (x)$ is principal, then K is locally compact if and only if its residue field is finite.*

Proof. Firstly, we prove that K is locally compact if and only if V_K is compact. Clearly, if V_K is compact, then any ball $B_a(r^+) = \{y \,|\, |y - a| \leq r\}$, where $a \in K$ and $r > 0$, is compact and if K is locally compact, there exists a ball $B_a(r^+)$ that is compact and hence V_K is compact. There are obvious continuous maps between such balls.

Also, V_K is compact if and only if V_K is complete and totally bounded (see [13] page 52 for a proof). Since V_K is closed in a complete set it is complete. We show that V_K is totally bounded if and only if $V_K/\mathbf{p}$ is finite. Note first that $(x^n) = \{y \in K \,|\, |y| \leq |x|^n\}$. Suppose $V_K/(x)$ is finite. We will show by induction that $V_K/(x^n)$ is finite. The trivial surjective homomorphism $V_K/(x^n) \longrightarrow V_K/(x^{n-1})$ has kernel $(x^{n-1})/(x^n)$, which is isomorphic to $V_K/(x)$ by mapping $a + (x)$ to $x^{n-1}a + (x^n)$. Hence the kernel is finite and by the induction hypothesis, so is the image. This implies that $V_K/(x^n)$ is finite as

well. We can then cover V_K by finitely many (open!) sets of the kind $a + (x^n)$, where $a \in V_K$. Since $|x^n| \longrightarrow 0$, this shows the total boundedness.

For the converse, suppose we could cover V_K with finitely many balls of radius ϵ for any $\epsilon > 0$. Let $\{B_i \,|\, 1 \leq i \leq n\}$ be a set of balls of radius $|x|/2$ that cover V_K and let a_i be a center of B_i. Then the sets $\{a_i + (x) \,|\, 1 \leq i \leq n\}$ cover V_K, which means that $V_K/(x)$ is finite. □

If K is a finite extension of $\mathbb{Q}_p$ and $x, y, \pi \in V_K$, we write $x \equiv y \pmod{\pi}$ when $x - y \in (\pi)$, the ideal in V_K generated by π. If $K = \mathbb{Q}_p$, note that $x \equiv y \pmod{p^n}$ iff $|x - y|_p \leq p^{-n}$ iff $x - y$ has a p-adic expansion without any entries before p^n, so this is an extension of the regular modulus on $\mathbb{Z}$.

Lemma 2.18. *The maximal ideal of the valuation ring $\mathbb{Z}_p$ of $\mathbb{Q}_p$ is $p\mathbb{Z}_p = (p)$ and for each $n \in \mathbb{Z}_{\geq 1}$, $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$, making $\mathbb{Z}_p$ compact and $\mathbb{Q}_p$ locally compact. Also, there are no other ideals in $\mathbb{Z}_p$ besides $p^n\mathbb{Z}_p$, where $n \in \mathbb{Z}_{\geq 1}$.*

Proof. The subring $p\mathbb{Z}_p$ is clearly the only maximal ideal of $\mathbb{Z}_p$. Furthermore, the quotient map $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ mapping x to $x \pmod{p^n}$ is surjective by Lemma 2.12 and has kernel $p^n\mathbb{Z}_p$. Lastly, if I is an ideal with greatest occurring norm p^{-n}, then $I = p^n\mathbb{Z}_p$. □

We would now like to be able to extend our norm on $\mathbb{Q}_p$ to (finite) extension fields. Recall that any two norms $|\cdot|_1$ and $|\cdot|_2$ on a vector space V over a locally compact field F are equivalent if and only if there exist constants $c_1, c_2 \in \mathbb{R}_{>0}$ such that $c_1|x|_1 \leq |x|_2 \leq c_2|x|_2$. Then, in the same way as on page 6 of [10], we can prove the following theorem.

Theorem 2.19. *All norms on a finite dimensional vector space V over a locally compact field F are equivalent.*

Corollary 2.20. *If $V = K$ is a vector space over F that is a field, then there exists at most one norm on K that extends the norm $|\cdot|$ on F.*

Proof. Suppose $|\cdot|_1$ and $|\cdot|_2$ are unequal norms on K that extend $|\cdot|$, say $|x|_1 < |x|_2$ for some $x \in K$. By the previous theorem, there exists a constant $c \in \mathbb{R}_{>0}$ such that $|x|_2 \leq c|x|_1$ for all $x \in K$. For sufficiently large $N \in \mathbb{Z}_{>0}$, however, we find that $c|x^N|_1 < |x^N|_2$. □

For the following lemma and theorem, let F be a locally compact field and $K \supset F$ a finite extension. We now want to extend the norm on F to K. To do this, we use the "norm" $\mathrm{N}_{K/F}$ of the field extension $F \subset K = F(\alpha)$.

Lemma 2.21. *If there exists a norm $||\cdot||$ on K that extends the norm $|\cdot|$ on F, then for $\alpha \in K$*

$$||\alpha|| = |\,\mathrm{N}_{K/F}(\alpha)|^{1/[K:F]}.$$

Proof. Let n be the degree of α and $L \ni \alpha$ a finite Galois extension of F. Then L contains all the conjugates of α. Suppose we have a norm $||\cdot||$ on L that is an extension of $|\cdot|$. For any conjugate α_i, let $\sigma_i \in \mathrm{Gal}(L/F)$ such that $\sigma_i(\alpha) = \alpha_i$. Then $|\cdot|_i$ defined by $|x|_i = |\sigma_i(x)|$ is also a norm extending $|\cdot|$. Hence by the previous corollary, they are equal and thus we conclude that $|\,\mathrm{N}_{F(\alpha)/F}(\alpha)| = ||\alpha||^n$, leaving only one option of defining $||\cdot||$:

$$||\alpha|| = |\,\mathrm{N}_{F(\alpha)/F}(\alpha)|^{1/n} = |\,\mathrm{N}_{K/F}(\alpha)|^{1/[K:F]},$$

where we have used Lemma 1.28. □

Of course, the next thing to do is to check whether this indeed gives us a norm.

Theorem 2.22. *There exists a unique non-archimedian norm on K extending the norm $|\cdot|$ on F.*

Since $\mathrm{N}_{K/F}$ is multiplicative and $\mathrm{N}_{K/F}(\alpha) = 0$ iff $\alpha = 0$ for each $\alpha \in K$, the only thing worth proving is the non-archimedianity. Proofs can be found on page 152 of [7] and page 61 of [9]. Since $\mathbb{Q}_p$ is locally compact, this procedure applies to finite extensions K of $\mathbb{Q}_p$. Note that the image of the norm in K is then contained in $\{p^q \,|\, q \in \mathbb{Q}\}$.

We define $\overline{\mathbb{Q}_p}$ as the (unique) algebraic closure of $\mathbb{Q}_p$. Since $|\cdot|_p$ extends uniquely to any algebraic extension of $\mathbb{Q}_p$, it also extends uniquely to $\overline{\mathbb{Q}_p}$. Also note that on $\overline{\mathbb{Q}_p}$, we have $\mathrm{Im}\,|\cdot|_p = \{p^q \mid q \in \mathbb{Q}\} \cup \{0\}$, since for example, $x^b - p^{-a}$ has a root $p^{-a/b}$ with norm $p^{a/b}$ for $a, b \in \mathbb{Z}$.

Remember that we were looking for a complete algebraic closure of $\mathbb{Q}_p$. It turns out that $\overline{\mathbb{Q}_p}$ is not complete. In order to prove this, we need to understand more about finite extension of $\mathbb{Q}_p$ first. From now on, we consider a finite extension K of $\mathbb{Q}_p$.

We can extend the order to elements $\alpha \in K$ by

$$\mathrm{ord_p}\,\alpha := -\log_p |\alpha|_p = -\log_p |\,\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n} = -\frac{1}{n}\log_p |\,\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p.$$

By Lemma 1.28(ii), $\mathrm{N}_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$, so we see that the image of K under $\mathrm{ord_p}$ is contained in $\frac{1}{n}\mathbb{Z}$. Since it is a subring under addition, it is of the form $\frac{1}{e}\mathbb{Z}$ where $e \in \mathbb{Z}$ divides n. This motivates the following definition.

Definition 2.23. The number $e \in \mathbb{Z}$ such that $\mathrm{Im}\,\mathrm{ord_p} = \frac{1}{e}\mathbb{Z}$ is called the *index of ramification* of K. If $e = 1$, K is an *unramified* extension of $\mathbb{Q}_p$ and if $e = n$, it is called *totally ramified*.

If e is the ramification index of K, we see that the maximal ideal $\mathbf{p}_K$ in the valuation ring $\mathcal{O}_K$ of K is principal and equal to (π), where $\pi \in K$ such that $\mathrm{ord_p}\,\pi = 1/e$. Since K is also complete because $\mathbb{Q}_p$ is complete, we conclude from Theorem 2.17 the following.

Corollary 2.24. *Any finite extension K of $\mathbb{Q}_p$ is locally compact.*

Note that if $\pi \in K$ is such that $\mathrm{ord_p}\,\pi = 1/e$, then any $x \in K$ can uniquely be written in the form $x = \pi^m \cdot u$. Just take $m = e \cdot \mathrm{ord_p}\,x$ and $u = x/\pi^m$.

Lemma 2.25. *Let $\mathbb{Q}_p \subset K$ be a finite extension of degree n with ramification index e such that the extension $\mathbb{F}_p \subset \mathcal{O}_K/\mathbf{p}$ is of degree f. Then $n = e \cdot f$.*

It can be proved that, if $\pi \in K$ has $\mathrm{ord_p}\,\pi = 1/e$ and if $\{\overline{y_i} \mid |y_i|_p = 1,\, 1 \leq i \leq f\}$ is a basis for $\mathcal{O}_K/\mathbf{p}$, then $\{\pi^j y^i \,|\, 1 \leq i \leq f,\, 0 \leq j \leq e-1\}$ is a basis for K over $\mathbb{Q}_p$. The details are rather tedious and can be found in [7]. The following lemma helps to characterize the unramified extensions of $\mathbb{Q}_p$. This will be important for proving that $\overline{\mathbb{Q}_p}$ is not complete.

Lemma 2.26. *There is exactly one unramified extension $K_f \supset \mathbb{Q}_p$ of degree f, which can be obtained by adjoining a primitive (p^f-1)th root of unity. If K is an extension of degree n with residue field of degree f and index of ramification e, then $K = K_f(\pi)$, where π is the root of an Eisenstein polynomial over K_f.*

Proof. We only prove the existence of K_f. Let $\overline{\alpha}$ be a generator of the cyclic group $\mathbb{F}_{p^f}^{\times}$. It's minimum polynomial $\overline{P}(x) = x^f + b_{f-1}x^{f-1} + \ldots + b_0$ over $\mathbb{F}_p$ has degree f, since $\mathbb{F}_{p^f} \subset \mathbb{F}_p(\overline{\alpha})$. Define $P(x) = x^f + a_{f-1}x^{f-1} + \ldots + a_0 \in \mathbb{Z}_p[x]$, where $\overline{a_i} = b_i$ for each i. Then $P(x)$ is irreducible over $\mathbb{Q}_p$, since if it weren't, we could use Gauss' Lemma to write is as a product of two polynomials in $\mathbb{Z}_p[x]$ and reducing modulo p would give a factorization of $\overline{P}$. Let $\alpha \in \overline{\mathbb{Q}_p}$ be a root of P. Now let $K_f = \mathbb{Q}_p(\alpha)$. Then $\alpha + \mathcal{O}_{K_f}$ is a root of $\overline{P} \in \mathbb{F}_p[x]$. We conclude that $[\mathcal{O}_{K_f}/\mathbf{p}_{K_f} : \mathbb{F}_p] = f \geq [K_f : \mathbb{Q}_p]$. The other inequality holds by Lemma 2.25. □

A proof for the rest of the theorem can be found in [9]. The proof makes use of the following lemma, which is also crucial for proving Theorem 2.29.

Lemma 2.27. *If $K \supset \mathbb{Q}_p$ with $0 \neq x \in \mathcal{O}_K$, there exists $a \in \mathcal{O}_K$ such that a is a (p^f-1)th root of unity and $x \equiv a \pmod{\pi}$, where π is an element of K with $\mathrm{ord_p}\,\pi = 1/e$.*

The proof is quite straightforward and can be found on page 67 of [9]. We first characterize precisely which extensions of $\mathbb{Q}_p$ are unramified.

Theorem 2.28. *The finite unramified extensions of $\mathbb{Q}_p$ are precisely the extensions $\mathbb{Q}_p(\alpha)$, where α is an mth root of unity such that p does not divide m.*

Proof. By Lemma 2.26, any finite unramified extension can be obtained by adjoining a (p^f-1)th root of unity for some f and clearly p does not divide that. For the converse, suppose $p \nmid m$ and let f be the order of $\overline{p}$ in $(\mathbb{Z}/m\mathbb{Z})^*$. Then $p^f - 1 = mn$ for some n. If α is a primitive (p^f-1)th root of unity, then α^n is a primitive mth root of unity and $\mathbb{Q}_p(\alpha^n) \subset \mathbb{Q}_p(\alpha)$ hence $\mathbb{Q}_p \subset \mathbb{Q}_p(\alpha^n)$ is an unramified extension. □

We are now ready to prove a generalization of Theorem 2.14 for finite extensions of $\mathbb{Q}_p$.

Theorem 2.29. *Let $K \supset \mathbb{Q}_p$ be a finite extension of degree n, with ramification index e and residue field of degree f and take $\pi \in K$ such that $\mathrm{ord_p}\,\pi = 1/e$. Then every element $x \in K$ can be written uniquely in the form $x = \sum_{i=m}^{\infty} a_i \pi^i$, where $m = \mathrm{ord_p}(x) \cdot e$ and each a_i is either 0 or a (p^f-1)th root of unity.*

Proof. Take $x \in \mathcal{O}_K$. We can use the previous lemma to find a unique $a_0 \in K$ such that $x \equiv a_0 \pmod{\pi}$ and $a_0^{p^f} = a_0$ (a_0 equals 0 iff $x \equiv 0 \pmod{\pi}$). Now we want to find an $a_1 \in A$ such that $x \equiv a_0 + a_1\pi \pmod{\pi^2}$ and $a_1^{p^f} = a_1$. The first condition is equivalent to $a_1 \equiv (x - a_0)/\pi \pmod{\pi}$. We may again apply the previous lemma (remembering that $(x - a_0)/\pi \equiv 0 \pmod{\pi}$ iff $a_1 = 0$), now with $(x - a_0)/\pi$ as our 'x'. Continuing in this fashion, we construct $a_2, a_3, \ldots$. The partial sums clearly form a Cauchy sequence, since $|\pi^i - \pi^j|_p \leq \max(p^{-i/e}, p^{-j/e})$. Since K is a finite extension of the complete space $\mathbb{Q}_p$, it is complete as well and the limit indeed makes sense. Now if $x \in K$, then we can write $x = \pi^m \cdot u$ for $m = e \cdot \mathrm{ord_p}\, x$ and $|u|_p = 1$, hence $u \in \mathcal{O}_K$. □

If $x = \sum_{i=m}^{\infty} a_i \pi^i$, this sum is called the *π-adic expansion* of that element.

We can now start to prove that $\overline{\mathbb{Q}_p}$ is not complete. The following lemma will be the crucial argument in the proof.

Lemma 2.30. *Suppose $\xi \in \overline{\mathbb{Q}_p}$ is algebraic over $\mathbb{Q}_p$ of degree n. Then there exists an arbitrarily large integer N such that*

$$a_{n-1}\xi^{n-1} + \ldots + a_1\xi + a_0 \not\equiv 0 \pmod{p^N}$$

for any coefficients $a_i \in \mathbb{Z}_p$ such that at least one is not divisible by p.

Proof. Let $M \in \mathbb{Z}_{>0}$. Suppose for each $N \geq M$ there did exist coefficients $a_{i,N}$ such that $\sum_{i=0}^{n-1} a_{i,N}\xi^i \equiv 0 \pmod{p^N}$. Since $\mathbb{Z}_p \subset \mathbb{Q}_p$ is compact, there exists a sequence (N_{j_1}) in $\mathbb{Z}_{\geq 0}$ such that $(a_{n-1,N_{j_1}})_{j_1}$ is a convergent subsequence of $(a_{n-1,N})_N$. In the same way, we find a subsequence (N_{j_2}) of (N_{j_1}) such that $(a_{n-2,N_{j_2}})$ is convergent and continuing in this fashion, we find a sequence $(N_{j_n})_{j_n}$ in $\mathbb{Z}_{\geq 0}$ such that for each i, $(a_{i,N_{j_n}})_{j_n}$ converges to some $a_i \in \mathbb{Z}_p$. The resulting element $\sum_{i=0}^{n-1} a_i\xi^i \equiv 0 \pmod{p^N}$ for each $N \in \mathbb{Z}_{>0}$ and is hence equal to 0. Since for each N, the elements $a_{i,N}$ were not all divisible by p, there exists an i such that $a_i \neq 0$. We conclude that ξ satisfies some non-trivial polynomial over $\mathbb{Q}_p$ of degree less than n, which is a contradiction. □

Theorem 2.31. *The algebraic closure $\overline{\mathbb{Q}_p}$ is not complete.*

Proof. We need to find a Cauchy sequence that cannot have a limit in $\overline{\mathbb{Q}_p}$. We will define it as (a_n) with

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

where b_i is a primitive $(p^{2^i} - 1)$th root of unity and (N_j) is a positive strictly increasing sequence of integers to be determined later. Note that $2^i \mid 2^{i'}$ implies that $p^{2^i} - 1 \mid p^{2^{i'}} - 1$, hence $b_{i'} \mid b_i$ when $i' > i$. Also note that the b_j for $j \leq i$ are the digits in the p-adic expansion of a_i in the unramified extension $\mathbb{Q}_p(b_i)$ as defined in Theorem 2.29. Moreover, (a_i) is clearly Cauchy.

We now show that $\mathbb{Q}_p(a_i) = \mathbb{Q}_p(b_i)$. By Theorem 2.26, $\mathbb{Q}_p(b_i)$ is unramified of degree 2^i (it is also Galois, since b_i is a primitive root of unity). If $b_i \notin \mathbb{Q}_p(a_i)$, there would

exist by the fundamental theorem of Galois theory (see [6]) an isomorphism σ of $\mathbb{Q}_p(b_i)$ that is the identity on $\mathbb{Q}_p(a_i)$ while $\sigma(b_i) \neq b_i$. However, a_i and $\sigma(a_i)$ would then have different p-adic expansions, since $\sigma(a_i) = \sum_{j=0}^{i} \sigma(b_j)p^{N_j}$.

Next, we choose $N_0 = 0$ and define N_j by induction. Suppose N_j for $j < k$ have been chosen. By Theorem 2.26, $[\mathbb{Q}_p(a_i) : \mathbb{Q}_p] = [\mathbb{Q}_p(b_i) : \mathbb{Q}_p] = 2^i$. We then choose $N_j > N_{j-1}$ according to the previous lemma such that for any coefficients $\alpha_i \in \mathbb{Z}_p$ not all divisible by p and for any $n < 2^i$ we have

$$\alpha_n a_i^n + \ldots + \alpha_1 a_i + \alpha_0 \not\equiv 0 \pmod{p^{N_j}}.$$

Suppose now that $a \in \overline{\mathbb{Q}_p}$ is the limit of (a_i) and say a satisfies an equation $\beta_n a^k + \ldots + \beta_1 a + \beta_0 = 0$. After dividing by the maximal norm of the β_i's, we may assume that all $\beta_i \in \mathbb{Z}_p$ and that not all are divisible by p. Now choose i such that $2^i > n$. Because $a \equiv a_i \pmod{p^{N_{i+1}}}$, a_i satisfies a forbidden equation $\pmod{p^{N_{i+1}}}$. □

Since $\overline{\mathbb{Q}_p}$ is not sufficient, we define the *complex p-adic numbers* $\mathbb{C}_p$ as the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_p$. We construct $\mathbb{C}_p$ from $\overline{\mathbb{Q}_p}$ exactly like we constructed $\mathbb{Q}_p$ from $\mathbb{Q}$. We extend $|\cdot|_p$ also in the same way and in the same way as Lemma 2.1 we see that the possible values of $|\cdot|_p$ remain the fractional powers of p and 0. Conveniently for us, the story does not continue forever and $\mathbb{C}_p$ is actually algebraically closed. Before we prove this, we prove two very helpful lemma's.

Lemma 2.32 (Krasner's Lemma)**.** *If L is a finite extension of $\mathbb{Q}_p$ and $b \in \overline{\mathbb{Q}_p}$ is closer to $a \in \overline{\mathbb{Q}_p}$ than all Galois conjugates of a over L, then $L(a) \subset L(b)$.*

Proof. Suppose that $a \notin L(b)$. Then a has at least one more conjugate a_i over $L(b)$ that is not in $L(b)$. Let σ be an isomorphism between $L(a, b)$ and $L(a_i, b)$ that fixes $L(b)$ and maps a to a_i. Then $|b - a_i|_p = |\sigma(b - a_i)|_p = |b - a|_p$ and since a_i is also a conjugate of a over L, we find that

$$|a_i - a|_p \leq \max(|a_i - b|_p, |b - a|_p) = |b - a|_p < |a_i - a|_p,$$

a contradiction. □

Lemma 2.33. *Let $\mathbb{Q}_p \subset L = \mathbb{Q}_p(\alpha)$ be a finite extension of degree n and $f = a_0 + \ldots + a_{n-1}x^{n-1} + x^n$ the minimum polynomial of α over $\mathbb{Q}_p$. Then there exists $\epsilon > 0$ such that for each monic $g = b_0 + \ldots + b_{n-1}x^{n-1} + x^n \in \mathbb{Q}[x]$ of degree n with $M_g = \max_i(|a_i - b_i|) < \epsilon$, there is a root β of g such that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$.*

Proof. Consider $g = (x - \beta_1) \cdots (x - \beta_n) = b_0 + \ldots + b_{n-1}x^{n-1} + x^n \in \mathbb{Q}[x]$ with each $\beta_i \in \overline{\mathbb{Q}_p}$ such that $M_g < \epsilon$. Let $N = \max_{0 \leq i \leq n}(|\alpha|^i)$ and note that $g(\alpha) = g(\alpha) - f(\alpha)$. Hence we see that

$$\prod_{i=1}^{n} |\alpha - \beta_i| = |g(\alpha) - f(\alpha)| \leq \sum_{i=1}^{n} |a_i - b_i||\alpha|^i \leq nM_gN.$$

We thus find at least one j such that $|\alpha - \beta_j| \leq n^{1/n}M^{1/n}N^{1/n}$, so for ϵ small enough we find, using Krasner's lemma, that $K(\alpha) \subset K(\beta_j)$. Since $g(\beta_j) = 0$ and g has degree n, we conclude that $[K(\beta_j) : K] \leq n$, so $K(\alpha) = K(\beta_j)$. □

Theorem 2.34. *The set of complex p-adic numbers $\mathbb{C}_p$ is algebraically closed.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{C}_p[x]$ be a monic irreducible polynomial with a root α in the algebraic closure of $\mathbb{C}_p$. Since $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$, we can find polynomials $g_j = x^n + a_{n-1,j}x^{n-1} + \ldots + a_{0,j} \in \overline{\mathbb{Q}_p}[x]$ such that $M_j = \max_i(|a_{i,j} - a_i|_p) < 1/j$. For j large enough, we can use Lemma 2.33 to find roots β_j of g_j such that

$$|\alpha - \beta_j|_p \leq n^{1/n} M_j^{1/n} N^{1/n} \longrightarrow 0,$$

where $N = \max_{0 \leq i \leq n}(|\alpha|_p^i)$. (We can always extend the norm to the finite extension $\mathbb{C}_p(\alpha)$.) This shows that (β_j) is a Cauchy sequence in $\mathbb{C}_p$. Since $\mathbb{C}_p$ is complete, it converges within $\mathbb{C}_p$ and the limit must equal $\alpha \in \mathbb{C}_p$. We have thus shown that every monic irreducible polynomial in $\mathbb{C}_p[x]$ has a root in $\mathbb{C}_p$, which is sufficient. □

2.3 Topological properties of $\overline{\mathbb{Q}_p}$ and $\mathbb{C}_p$

In order to find out with what kind of normed fields we are dealing, we investigate the topological properties of $\overline{\mathbb{Q}_p}$ and $\mathbb{C}_p$ in this section. We are going to show that both fields are Haussdorff, whereas in contrast to $\mathbb{Q}_p$ and its finite extensions, $\mathbb{C}_p$ and $\overline{\mathbb{Q}_p}$ are not locally compact. Curiously, both $\overline{\mathbb{Q}_p}$ and $\mathbb{C}_p$ are also totally disconnected. Before we will be able to show this, we need some information about the residue fields. The following definition will help with this.

Definition/lemma 2.35. *The union $\mathbb{Q}_p^{ur}$ of all finite unramified extensions of $\mathbb{Q}_p$ is a field called the* maximal unramified extension of $\mathbb{Q}_p$.

Proof. We need to check that this is indeed a field. We characterized unramified extensions in Lemma 2.26. With the same notation as in that lemma, suppose $x, y \in \mathbb{Q}_p^{ur} = \cup_f K_f$, so say $x \in K_g$ and $y \in K_h$. We consider K_{gh}. Since $p^n - 1 \mid p^{gh} - 1$ when $n \mid gh$, we see that $K_n \subset K_{gh}$ for $n \in \{g, h\}$. Hence x and y are both in K_{gh} and we are done. □

We write $\mathbb{Z}_p^{ur}$ for the valuation ring of $\mathbb{Q}_p^{ur}$. Since the image under $\mathrm{ord_p}$ of $\mathbb{Q}_p^{ur}$ is still $\mathbb{Z}$ by definition, we find that $\mathbb{Z}_p^{ur}$ has maximal ideal $p\mathbb{Z}_p^{ur}$.

Lemma 2.36. *The residue fields of $\mathbb{Q}_p^{ur}$ and $\overline{\mathbb{Q}_p}$ are both equal to $\overline{\mathbb{F}_p}$.*

Proof. We first prove that the the residue field of $\mathbb{Q}_p^{ur}$ an algebraic extension of $\overline{\mathbb{F}_p}$. Consider $\alpha \in \mathbb{Z}_p^{ur}$. Since $\mathbb{Q}_p \subset \mathbb{Q}_p^{ur}$ is algebraic, there exist $n \in \mathbb{Z}$ and coefficients $a_i \in \mathbb{Q}_p$ such that $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$. Then by the non-archimedianity of the norm, for each $i < n$, we have $|a_i|_p|\alpha|_p^i \leq |\alpha|_p^n$, hence $|a_i|_p \leq |\alpha|_p^{n-i} \leq 1$ and $a_i \in \mathbb{Z}_p$ for each i. Therefore, for any $\overline{\alpha} \in \mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur}$, we can find a $q \in \mathbb{Z}_p[x]$ such that $q(\alpha) = 0$. Note that by Lemma 2.18, $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ and we have an obvious inclusion $\mathbb{Z}_p/p\mathbb{Z}_p \to \mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur}$. Now $\overline{\alpha}$ is a zero of $\overline{q}(x) \in \mathbb{F}_p[x]$, as desired. The same argument works to show that the residue field of $\overline{\mathbb{Q}_p}$ is an algebraic extension of $\mathbb{F}_p$, so it is a subset of $\overline{\mathbb{F}_p}$.

Now suppose $\overline{f}(\overline{\alpha}) = 0$ for some monic irreducible $\overline{f} \in \mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur}[x]$ and $\overline{\alpha} \in \overline{\mathbb{F}_p}$. Then we can find an $f \in \mathbb{Z}_p^{ur}[x]$ such that the coefficients of f are either 0 or have norm 1 and $f(\alpha) = \beta \in p\mathbb{Z}_p^{ur}$. If a is the constant coefficient of f (which has norm 1, since $\overline{f}$ is irreducible), then $|a - \beta|_p = 1$, so $\mathrm{ord_p}\,(a - \beta) = 0$. Also, the polynomial equation $f(\alpha) \in p\mathbb{Z}_p^{ur}$ yields that $|\alpha|_p \leq 1$. Hence $\mathrm{ord_p}\,\alpha = \frac{1}{n}\,\mathrm{ord_p}\,\alpha^n = \frac{1}{n} \cdot \mathrm{ord_p}\,(a - \beta) = 0$, so $|\alpha|_p = 1$ and $\alpha \in \mathbb{Z}_p^{ur}$. This shows that $\overline{\alpha} \in \mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur}$, so $\mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur} = \mathbb{F}_p$.

Since $\mathbb{Q}_p^{ur} \subset \overline{\mathbb{Q}_p}$ and we have a trivial inclusion from $\mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur}$ into the residue field of $\overline{\mathbb{Q}_p}$, it must be $\overline{\mathbb{F}_p}$ as well. □

As we shall soon see, 'closed' and 'open' discs are both closed and open in the topology on $\mathbb{C}_p$, so we need to introduce some notation. For $a \in \mathbb{C}_p$ and $r > 0$, we write $B_a(r) := \{x \in \mathbb{C}_p \,|\, |x - a|_p < r\}$, $B_a(r^+) := \{x \in \mathbb{C}_p \,|\, |x - a|_p \leq r\}$ and $C_a(r) = B_a(r^+) \setminus B_a(r)$. We will speak of $B_a(r)$ and $B_a(r^+)$ as respectively the *open* and *closed* disc around a of radius r and of $C_a(r)$ as the circle around a of radius r. Also, we abbreviate $B(r) := B_0(r)$. We are now ready to prove the main theorem of this section.

Theorem 2.37. *The spaces $\mathbb{C}_p$ and $\overline{\mathbb{Q}_p}$ are totally disconnected Hausdorff spaces that are not locally compact.*

Proof. For the disconnectedness, consider $a \in \mathbb{C}_p$. If $b \in C_a(r)$, then $B_b(\epsilon) \subset C_a(r)$ for each $\epsilon < r$ by the non-archimedianity of the norm. Hence any circle is open and thus for $*, \sim \in \{<, \leq\}$ any set of the kind $A = \{x \in \mathbb{C}_p \,|\, r_1 * |x|_p \sim r_2\}$ is open, which shows that any ball is disconnected.

In order to show that $\mathbb{C}_p$ is not locally compact, let A and B be the valuation rings of $\overline{\mathbb{Q}_p}$ and $\mathbb{C}_p$ respectively with maximal ideals M and N. By Lemma 2.36, $A/M = \overline{\mathbb{F}_p}$. The map $A/M \longrightarrow B/N$ mapping $x + M \mapsto x + N$ is a well-defined injective homomorphism, hence B/N is also infinite. We proceed as in the proof of Theorem 2.17. If B were compact, it could be covered by finitely many 'open' balls $B_i = a_i + N$ of radius 1. But then B/N would be finite, a contradiction.

Lastly, since the image of the norm is $\mathbb{Q}$, $\mathbb{C}_p$ is Haussdorff. The proofs for $\overline{\mathbb{Q}_p}$ are exactly the same. □

2.4 p-adic number fields

We take a brief intermezzo to discuss a generalization of the p-adic numbers: the **p**-adic numbers, where $\mathbf{p} \subset \mathcal{O}_K$ is a prime ideal in the ring of integers of a number field K. Even though we will see in this section that we learn everything there is to know about **p**-adic norms by studying the p-adic case, it is in Chapter 3 convenient to be able to speak of **p**-adic norms and valuations as well. In this section, let $C > 0$ be a constant and K a number field.

Definition 2.38. If $\mathbf{p}$ is a prime ideal of $\mathcal{O}_K$, we define the $\mathbf{p}$-*adic valuation* $\mathrm{ord_p}(x)$ for $x \in K^*$ as the exponent of $\mathbf{p}$ in the factorization of the fractional ideal $x\mathcal{O}_K$ into prime ideals. The $\mathbf{p}$-*adic norm* $|x|_\mathbf{p}$ is defined as $C^{-\,\mathrm{ord_p}(x)}$ if $x \in K^*$ and as 0 when $x = 0$.

Note that the definition of the $\mathbf{p}$-adic valuation is indeed a generalization of the p-adic valuation on $\mathbb{Q}$. Also, if $C \neq K \in \mathbb{R}_{>0}$ is another constant, then $K = C^\alpha$ for some $\alpha \in \mathbb{R}_{>0}$ and we see that the $\mathbf{p}$-adic norm is, up to equivalence, independent of the choice of the constant C. For convenience, we might then as well choose $C = \mathrm{N}(\mathbf{p})$ in order to make the generalization with respect to the p-adic norm more explicit. For the same reason as in the p-adic case, the $\mathbf{p}$-adic norm is indeed a norm and it is non-archimedian.

Lemma 2.39. *If $\mathbf{p}$ and $\mathbf{q}$ are different prime ideals in $\mathcal{O}_K$, then $|\cdot|_\mathbf{p}$ is not equivalent to $|\cdot|_\mathbf{q}$.*

Proof. If $\mathbf{p} \neq \mathbf{q}$, then $\mathbf{p} \not\subset \mathbf{q}$ and $\mathbf{q} \not\subset \mathbf{p}$ since both are maximal ideals. Thus, we may choose $a \in \mathbf{p} \setminus \mathbf{q}$ and $b \in \mathbf{q} \setminus \mathbf{p}$. Then $\mathrm{ord}_\mathbf{p} a > 0$ and $\mathrm{ord}_\mathbf{q} a = 0$, while $\mathrm{ord}_\mathbf{p} b = 0$ and $\mathrm{ord}_\mathbf{q} b > 0$, which shows that $|\cdot|_\mathbf{p}$ is not equivalent to $|\cdot|_\mathbf{q}$. □

Lemma 2.40. *Suppose that K is a finite extension of $\mathbb{Q}$ and that p is a prime number such that $(p) = \mathbf{p}_1^{a_1} \cdots \mathbf{p}_n^{a_n}$ is the factorization into prime ideals in K. Then for each i, the restriction of the $\mathbf{p}_i$-adic norm to $\mathbb{Q}$ is equivalent to $|\cdot|_p$. In other words, each $\mathbf{p}_i$-adic norm is equivalent to an extension of $|\cdot|_p$ to K.*

Proof. For each i, $\mathbf{p}_i^{a_i} \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ and since $p \in \mathbf{p}_i^{a_i} \cap \mathbb{Z}$, we conclude that $\mathbf{p}_i^{a_i} \cap \mathbb{Z} = (p)$ as ideals in $\mathbb{Z}$. Also, $p \notin \mathbf{p}_i^{b_i}$ for any $b_i > a_i$. Hence for any $m \in \mathbb{Z}$, we have $m \in \mathbf{p}_i^{a_i \cdot n}$ if and only if $p^n \mid m$, so $\mathrm{ord}_{\mathbf{p}_\mathrm{i}}(m) = a_i \, \mathrm{ord}_\mathrm{p}(m)$ and we see that $|\cdot|_{\mathbf{p}_i} = |\cdot|_p^{a_i \cdot f}$ on $\mathbb{Q}$, where $\mathrm{N}(\mathbf{p}) = p^f$, so they are equivalent. □

We already saw in the remarks below Lemma 1.56, that there is a unique prime number p in each prime ideal $\mathbf{p}$. Thus, for each prime ideal $\mathbf{p}$ in K, the $\mathbf{p}$-adic norm is equivalent to an extension of a unique p-adic norm.

Theorem 2.41. *Suppose that $K = \mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$, f is the minimum polynomial of α over $\mathbb{Q}$, $\mathbf{p}$ is a prime ideal in $\mathcal{O}_K$ above p and that L is the completion of K with respect to $|\cdot|_\mathbf{p}$. If $f = f_1 \cdots f_n$ is the decomposition of f into irreducibles in $\mathbb{Q}_p[x]$, then there exists an i such that $L \simeq \mathbb{Q}_p(\alpha_i)$, where α_i is a root of f_i. Also, the $\mathbf{p}$-adic norm on L is equivalent to the p-adic norm induced by $\mathbb{Q}_p(\alpha_i)$.*

Proof. By Lemma 2.40, the restriction of $|\cdot|_\mathbf{p}$ to $\mathbb{Q}$ is equivalent to $|\cdot|_p$. Since L is complete, it thus contains $\mathbb{Q}_p$. But L also contains α, which is a root of f. Therefore, L must contain a homomorphic image of $\mathbb{Q}_p(\alpha_i)$ for some i. But $\mathbb{Q}_p(\alpha_i)$ contains $\mathbb{Q}$ and a root of f, so it must contain a homomorphic image of $\mathbb{Q}(\alpha)$. Also, since the p-adic norm extends uniquely to $\mathbb{Q}_p(\alpha_i)$ by Theorem 2.22, the $\mathbf{p}$-adic norm restricted to the image of $\mathbb{Q}_p(\alpha_i)$ in L must be equivalent to the p-adic norm. Since $\mathbb{Q}_p(\alpha_i)$ is complete with respect to this norm, we have $L \simeq \mathbb{Q}_p(\alpha_i)$ as desired. □

Theorem 2.42. *Suppose that $K = \mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$, f is the minimum polynomial of α over $\mathbb{Q}$ and $f_i \in \mathbb{Q}_p[x]$ is an irreducible factor of $f \in \mathbb{Q}_p[x]$. Then there is a unique prime ideal $\mathbf{p}$ above p in K such that the injection $\mathbb{Q}(\alpha) \to \mathcal{K} = \mathbb{Q}_p[x]/(f_i)$ mapping α to $x+(f_i)$ induces a norm on K that is equivalent to the norm $|\cdot|_\mathbf{p}$. Moreover, $\mathcal{K}$ is isomorphic to the completion $K_\mathbf{p}$ of K with respect to $|\cdot|_\mathbf{p}$.*

Proof. We define $\mathbf{p} = \{x \in \mathcal{O}_K \mid |x|_p < 1\}$, where $|\cdot|_p$ is the p-adic norm on K induced by $\mathcal{K}$. (Note that $|\cdot|_p$ extends uniquely to $\mathcal{K}$ by Theorem 2.22.) It is now easy to check that $\mathbf{p}$ is maximal in $\mathcal{O}_K$ and that $|\cdot|_{\mathbf{p}}$ is equivalent to $|\cdot|_p$. By Lemma 2.39, $\mathbf{p}$ is unique with this property. Since $\mathcal{K}$ contains (an isomorphic image of) K and is complete with respect to $|\cdot|_p$, it also contains (an isomorphic image of) $K_{\mathbf{p}}$. We see that $|f_i(\alpha)|_{\mathbf{p}}$ is a non-zero power of $|f_i(x + (f_i))|_p = 0$, so $f_i(\alpha) = 0$. Since $K_{\mathbf{p}}$ contains $\mathbb{Q}_p$ and a root of f_i and $\mathcal{K}$ is the smallest such field, we find that $K_{\mathbf{p}} \simeq \mathcal{K}$. □

Lemma 2.40 and Theorem 2.41 show that we can go back and forth between prime numbers and prime ideals and that is does not matter whether we study finite extensions of $\mathbb{Q}_p$ or completions of finite extensions of $\mathbb{Q}$. Luckily for us, studying the p-adic case is thus sufficient for understanding the $\mathbf{p}$-adic theory in general.

The following corollary is going to be very useful in Chapter 3.

Corollary 2.43. *Suppose that $f \in \mathbb{Q}[x]$ is irreducible in both $\mathbb{Q}[x]$ and $\mathbb{Q}_p[x]$. Then there is a unique prime ideal $\mathbf{p}$ above p in $\mathbb{Q}[x]/(f) =: K$.*

Proof. Suppose $\mathbf{p}$ and $\mathbf{q}$ are two prime ideals in K above p such that $K_{\mathbf{p}}$ and $K_{\mathbf{q}}$ are the completions of K with respect to the $\mathbf{p}$- and $\mathbf{q}$-adic norms respectively . By Theorem 2.41, we find that $K_{\mathbf{p}} \simeq \mathbb{Q}_p(\alpha) \simeq K_{\mathbf{q}}$ since f is still irreducible in $\mathbb{Q}_p[x]$. This implies that the $\mathbf{p}$- and $\mathbf{q}$-adic norm are equivalent, which by Lemma 2.39 shows that $\mathbf{p} = \mathbf{q}$. □

2.5 Analysis on $\mathbb{C}_p$

Now we have constructed the complex p-adic numbers and have investigated some of its topological properties, we are ready to do analysis on $\mathbb{C}_p$. Therefore, when not explicitly mentioned, we will in this section be working in $\mathbb{C}_p$.

In this section, we will mostly be dealing with formal power series. If R is a ring, let $R[[x]]$ denote the ring of power series over R, with addition and multiplication as usual. We first show the elementary facts about power series in $\mathbb{C}_p[[x]]$.

Lemma 2.44. *A series $\sum_{n=1}^{\infty} a_n x^n$ converges when $|x|_p < r$ and diverges when $|x|_p > r$, where $r = 1/\limsup |a_n|_p^{1/n}$ is the* radius of convergence. *If $|x|_p = r$, the series converges if and only if $|a_n|_p |r|_p^n \longrightarrow 0$.*

The proof is not difficult once you remember that the series converges if and only if $a_n \longrightarrow 0$ and can be found in [9].

Lemma 2.45. *Every power series over K that converges in an open or closed disc is continuous on that disc.*

The proof is a careful, but quite straightforward work with inequalities and makes important use of the archimedian property of the norm. It can be found in [9]. The two

most important power series we know in $\mathbb{R}[[x]]$ and $\mathbb{C}[[x]]$ are the exponential and the logarithm. As formal power series, they can be defined in $\mathbb{C}_p[[x]]$ just as easily:

$$\log_p(1+x) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \text{ and } \exp_p(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

In order to determine their radii of convergence and to show that the usual properties still hold, we need the following two lemma's.

Lemma 2.46. *Let $f \in \mathbb{C}_p[[x]]$ be a power series such that there exists a sequence (x_m) in $\mathbb{C}_p$ with $x_m \neq 0$ for infinitely many m and $f(x_m) = 0$ for each m and $x_m \to 0$. Then $f = 0 \in \mathbb{C}_p[[x]]$.*

Proof. Suppose $\sum a_n x^n = f \neq 0 \in K[[x]]$ and let k be the smallest integer such that $a_k \neq 0$. We can then write $f(x) = x^k g(x)$ with $g(0) = a_k \neq 0$. Since g is continuous by the previous lemma, we find that $g(x_m) \longrightarrow g(0) = a_k$, while $g(x_m) = 0$ for infinitely many m, a contradiction. □

Lemma 2.47. *If $n = a_0 + a_1 p + \ldots + a_s p^s \in \mathbb{Z}_{\geq 0}$, where $0 \leq a_i \leq p-1$ for each i (i.e. n in base p), then*

$$\mathrm{ord_p}(n!) = \frac{n - \sum a_i}{p-1}.$$

Proof. The proof is by induction on n. The case $n = 1$ is trivial. Suppose n is as above and that the equation holds for n. If $k = \mathrm{ord_p}(n+1)$, then apparently $a_0 = a_1 = \ldots = a_{k-1} = p-1$, $a_k \neq p-1$ and $n+1 = (a_k+1)p^k + a_{k+1}p^{k+1} + \ldots + a_s p^s$. If b_i are the coefficients of $n+1$ in base p, then $\sum b_i = \sum a_i - k(p-1) + 1$ and the equation now follows. □

Theorem 2.48. *The disc of convergence of $\log_p(1+x)$ is $B_0(1) \subset \mathbb{C}_p$ and the disc of convergence of $\exp_p(x)$ is $B_0(p^{1/(1-p)}) \subset \mathbb{C}_p$.*

Proof. For $\log_p$, we see that $|a_n|_p = |1/n|_p = p^{\mathrm{ord_p}\, n}$ and hence $\lim_{n\to\infty} |a_n|_p^{1/n} = 1$. If $|x|_p = 1$, then $|a_n x^n|_p = p^{\mathrm{ord_p}\, n} \geq 1$ and the series diverges.

For $\exp_p$, note that $|a_n|_p = p^{\mathrm{ord_p}\, n!}$. If $r = 1/\limsup |a_n|_p^{1/n}$, this implies that

$$\mathrm{ord_p}\, r = -\,\mathrm{ord_p}\,(\limsup_{n\to\infty} |a_n|_p^{1/n}) = -\limsup_{n\to\infty} \frac{1}{n}\,\mathrm{ord_p}\,|a_n|_p$$

and since $\mathrm{ord_p}\,|x|_p = -\,\mathrm{ord_p}\, x$, we get

$$\mathrm{ord_p}\, r = \liminf_{n\to\infty} \frac{1}{n}\,\mathrm{ord_p}\,\frac{1}{n!} = \liminf_{n\to\infty} \frac{n - S_n}{n(1-p)},$$

where S_n is the sum of the coefficients of n in base p. Since $S_n/n \longrightarrow 0$, this implies that $\mathrm{ord_p}\, r = 1/(1-p)$ and hence $r = p^{1/(1-p)}$. If $\mathrm{ord_p}\, x = 1/(p-1)$, then $\mathrm{ord_p}\, a_n x^n = S_n/(p-1)$. Now the sequence $(a_{p^m} x^{p^m})$ has constant norm $p^{1/(p-1)}$ since $S_{p^m} = 1$ and thus $a_n x^n \not\to 0$. □

Note that the radius of convergence of the p-adic exponential function is very different from that of the exponential in $\mathbb{C}[[x]]$, which converges everywhere. This lack of convergence of $\exp_p$ may seem undesirable, but in Section 2.6 we will see that this allows us to prove very useful theorems on p-adic power series. We continue by proving the usual properties of the logarithm and the exponential.

Theorem 2.49. *The following equalities hold for each x, y in the appropriate discs of convergence:*

$$\log_p[(1+x)(1+y)] = \log_p(1+x) + \log_p(1+y) \text{ and } \exp_p(x)\exp_p(y) = \exp_p(x+y).$$

Proof. For the $\log_p$, note that $x, y \in B_0(1)$ implies that $x + y + xy \in B_0(1)$, so we can speak of $\log_p[(1+x)(1+y)]$. Since the equality holds over $\mathbb{R}$, we find that

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

for $x, y \in (-1, 1)$. Hence for any fixed $y \in (-1, 1)$, the difference vanishes for $x \in (-1, 1)$. With $x_m = 1/m$, we can use Lemma 2.46 to conclude that the difference is the zero series in $\mathbb{Q}[[x]]$ for any fixed $y \in (-1, 1)$ and hence the difference is the zero series in $\mathbb{Q}[[x, y]]$. But as a formal power series, there is no difference between log and $\log_p$, since all coefficients are in $\mathbb{Q} \subset \mathbb{Q}_p$. Thus the equality holds over $\mathbb{C}_p$ as well.

We can apply the same reasoning to $\exp_p$. □

Theorem 2.50. *The functions* $\exp_p : B_0(p^{1/(1-p)}) \longrightarrow B_1(p^{1/(1-p)})$ *and* $\log_p : B_1(p^{1/(1-p)}) \longrightarrow B_0(p^{1/(1-p)})$ *are mutually inverse.*

Proof. Showing that the images are in the right disc is straightforward. The inverse statement can be proved using the same reasoning as in the previous lemma. □

We have shown that the $\exp_p$ and $\log_p$ still behave like they do in $\mathbb{C}$, which is very convenient. It enables us to use the exponential and the logarithm to define more power series. The following power series has an important application in our method for solving Diophantine equations in Chapter 3.

Lemma 2.51. *For $a \in \mathbb{C}_p$ such that $\mathrm{ord_p}(a) > \frac{1}{p-1}$ the power series*

$$(1+a)^x := \exp_p(x \log_p(1+a)) \in \mathbb{C}_p[[x]]$$

converges when $\mathrm{ord_p}(x) \geq 0$.

Proof. By Lemma 2.48, we know that $(1+a)^x$ converges if and only if $\mathrm{ord_p}(x) + \mathrm{ord_p}(\log_p(1+a)) > \frac{1}{p-1}$. Now

$$\log_p(1+a) = a - \frac{a^2}{2} + \frac{a^3}{3} - \dots$$

and since $\mathrm{ord_p}(a) > \frac{1}{p-1}$, one can see that $\mathrm{ord_p}(\log_p(1+a)) = \min(\mathrm{ord_p}(a), \mathrm{ord_p}\, a^2/2, \dots) > \frac{1}{p-1}$. □

Remark 2.52. Suppose a series of rational numbers converges to a rational number with respect to $|\cdot|_p$ and to a rational number with respect to $|\cdot|_\infty$. You might expect these limits to be the same, but in general, they are not. For a counterexample, see [9] page 81.

2.6 Newton Polygons

In this section we investigate the roots of polynomials in $\mathbb{C}_p[x]$. Hence we do no harm when we consider only polynomials that are normalized such that their constant coefficient equals 1. The set of such polynomials will be denoted as $1 + x\mathbb{C}_p[x]$. An important tool for studying these roots are Newton polygons.

Definition 2.53. The *Newton polygon* of a polynomial $f = \sum_{i=0}^{n} a_i x^i \in 1 + x\mathbb{C}_p[x]$ is the polygon defined as follows:

(1) draw the points $(i, \operatorname{ord}_p a_i)$ for each $0 \leq i \leq n$ such that $a_i \neq 0$ in the plane;

(2) starting at $(0, \operatorname{ord}_p a_0) = (0, 0)$, rotate the upper y-axis counter-clockwise until you 'hit' a point drawn in step (1);

(3) pick the drawn point $(i, \operatorname{ord}_p a_i)$ furthest away (horizontally) from $(0, 0)$ on the line and draw the line segment between both points;

(4) if $i = n$, stop: the polygon is finished;

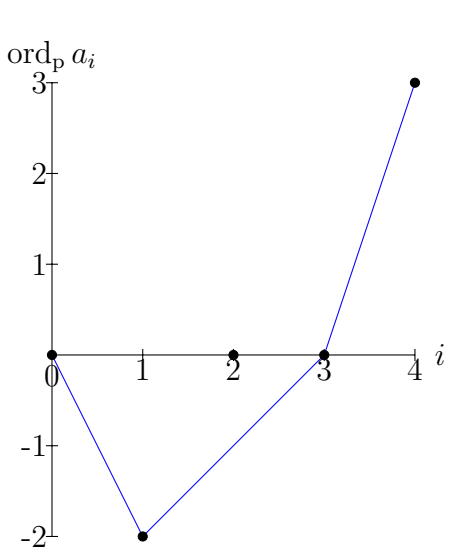
(5) otherwise, consider the vertical half line through and above $(i, \operatorname{ord}_p a_i)$ and rotate it counterclockwise until you 'hit' a drawn point, then continue at step (3).

This construction is called the *convex hull* of the points $(i, \operatorname{ord}_p a_i)$. The *slopes* of the Newton polygon are the slopes of the lines it consists of and the *length* of an edge of the polygon is the length of the projection of that edge onto the horizontal axis.

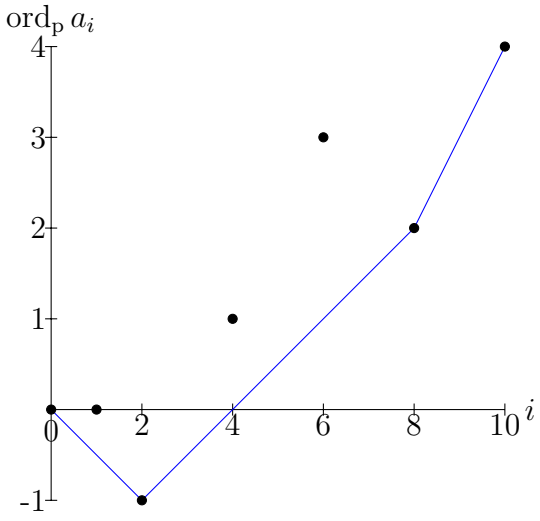
Recall from Definition 1.5 that the coefficients of any polynomial f are $\pm$ the elementary symmetric polynomials in the roots of f. This observation is crucial for proving the following theorem, which immediately illustrates the strength of Newton polygons.

Theorem 2.54. *If the Newton polygon of $f = \sum_{i=1}^{n} a_i x^i \in 1 + x\mathbb{C}_p[x]$ has slopes $\mu_1, \ldots \mu_r$ ($r \leq n$) with corresponding lengths $l_1, \ldots l_r$, then for each k, f has exactly l_k roots in $\mathbb{C}_p$ with order $-\mu_k$.*

Proof. Write $f(x) = (1 - x/\alpha_1) \cdots (1 - x/\alpha_n)$ and let $\lambda_i := \operatorname{ord}_p 1/\alpha_i = -\operatorname{ord}_p \alpha_i$ for each i. Order the roots such that $\lambda_1 \leq \ldots \leq \lambda_n$ and suppose that $\lambda_1 = \ldots = \lambda_r < \lambda_{r+1}$. Now a_i is the ith symmetric polynomial in the $1/\alpha_j$'s, which is the sum of all possible products of i of the $1/\alpha_j$'s. Hence, using that $\operatorname{ord}_p (x + y) \geq \min(\operatorname{ord}_p x, \operatorname{ord}_p y)$ (which is equivalent to the non-archimedianity of $|\cdot|_p$), we find that $\operatorname{ord}_p a_i \geq i\lambda_r$. Thus each point $(i, \operatorname{ord}_p a_i)$ is on or above the line $\mathcal{L}$ through $(0, 0)$ and $(r, r\lambda_r)$.



(a) $8x^4 - 3x^3 + x^2 + \frac{1}{4}x + 1$ with $p = 2$



(b) $81x^{10} + 2x^9 - 18x^8 + 27x^6 + 5x^5 + 6x^4 + \frac{1}{3}x^2 - 2x + 1$ with $p = 3$

Figure 2.1: Two Newton polygons for polynomials.

If we now consider a_r, we see that it is a sum of all products of exactly r of the $1/\alpha_j$'s. But all of such terms have order $> r\lambda_r$, except for $1/(\alpha_1 \cdots \alpha_r)$. Hence by Lemma 2.6, $\operatorname{ord}_p a_r = r\lambda_r$, so $(r, \operatorname{ord}_p a_r)$ lies on $\mathcal{L}$.

In order to show that r is the biggest integer such that this can happen, consider $i > r$. Then $\operatorname{ord}_p a_i > i\lambda_r$ by the same arguments as above. We conclude that the line between $(0, 0)$ and $(r, r\lambda_r)$ is the first segment of the Newton polygon.

Note that we are only interested in the slopes of the polygon, so we can translate all points and segments together by any value we like. So if we have $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = \ldots = \lambda_{s+r} < \lambda_{s+r+1}$, we can use $(x, y) \longrightarrow (x - s, y - \operatorname{ord}_p a_s)$ to get to the same situation as before. After considering all the roots, this results in the statement of the theorem. □

A direct application of Theorem 2.54 is the following theorem.

Theorem 2.55. *Any* $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ *with* $\operatorname{ord}_p a_n - \operatorname{ord}_p a_0 = k \in \mathbb{Z}$ *such that* $\gcd(k, n) = 1$ *and for each* i, $\operatorname{ord}_p a_i \geq \operatorname{ord}_p a_0 + \frac{k}{n} i \geq 0$, *is irreducible.*

Proof. Note that the last condition holds if and only if the Newton polygon of f consists of only one segment, which then has slope $\lambda = k/n$. Also note that the Newton polygon of f is the one of f/a_0 moved $\operatorname{ord}_p a_0$ upwards. Then by the previous theorem, all roots $\alpha_i \in \mathbb{C}_p$ have $\operatorname{ord}_p 1/\alpha_i = k/n$, so $\operatorname{ord}_p \alpha_i = -k/n$. Suppose that $f = g \cdot h$ with $g = \sum_{i=0}^{m} b_i x^i$ and h in $\mathbb{Z}[x]$. Then $\operatorname{ord}_p b_0 = -mk/n$ and mk/n is an integer, which can only be true when $m = n$ or $m = 0$. □

Example 2.56. Polynomials $f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$, such that

(i) $p \nmid a_n$ and $p \mid a_i$ for $i \neq n$, but $p^2 \nmid a_0$ (Eisenstein polynomials),

(ii) $p \nmid a_0$, $p \mid a_i$ for $i \neq 0$, but $p^2 \nmid a_n$ ('reversed' Eisenstein polynomials) or

(iii) $p \nmid a_0$, $p^{n-1} \mid a_n$, $p^n \nmid a_n$ and for each i, $p^i \mid a_i$ are irreducible.

We now move on from polynomials to power series.

Definition 2.57. For a power series $f \in 1 + x\mathbb{C}_p[[x]]$, we define the Newton polygon in the same way as for a polynomial. However, we need to be careful about a few things:

(1) We can get infinitely many segments. This poses no problem, we will just have an infinite polygon.

(2) We could hit infinitely many points on a line. In that case, the polygon will end with that infinitely long line.

(3) We could arrive at a case where the line we rotate hits no points, but when we rotate it a little more, it has moved past some points. For instance, when $\operatorname{ord}_p a_i = 1$ for each $i > 0$ and $\operatorname{ord}_p a_0 = 0$. In this case, we let the slope be the supremum of the slopes of the lines that are below all these points. (We could also in general have defined the Newton polygon in this way.)

The following lemma's all prepare for the p-adic Weierstrass preparation theorem, which can be seen as a generalization of Theorem 2.54 for power series.

Lemma 2.58. *The radius of convergence of $f = 1 + \sum_{i=1}^{\infty} a_i x^i \in 1 + x\mathbb{C}_p[[x]]$ is p^s, where s is the supremum of the slopes of the Newton polygon of f.*

Proof. Note that $\operatorname{ord}_p a_i x^i = \operatorname{ord}_p a_i + i \operatorname{ord}_p x$. But if $\operatorname{ord}_p x > -s$, then, since the slopes of a Newton polygon are increasing towards s, we see that $(i, \operatorname{ord}_p a_i + i \operatorname{ord}_p x)$ will grow arbitrarily high for large i. Hence $\operatorname{ord}_p a_i x^i \to \infty$ and the power series converges. With the same argument, if $\operatorname{ord}_p x < -s$, $\operatorname{ord}_p a_i x^i$ will be negative for large i, so f does not converge. □

Lemma 2.59. *Let $f = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + x\mathbb{C}_p[[x]]$ with first slope λ_1 of its Newton polygon and let $c \in \mathbb{C}_p$ be such that $\lambda = \operatorname{ord}_p c \leq \lambda_1$. Suppose that f converges on $B(p^{\lambda+})$, which by the previous lemma holds when $\lambda < \lambda_1$ or when the Newton polygon of f has more than one segment. Then the Newton polygon of $g = (1 - cX)f$ is obtained by attaching the Newton polygon of f to the line from $(0, 0)$ to $(1, \lambda)$. Moreover, g converges on exactly the same set as f.*

Proof. We will first reduce the proof to the case where $c = 1$ and $\lambda = 0$: suppose the lemma holds for $c = 1$ and let f and g be as above. Then the Newton polygons of $f'(x) := f(x/c)$ and $g'(x) = g(x/c)$ are that of f and g, minus the line $y = \lambda x$ and we see that f' and g' satisfy the lemma with c, λ, λ_1 replaced by $1, 0, \lambda_1 - \lambda$. Then we can apply the lemma for $c = 1$ and note that $g(x) = g'(cx)$ and $f(x) = f'(cx)$ and that the Newton polygons of $g(cx)$ and $f(cx)$ equal the Newton polygons of $g(x)$ and $f(x)$ with the line $y = \lambda x$ added, to conclude that the lemma holds in the general case.

We now prove the lemma for $c = 1$ and $\lambda = 0$. Write $g(x) = 1 + \sum_{i=1}^{\infty} b_i x^i$. Then $b_{i+1} = a_i - a_{i+1}$, so $\operatorname{ord}_p b_{i+1} \geq \min(\operatorname{ord}_p a_i, \operatorname{ord}_p a_{i+1})$ with equality when $a_i \neq a_{i+1}$, which clearly occurs when $(i, \operatorname{ord}_p a_i)$ is a vertex of the polygon of f. So at vertices, $\operatorname{ord}_p b_{i+1} = \operatorname{ord}_p a_i$ and hence the polygons of f and g have the desired shape when the Newton polygon of f has infinitely many vertices. If not, suppose that λ_f is the final slope of f. Since $\operatorname{ord}_p b_{i+1} \geq \operatorname{ord}_p a_i$, we need to check that g cannot have a slope λ_g greater than λ_f. Suppose it does. Then for some j, $\operatorname{ord}_p b_{i+1} > \operatorname{ord}_p a_i$ for all $i \geq j$, which implies that $a_j = a_{j+1} = a_{j+1} = \ldots$, which contradicts the convergence of f on $B(1)$. Therefore, in the case of a last segment, their slopes are equal. Since the second vertex of g is $(1, 0)$, we find that the Newton polygon of g is that of f attached to the line from $(0, 0)$ to $(1, 0)$. Lastly, g and f converge on the same set by the previous lemma. □

The next step is to try and deduce the orders of the roots of power series from their Newton polygon.

Lemma 2.60. *Let $f = 1 + x\mathbb{C}_p[[x]]$ be a power series with Newton polygon with first slope λ_1 that converges on the closed disc $B(p^{\lambda_1+})$ and suppose that the first line of this polygon actually hits a point $(i, \operatorname{ord}_p a_i)$. Both conditions are satisfied when the polygon has more than one slope. Then there exists an $\alpha \in \mathbb{C}_p$ such that $f(\alpha) = 0$ and $\operatorname{ord}_p 1/\alpha = \lambda_1$.*

Proof. Again we can reduce to the case $\lambda_1 = 0$. Suppose the lemma holds for $\lambda_1 = 0$ and let f be as in the lemma. Since $\lambda_1 \in \mathbb{Q}$, we may consider $\pi = p^{\lambda_1} \in \mathbb{Q}_p$ such that $\operatorname{ord}_p \pi = \lambda_1$. Then $g(x) = f(x/\pi)$ satisfies the lemma with $\lambda_1 = 0$ and we find a root β as in the lemma. Then $\alpha = \beta/\pi$ is the desired root of f.

So we consider $\lambda_1 = 0$. Since f converges on $B(1^+)$, the orders $\operatorname{ord}_p a_i \to \infty$, so we can define N to be the greatest i for which $\operatorname{ord}_p a_i = 0$. Also, let $f_n = 1 + \sum_{i=1}^{n} a_i x^i$. If $n \geq N$, Lemma 2.54 implies that f_n has precisely N roots $\alpha_{n,1}, \ldots \alpha_{n,N}$ in $\mathbb{C}_p$ with $\operatorname{ord}_p \alpha_{n,i} = 0$ for each i. We define the sequence (α_n) as follows: let $\alpha_0 = \alpha_{N,1}$ and let α_{n+1} be the element of $\{\alpha_{N+n,1}, \ldots, \alpha_{N+n,N}\}$ that minimizes $|\alpha_{N+n,i} - \alpha_n|_p$.

By the construction of (α_n)

$$|\alpha_{n+1} - \alpha_n|_p^N \leq \prod_{i=1}^{N} |\alpha_{(n+1),i} - \alpha_n|_p = \prod_{i=1}^{N} |1 - \alpha_n/\alpha_{(n+1),i}|_p,$$

the last equality being true since $|\alpha_n|_p = 1$. Now suppose that $n \geq N$ and β is a zero of f_{n+1} unequal to one of the $\alpha_{(n+1),i}$. Then by definition of N, $\operatorname{ord}_p (1/\beta) > 0$, so $|\beta|_p > 1$, hence $|1 - \alpha_n/\beta|_p = 1$. So the last product equals $|f_{n+1}(\alpha_n)|_p = |f_{n+1}(\alpha_n) - f_n(\alpha_n)|_p = |a_{n+1}\alpha_n^{n+1}|_p = |a_{n+1}|_p \longrightarrow 0$. We conclude that (α_n) is a Cauchy sequence.

Let α be the limit of (α_n). In order to show that $0 = f(\alpha) = \lim_{n\to\infty} f_n(\alpha)$, we compute $|(\alpha^i - \alpha_n^i)/(\alpha - \alpha_n)|_p = |\sum_{j=1}^{i} \alpha^{i-j}\alpha_n^{j-1}|_p \leq 1$. Since also $|a_i|_p \leq 1$ for each i, we find that

$$|f_n(\alpha)|_p = |f_n(\alpha) - f_n(\alpha_n)|_p = |\alpha - \alpha_n|_p \left| \sum_{i=1}^{n} a_i \frac{\alpha^i - \alpha_n^i}{\alpha - \alpha_n} \right|_p \leq |\alpha - \alpha_n|_p.$$

We conclude that $f(\alpha) = 0$, finishing the proof. □

Using the same ideas, we can prove another useful lemma.

Lemma 2.61. *Let $f = 1+\sum_{i=1}^{\infty} a_i x^i \in 1+x\mathbb{C}_p[[x]]$ converge on a disc including $\alpha \in \mathbb{C}_p$, which is a root of f. If $g = 1+\sum_{i=1}^{\infty} b_i x^i = f \cdot \sum_{j=1}^{\infty}(x/\alpha)^j$, i.e. f divided by $1 - X/\alpha$, then g converges on $B(|\alpha|_p^+)$.*

Proof. By computing the product, we find that the coefficients of g are $b_i = \sum_{k=1}^{i}(1/\alpha)^j a_{i-j}$. Hence, if again $f_n = 1+\sum_{i=1}^{n} a_i x^i$, then $f_n(\alpha) = b_n\alpha^n$ and we see that $|b_n\alpha^n|_p \longrightarrow 0$. □

The previous lemmas together prove the main theorem of this section.

Theorem 2.62 (p-adic Weierstrass preparation theorem)**.** *Suppose $f = 1+\sum_{i=1}^{\infty} a_i x^i \in 1+x\mathbb{C}_p[[x]]$ converges on $B(p^{\lambda+})$ and let N be the greatest i such that $(i, \operatorname{ord}_p a_i)$ lies on an edge of slope $\leq \lambda$. This N always exists, since the convergence is on the* closed *disc $B(p^{\lambda+})$. Then there exists a power series $g = 1+\sum_{i=1}^{\infty} b_i x^i \in 1+x\mathbb{C}_p[[x]]$ that converges and is non-zero on $B(p^{\lambda+})$ and a uniquely determined polynomial $h \in 1+x\mathbb{C}_p[x]$ of degree N such that $f = h \cdot g$. Also, the Newton polygon of h coincides with that of f up to $(N, \operatorname{ord}_p a_N)$.*

Proof. We prove this by induction on N. If $N = 0$, the Newton polygon of f has no edge of slope $\leq \lambda$. If f had a root $\alpha \in B(p^{\lambda+})$, then we could combine Lemma's 2.61 and 2.59 to find that the first slope of the Newton polygon of f had slope $-\operatorname{ord}_p \alpha \leq \lambda$, a contradiction. Therefore, $h = 1$ and $g = f$ work for $N = 0$.

Now let $N \geq 1$ and assume the theorem is true for $N-1$ and let $\lambda_1 \leq \lambda$ be the first slope of the Newton polygon of f. By the conditions of the theorem, we may apply Lemma 2.60 to conclude that f has a root $\alpha \in \mathbb{C}_p$ with $\operatorname{ord}_p \alpha = -\lambda_1$. By Lemma 2.61, $f' = f\sum_{i=0}^{\infty}(X/\alpha)^n$ converges on $B(p^{\lambda_1+})$. Let b_i be the coefficients of f'. Similar to the previous lemma, we then see that

$$\operatorname{ord}_p b_i \geq \min(\operatorname{ord}_p 1/\alpha^i, \operatorname{ord}_p a_1/\alpha^{i-1}, \ldots, \operatorname{ord}_p a_{i-1}/\alpha, \operatorname{ord}_p a_i) \geq i\lambda_1,$$

hence the first slope μ of f' has $\mu \geq \lambda_1$. We may now apply Lemma 2.59 to see that f' has the same Newton polygon as f without the first segment and that f' converges on $B(p^{\lambda+})$.

We conclude that f' satisfies the conditions of the theorem for $N-1$ and by the induction hypothesis we then find a $h' \in 1+x\mathbb{C}_p[x]$ of degree $N-1$ and $g \in 1+x\mathbb{C}_p[[x]]$ such that $f' = h' \cdot g$ and g converges and is non-zero on $B(p^{\lambda+})$ and h' has the same polygon as f' up to $(N-1, \operatorname{ord}_p a_{N-1})$. Multiplying by $x - \alpha$ yields

$$f = (x-\alpha) \cdot f' = (x-\alpha) \cdot h' \cdot g = h \cdot g,$$

where $h = (x-\alpha) \cdot h'$. Moreover, h is uniquely determined by its roots since it has constant coefficient 1. □

Remark 2.63. The p-adic Weierstrass theorem can be stated even stronger. Namely, h and g can be shown to be in $K[[x]]$ if K is a complete subfield of $\mathbb{C}_p$ and $f \in K[x]$. However, this is a non-trivial result that (probably) does not easily follow from what we have done so far.

Corollary 2.64. *If λ is the slope of a segment of length N of the Newton polygon of $f \in 1 + x\mathbb{C}_p[[x]]$, then there are exactly N roots $\alpha \in \mathbb{C}_p$ such that $f(\alpha) = 0$ and* $\operatorname{ord}_{\mathrm{p}} \alpha = -\lambda$.

Theorem 2.65 (Strassmann)**.** *Let $0 \neq f = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{C}_p[[x]]$ be a power series that converges on $\mathbb{Z}_p$ and choose $N \in \mathbb{Z}_{\geq 0}$ as the largest i such that $|a_i|_p = \max_n |a_n|_p$. Then f has at most N roots in $\mathbb{Z}_p$.*

Proof. Note that $\operatorname{ord}_{\mathrm{p}} a_N = \max(\{n \mid \operatorname{ord}_{\mathrm{p}} a_n = \min_m(\operatorname{ord}_{\mathrm{p}} a_m)\})$ and hence $(N, \operatorname{ord}_{\mathrm{p}} a_N)$ is the point where the slope starts to be positive for the first time. Thus, the Weierstrass preparation theorem says together with Theorem 2.54 that f has exactly N zeros in $B(1)$ and thus at most N in $\mathbb{Z}_p$. □

Strassmann's theorem will be a very important tool for tackling Diophantine equations in Chapter 3. The p-adic Weierstrass preparation theorem has more interesting consequences, though. For example, unlike in $\mathbb{C}$, entire power series over $\mathbb{C}_p$ have the beautiful property that they behave like polynomials when considering their roots.

Theorem 2.66 (Factorization of entire power series)**.** *Any power series $f \in \mathbb{C}_p[[x]]$ with $f(0) = a_0 \neq 0$ that converges everywhere has countably many roots and*

$$f = a_0 \prod_{\alpha \,:\, f(\alpha)=0} \left(1 - \frac{x}{\alpha}\right).$$

Proof. If f is a polynomial, the theorem is clear. Otherwise, we consider $f' = f/a_0$. We conclude from Lemma 2.58 that the slopes of the Newton polygon of f' approach infinity. Now for any λ, we can apply the Weierstrass preparation theorem to find $f' = h_\lambda \cdot g_\lambda$ with the appropriate properties. Let b_i^λ be the coefficients of g_λ and consider the first slope μ_λ of g_λ. Since g_λ is non-zero on $B(p^\lambda)$, we conclude from Lemma 2.60 that $\mu_\lambda > \lambda$ and hence $\mu_\lambda \to \infty$ when $\lambda \to \infty$ *if* the Newton polynomial of g_λ actually hits a point. So if there are infinitely many λ such that g_λ has a Newton polygon consisting of just one segment, this reasoning fails. However, we then have that all $(b_i^\lambda, \operatorname{ord}_{\mathrm{p}} b_i^\lambda)$ $(i > 0)$ are on a line with slope μ_λ. Using Lemma 2.58, we then see, as the radius of convergence is greater than p^λ, that the slopes still approach infinity. In conclusion, all coefficients converge to 0, such that $g_\lambda \to 1$ as $\lambda \to \infty$. Since any root of f' is a root of h_λ for some λ, we see that f equals the infinite product over its roots. □

Corollary 2.67. *If $f \in \mathbb{C}_p[[x]]$ is entire, i.e. it converges everywhere, and non-zero on $\mathbb{C}_p$, then f is constant.*

In $\mathbb{C}$, a result like this can never be obtained, since the exponential converges and is non-zero on the whole of $\mathbb{C}$. Therefore, the lack of convergence of the p-adic exponential series was already an indirect consequence of the p-adic Weierstrass preparation theorem.

3 Diophantine equations

Now that we have studied local and global number theory it is time to put our knowledge to use. Therefore, this chapter will be devoted to solving Diophantine equations. The only solutions we will be studying in this chapter are integer solutions. Thus, when we speak of a *solution* to a Diophantine equation, we actually mean an *integer solution*.

3.1 Skolem's method for solving Thue equations

In this section we shall study a method for solving Diophantine equations that was introduced by the Norwegian mathematician Thoralf Skolem (1887-1963). The class of Diophantine equations we are going to apply this method to are equations of the kind $f(x, y) = 1$, where $f \in \mathbb{Z}[x, y]$ is an irreducible *binary form*. A binary form is nothing more than a homogeneous polynomial in two variables, which we will choose to be x and y. It is important to note that there already exists an algorithm to find all solutions of equations $f(x, y) = A$, where $A \in \mathbb{Z} \setminus \{0\}$ and $f \in \mathbb{Z}(x, y)$ is an irreducible binary form of degree at least 3. Such equations are called *Thue equations*, after the Norwegian mathematician Axel Thue (1863-1922), who proved in 1909 that they always have finitely many (integer) solutions. It may not come as a surprise that Skolem was actually a PhD student of Thue. In 1968, Alan Baker provided an effective upper bound on $\max(|x|, |y|)$ for solutions of a Thue equation and in 1989, De Weger and Tzanakis presented an efficient algorithm for finding the solutions of any Thue equation [17].

So if there already exists an algorithm for finding the solutions, why should we study them again using another method? First of all, the methods of Thue and Baker are analytical. They make use of *Diophantine approximation*, which is a theory that studies the approximation of real numbers by rationals. Skolem's method, which we will present in this section, is of an algebraic nature. Secondly, the idea behind Skolem's method allows us to solve Diophantine equations that are not easily solved with Thue's method. In Section 3.2 for example, we will show that the equation $x^3 + dy^3 = 1$ has at most two solutions $(x, y) \in \mathbb{Z}^2$ for any $d \in \mathbb{Z}$. Such a general result about a class of degree 3 Diophantine equations is difficult to obtain by Thue's approximation techniques. Furthermore, the Chabauty-Coleman method for finding rational points on curves of genus $g \geq 2$ (see [12]) is inspired by Skolem's p-adic method. The main theorems of this section are based on the ideas presented in Proposition 4.5.17 of [2]. We begin this section by studying binary forms in general.

Lemma 3.1. *If $f \in \mathbb{Q}[x, y]$ is a binary form of degree n such that the degree of $f(x, 1)$ is n as well. Then f is irreducible if and only if $f(x, 1) \in \mathbb{Q}[x]$ is irreducible.*

Proof. Firstly, suppose f is irreducible. Then the coefficient for x^n is non-zero, so $f(x,1)$ has degree n. Suppose that $g(x) = f(x,1)$ were reducible, say $g = h \cdot k$ with $\deg h = m$ and $\deg k = n - m$. Now let h' and k' be the polynomials obtained by adding the power of y to each monomial such that h' is homogeneous of degree m and k' is homogeneous of degree $n-m$. Then $h'k'$ is homogenous of degree n and its coefficient for $x^i y^{n-i}$ is the same as the coefficient for x^i in hk, so we conclude that $h'k' = f(x,y)$. Conversely, if f were reducible, then a factorization of f includes a factor of x in both factorizations, so $f(x,1)$ would be reducible as well. □

Since the study of the equation $f(x,y) = 1$, where $f \in \mathbb{Z}[x,y]$ is reducible, say $f = g \cdot h$, actually corresponds to finding solutions to $g(x,y) = \pm 1$ and $h(x,y) = \pm 1$, we may restrict ourselves to irreducible polynomials. The following lemma allows us to use Dirichlet's unit theorem, which is the starting point for Skolem's method.

Lemma 3.2. *Let $f \in \mathbb{Q}[x,y]$ be an irreducible binary form of degree n such that $f(x,1)$ is monic of degree n. Then for any $a, b \in \mathbb{Q}$, $f(a,b) = \mathrm{N}_{K/\mathbb{Q}}(a - b\theta)$, where θ is a root of $f(x,1)$ in $\mathbb{C}$ and $K = \mathbb{Q}(\theta)$.*

Proof. Since f is monic, $f(x,1)$ has degree n. Consider $f(x,1)$ and let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be its n roots. Then we can write $f(x,1) = (x - \alpha_1) \cdots (x - \alpha_n)$. Using the same idea as in the proof of Lemma 3.1, we find that $f(x,y) = (x - \alpha_1 y) \cdots (x - \alpha_n y)$. Let $\theta = \alpha_1$ and $K = \mathbb{Q}(\theta)$. Then by Lemma 3.1, $[K : \mathbb{Q}] = n$ and we see that the α_i are the Galois conjugates of θ, so that $f(a,b) = \mathrm{N}_{K/\mathbb{Q}}(a - b\theta)$ for each $a, b \in \mathbb{Q}$. □

We call a binary form $f(x,y)$ *monic*, whenever $f(x,1)$ is monic of the same degree. We already saw that Pell's equation had infinitely many solutions. Similarly, we can now say that any binary form of degree 2 has infinitely many solutions.

Corollary 3.3. *Let $f(x,y) = x^2 + axy + by^2 = 1$, where $a, b \in \mathbb{Z}$. If $f(x,1)$ has two real roots, the Diophantine equation $f(x,y) = 1$ has infinitely many solutions (x,y).*

Proof. Let θ be a root of $f(x,1)$. By Lemma 3.2 we can rewrite the equation as $\mathrm{N}_{K/\mathbb{Q}}(x - y\theta) = 1$, where $K = \mathbb{Q}(\theta)$. The proof now follows that of Theorem 1.84, where we concluded the same thing for Pell's equation. □

The following theorem gives a description of the amount of solutions to a special class of Thue equations of degree 3. In order to avoid writing out all cases that may arise in detail, we will need the notion of *effectively computable*. A bound is called effectively computable when there exists a (finite) algorithm to compute it. In the remaining theorems of this section, the proofs serve as the desired algorithms.

Theorem 3.4. *Suppose that $f \in \mathbb{Z}[x,y]$ is a monic irreducible cubic binary form such that $f(x,1)$ has a negative discriminant. Let θ be the real root of $f(x,1)$. Also, suppose that there exists some power $m \in \mathbb{Z} \setminus \{0\}$ such that the fundamental unit ϵ of $K = \mathbb{Q}(\theta)$ has $\epsilon^m = \pm 1 + p(v_0 + v_1\theta + v_2\theta^2) =: \pm 1 + p\alpha$ with p an odd prime such that $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$. If $f(x,1)$ is irreducible over $\mathbb{Q}_p$, then there is an effectively computable bound to the number of solutions of the Diophantine equation $f(x,y) = 1$.*

Proof. By Lemma 3.2, we can write $f(x,y) = \mathrm{N}_{K/\mathbb{Q}}(x - y\theta)$. Since the discriminant of $f(x,1)$ is negative, we know that $f(x,1) \in \mathbb{Z}[x]$ has one real and two complex roots. Thus, Dirichlet's unit theorem tells us that the unit group of K one fundamental unit ϵ of norm 1. Solving $f(x,y) = 1$ now amounts to finding $x, y, k \in \mathbb{Z}$ such that $x - y\theta = \epsilon^k$. Consider a root of g, which we also call θ by abuse of notation. We consider $\mathbb{Q}_p(\theta)$. By Corollary 2.43, we can define $\mathbf{p}$ as the unique prime ideal in K above p. By Theorem 2.41 and Lemma 2.40, $\mathbf{p}$ induces a norm $|\cdot|_{\mathbf{p}}$ on $\mathbb{Q}_p(\theta)$ which is equivalent to $|\cdot|_p$. Suppose there exist an $0 \leq l < |m|$ and a $k \in \mathbb{Z}$ such that $x - y\theta = \epsilon^{mk+l}$, which is equivalent to $\epsilon^l(x - y\theta) = \epsilon^{mk}$.

Remember that $\mathrm{ord}_{\mathbf{p}}(\alpha) \geq 0$. Therefore, since $p > 2$, $\mathrm{ord}_{\mathrm{p}}(p\alpha) \geq 1 > \frac{1}{p-1}$ and we can apply Lemma 2.51 to see that $\epsilon^{mk} = (1 + p\alpha)^k$ converges as a power series in k for each $k \in \mathbb{Z}_p$:

$$\epsilon^l(x - y\theta) = \epsilon^{mk} = (1 + p\alpha)^k = \exp_p(k \log_p(1 + p\alpha)) = \sum_{j \geq 0} c_j k^j.$$

Notice that $c_0 = 1$, $c_1 = \log_p(1 + p\alpha) = p\alpha - \frac{(p\alpha)^2}{2} + \frac{(p\alpha)^3}{3} - \ldots \equiv p\alpha \pmod{p^2\mathbb{Z}_{\mathbf{p}}}$ and using Lemma 2.47, we see that $c_j \equiv 0 \pmod{p^2\mathbb{Z}_{\mathbf{p}}}$ for each $j \geq 2$. Also, $\mathrm{ord}_{\mathrm{p}}\, c_j \to \infty$. Here $\mathbb{Z}_{\mathbf{p}} = \{x \in \mathbb{Q}_p(\theta) \mid |x|_{\mathbf{p}} \leq 1\}$.

Since $f(x,1)$ is irreducible in $\mathbb{Q}_p[x]$, $1, \theta, \theta^2$ are linearly independent over $\mathbb{Q}_p$ and we may collect the coefficients of 1, θ and θ^2, so that

$$\epsilon^l(x - y\theta) = \sum_{j \geq 0} f_{0,j} k^j + \sum_{j \geq 0} f_{1,j} k^j \theta + \sum_{j \geq 0} f_{2,j} k^j \theta^2. \tag{3.1}$$

Let $n_i = \mathrm{ord}_{\mathrm{p}}\, v_i$ for each i. Since $\mathrm{ord}_{\mathrm{p}}(p^{r-2}/n) \geq 0$ for each $r \geq 2$, we see that $f_{0,0} = 1$, $f_{1,0} = f_{2,0} = 0$ and $f_{0,j} \equiv pv_j \pmod{p^{n_j+2}\mathbb{Z}_p}$ for each j. Also, $f_{0,j} \equiv 0 \pmod{p^{n_j+2}\mathbb{Z}_p}$ for each $j \geq 2$ and $\mathrm{ord}_{\mathrm{p}}\, f_{i,j} \to \infty$ when $j \to \infty$.

Firstly, as a potential shortcut, suppose that $n_i = 0$ for each i and that there do not exist $(x,y) \in \mathbb{Z}^2$ that solve $f(x,y) = 1$ such that $\epsilon^l(x - y\theta) = a_0 + a_1\theta + a_2\theta^2$, where $a_i \equiv 0^i \pmod{p\mathbb{Z}_p}$ for each i. Suppose that $a_i \not\equiv 0^i \pmod{p\mathbb{Z}_p}$. We can then compare the coefficients for θ^i on the left and right hand side of 3.1 to obtain that $\sum_j f_{i,j} k^j = a_i \not\equiv 0^i \pmod{p\mathbb{Z}_p}$. Since $f_{i,j} \equiv 0 \pmod{p\mathbb{Z}_p}$ for $j \geq 0$ and $f_{i,0} = 0^i$, $a_0 \not\equiv 0 \pmod{p\mathbb{Z}_p}$, we can apply Strassmann's theorem with $N = 0$ to find that such a k does not exist.

Secondly, we consider the general case. We again write $\epsilon^l(x - y\theta) = a_0 + a_1\theta + a_2\theta^2$. Note that each a_i is a linear expression in x and y. If one a_i is constant, i.e. does not depend on x and y, we can collect the coefficients of θ^i in 3.1. Since $\mathrm{ord}_{\mathrm{p}}\, f_{i,j} \to \infty$ when $j \to \infty$, there exists an N to apply Strassmann with and this N can be computed by finding the values of the coefficients. Since the power series we consider does not depend on (x,y), we find at most N solutions to $f(x,y) = 1$ that correspond to this value of l. If no a_i is constant, we know at least that $\{1, a_0, a_1, a_2\}$ is a $\mathbb{Q}$-linearly dependent set in the $\mathbb{Q}$-vector space spanned by $1, x, y$. Therefore, we can find $\beta_i \in \mathbb{Q}$ such that

$$\beta_0 a_0 + \beta_1 a_1 + \beta_2 a_2 = \beta_3.$$

If $\beta_i \neq 0$ for each $i \in \{0,1,2\}$, we consider the $\mathbb{Q}$-basis

$$\mathcal{B} = \left\{1, \frac{1}{\beta_0\beta_1} - \frac{\theta}{\beta_1}, -\frac{1}{\beta_0\beta_2} + \frac{\theta^2}{\beta_2}\right\}$$

for $\mathbb{Q}(\theta)$. In this basis, the coefficient of $\epsilon^l(x - y\theta)$ for 1 is equal to β_3/β_0. Since β_3/β_0 is independent of the values of x and y, we may collect the coefficients for 1 in the basis $\mathcal{B}$ on both sides of 3.1. Again, since $\operatorname{ord}_{\mathbf{p}} c_j$ grows to infinity, we know that we can apply Strassmann for some N, which we can compute by calculating the coefficients explicitly. Since the power series we constructed is independent of (x, y), this gives at most N solutions to $f(x, y) = 1$ that correspond to this value of l. If $\beta_i = 0$ for one $i \in \{0,1,2\}$, we can construct an analogous basis and do the same. The case that two β_i are 0 is the case where one α_i is constant and has already been dealt with.

The above algorithm works for each $l \in \{0,1,2\}$ and hence results in a computable upper bound for the amount of solutions of $f(x, y) = 1$. □

Keeping the notation of the previous theorem, note that the powers of the fundamental unit that are multiples of p are most likely to be of the form $\pm 1 + p(v_0 + v_1\theta + v_2\theta^2)$, since the coefficients p arise naturally from Newtons binomium. Moreover, Lemma 1.56 ensures us that we can find such a power for every prime p, namely $p^3 = |\,\mathrm{N}(p)|$. This draws the question whether we might always be able to choose our prime p in such a way that f is irreducible in $\mathbb{Q}_p[x]$. Unfortunately, there exist examples of polynomials that are reducible in $\mathbb{Q}_p[x]$ for every prime p, while still being irreducible over $\mathbb{Q}$. See [8] for such examples.

However, such counterexamples only exist for polynomials of composite degree, not for polynomials of prime degree. This is a consequence of Chebotarev's Density Theorem. The formulation and proof of this theorem can be found in [11]. We formulate a corollary of Chebotarev's Density Theorem that is sufficient for our purposes.

Theorem 3.5. *Suppose $f \in \mathbb{Z}[x]$ is irreducible and consider the Galoisgroup G of f over $\mathbb{Q}$ as a subset of S_n. If G contains a permutation with cycle pattern $(n_1, \ldots, n_k)$, then there are infinitely many primes p such that $f \pmod p$ has a factorization into irreducibles of degrees $n_1, \ldots, n_k$ in $\mathbb{F}_p[x]$.*

This allows us to discard the conditions of Theorem 3.4.

Theorem 3.6. *Suppose that $f \in \mathbb{Z}[x, y]$ is a monic irreducible cubic binary form with negative discriminant. Then there exists an effectively computable bound to the number of solutions of the Diophantine equation $f(x, y) = 1$.*

Proof. Since the discriminant of f is negative, its Galois group must be S_3. The group S_3 contains a cycle of length 3, so by Theorem 3.5, there exists a prime $p \neq 2$ such that $f \pmod p$ is irreducible in $\mathbb{F}_p[x]$. We can find this prime by checking the irreducibility of $f \pmod q$ for all primes q, starting at 3. Now f is irreducible over $\mathbb{Q}_p$ as well. Let θ be a root of $f(x, 1)$ and $K = \mathbb{Q}(\theta)$ with fundamental unit ϵ. By Lemma 1.56, ϵ^{p^3} is of the desired form. Now we can apply Theorem 3.4. □

Let us apply the proof of Theorem 3.4 to two specific examples. In both examples, we need the value of the discriminant of the number field. There exist very effective methods for computing these. One of these can be found in chapter 3 of [16]. I have used *Mathematica* to do the computations.

Proposition 3.7. *The only solutions to the Diophantine equation* $f(x,y) = x^3 + 6xy^2 - y^3 = 1$ *are* $(x,y) = (1,0)$, $(x,y) = (0,-1)$ *and* $(x,y) = (1,6)$.

Proof. Firstly, $f(x,1) = x^3 + 6x - 1$ has no roots $\pmod 5$ and is hence irreducible in $\mathbb{Q}[x]$. Moreover, $f(x,1)$ has no roots $\pmod 9$ and is hence irreducible in $\mathbb{Q}_3[x]$ as well. Also, the discriminant $\Delta(f) = -4 \cdot 6^3 - 27 < 0$. Let θ be a root of $f(x,1)$. Since the discriminant of $\mathbb{Q}(\theta)$ is -891, we can apply Theorem 1.82, to compute that a unit ϵ is a fundamental unit when $1 < \epsilon <\sim 35.9$. We find that $\epsilon = -\theta$ is a unit with norm 1 and $1/\epsilon \sim 6$, making $1/\epsilon$ and hence ϵ a fundamental unit. Since $\epsilon^3 = 1 - 6\theta$, we can apply Theorem 3.4 with $p = 3$. Let $\mathbf{p}$ be the unique ideal in $\mathbb{Q}(\theta)$ above 3. We compute that

$$\begin{aligned}
\epsilon^0(x - y\theta) &= x - y\theta, \\
\epsilon^1(x - y\theta) &= -x\theta + y^2\theta^2 \text{ and} \\
\epsilon^2(x - y\theta) &= -y + 6y\theta + x\theta^2.
\end{aligned}$$

In the notation of Theorem 3.4, $\alpha = -2\theta$ and $v_0 = 0$, $v_1 = -2$, $v_3 = 0$. We compute that

$$\exp_3(k \log_3(1 - 6\theta)) \equiv 1 - \left(6\theta - \frac{6^2}{2}\theta^2 - 2 \cdot 6^2\theta^3\right) k + \frac{6^2}{2}\theta^2 k^2 - 2 \cdot 6^2\theta^3 k^3 \pmod{3^3\mathbb{Z}_{\mathbf{p}}}.$$

Since the coefficient of $x - y\theta$ for θ^2 is constant and equal to 0, we can compare the coefficients for θ^2 to find that $0 = \sum_{j \geq 0} f_{2,j} k^j$, where $f_0 = 0$, $f_1 \not\equiv 0 \pmod{3^3\mathbb{Z}_3}$, $f_2 \not\equiv 0 \pmod{3^3\mathbb{Z}_3}$ and $f_j \equiv 0 \pmod{3^3\mathbb{Z}_p}$ for $j \geq 3$. Therefore, we can apply Strassmann with $N = 2$ to find at most two solutions for $l = 0$. Since $(x,y) = (1,0)$ and $(x,y) = (1,6)$ are solutions corresponding to $l = 0$ with respectively $k = 0$ and $k = 1$, they are all. Now we consider $l = 1$. The coefficient for 1 of $\epsilon^l(x - y\theta)$ is constant and equal to 0 and we see that we can collect the coefficients for 1 and apply Strassmann with $N = 0$ to find no solutions for this l. Lastly, we check $l = 2$. We see that $(x,y) = (0,-1)$ is a solution corresponding to $k = 1$. In order to prove that this is the only one, we write $a_0 = -y$, $a_1 = 6y$, $a_2 = x$. We see that $a_1 = -6a_0$. In the basis $\mathcal{B} = \{1, \theta - 1/6, \theta^2\}$, the coefficient of $\epsilon^2(x - y\theta)$ for 1 is equal to 0. The constant coefficient of $\exp_3(k \log_3(1 - 6\theta))$ in the new basis is a power series $\sum_{j \geq 0} b_j k^j$ with $b_0 = 1$, $b_1 \equiv 1 \pmod{3\mathbb{Z}_3}$ and $b_j \equiv 0 \pmod{3\mathbb{Z}_3}$ for $j \geq 2$. Therefore, we can apply Strassmann with $N = 1$ to this power series to conclude that $(0,-1)$ was indeed the only solution for $l = 2$. □

Proposition 3.8. *The only solutions to the Diophantine equation* $x^3 + 2y^3 = 1$ *are* $(x,y) = (1,0)$ *and* $(x,y) = (-1,1)$.

Proof. Let $f(x,y) = x^3 + 2y^3$. Then $f(x,1) \in \mathbb{Z}[x]$ is Eisenstein with $p = 2$, hence irreducible. We also see that $f(x,1)$ has one real and two complex roots. Since $x^3 + 2$

has no roots modulo 9, it is irreducible over $\mathbb{Q}_3$ as well. We want to apply Theorem 3.4 with $p = 3$. Let θ be a third root of 2 and $\mathbf{p}$ the unique ideal in $\mathbb{Q}(\theta)$ above 3. We can check that $\epsilon = -1 - \theta$ is a unit in the ring of integers of $\mathbb{Q}(\theta)$. The discriminant of $\mathbb{Q}(\theta)$ is -108. Applying Theorem 1.82, we find that ϵ is a fundamental unit when $1 < \epsilon <\sim 7.1$. Since $1/\epsilon \sim 3.8$, $1/\epsilon$ is a fundamental unit and ϵ as well. We compute that

$$\epsilon^3 = (-1-\theta)^3 = 1 - 3\theta - 3\theta^2,$$

so Theorem 3.4 applies with $p = 3$. We compute that

$$\begin{aligned}
\epsilon^0(x - y\theta) &= x - y\theta, \\
\epsilon^1(x - y\theta) &= -x - (y - x)\theta + y\theta^2 \text{ and} \\
\epsilon^2(x - y\theta) &= -x - 2y + (y - 2x)\theta + (2y - x)\theta^2.
\end{aligned}$$

We see that the coefficient of $\exp_3(k \log_3(1+3\theta-3\theta^2))$ for θ^2 is equal to $-3k \pmod{3^2\mathbb{Z}_3}$. Therefore, we can apply Strassmann with $N = 1$ to the power series obtained for the coefficient of θ^2 to find at most one solution for $l = 0$. Since $(1, 0)$ is such a solution with $k = 0$, it is the only one. For $l = 1$, we notice that $\epsilon^1(x - y\theta) \not\equiv 1 \pmod{3\mathbb{Z}_\mathbf{p}}$, regardless of the values of x and y. Thus, we find no solutions for this l. Lastly, we consider $l = 2$. Since $-3(-x - 2y) + 4(y - 2x) - 5(2y - x) = 0$, we consider the basis $\mathcal{B} = \{1, -\frac{1}{12} + \frac{1}{4}\theta, -\frac{1}{15} - \frac{1}{5}\theta^2\}$. In this basis, $\epsilon^2(x - y\theta)$ has a coefficient for 1 equal to 0. Also, we can compute that $\pmod{3^2\mathbb{Z}_\mathbf{p}}$ we have

$$\exp_3(k \log_3(1-3\theta-3\theta^2)) \equiv 1-(3\theta+3\theta^2)k = 1-12\left(-\frac{1}{12} + \frac{1}{4}\theta\right)k+15\left(-\frac{1}{15} - \frac{1}{5}\theta^2\right)k.$$

Thus, we can apply Strassmann with $N = 1$ to the power series obtained by comparing the coefficients for 1 to find at most one solution for $l = 2$. Since $(x, y) = (-1, 1)$ is a solution corresponding to $l = 2$ and $k = 0$, it is the only one. □

Note that the proof of Theorem 3.4 explicitly uses the fact that the degree of $f(x, 1)$ is at least 3. A similar proof would hence not work for monic irreducible forms f of degree 2 such that $f(x, 1)$ has two real roots. Of course, it could never have worked because of Corollary 3.3. We can, however, proof an analogous statement in the degree 4 case. First we can find a condition on f using Theorem 3.5.

Lemma 3.9. *Suppose that $f(x, y) \in \mathbb{Z}[x, y]$ is a monic irreducible binary form of degree 4 such that $f(x, 1)$ has four non-real roots. Then there exists a prime number $p \neq 2$ such that there is an irreducible factor g of $f(x, 1)$ in $\mathbb{Q}_p[x]$ of degree ≥ 3 if and only if the Galois group of $f(x, 1)$ is not the Klein group V_4.*

Proof. Suppose that the Galois group of $f(x, 1)$ is not V_4. From Galois theory, we know that the Galois group of f must then be C_4, D_4, A_4 or S_4, up to inner automorphisms. All of these groups contain either a cycle of length 4 or a cycle of length 3, so we conclude from Theorem 3.5 that infinitely many such primes exist.

For the converse, suppose that g is an irreducible factor of $f(x, 1)$ in $\mathbb{Q}_p[x]$ of degree ≥ 3 for a prime $p > 2$. We can use Hensel's Lemma to find that $g \pmod p$ is also an

irreducible factor of $f \pmod p$ in $\mathbb{F}_p[x]$. If p divides the discriminant of g, then the derivative $g' = 0$. Because g is irreducible, g divides $\phi(x) = x^{p^n} - x$, say $\phi = g \cdot q$, where n equals 3 or 4 and $q \in \mathbb{F}_p[x]$. But then the derivative $\phi' = q' \cdot g$, so g divides both ϕ and ϕ', a contradiction since the degree of g is greater than 1. Therefore, p does not divide the discriminant of f. Then the fact that the degree of g is ≥ 3 implies that we can find a cycle of length 3 or 4 in the Galois group of $f(x, 1)$ (see [6] page 36). Such a cycle does not exist in V_4. □

Theorem 3.10. *Suppose that $f(x, y) \in \mathbb{Z}[x, y]$ is a monic irreducible binary form of degree 4 such that $f(x, 1)$ has four non-real roots and the Galois group of $f(x, 1)$ is not V_4. Then there exists an effectively computable bound for the number of solutions to the Diophantine equation $f(x, y) = 1$.*

Proof. By the previous theorem, there exists a prime $p > 2$ and an irreducible factor g of $f(x, 1)$ in $\mathbb{Q}_p[x]$ of degree ≥ 3. Let θ be a root of $f(x, 1)$ and using Lemma 1.56, take $m \in \mathbb{Z} \setminus \{0\}$ such that the fundamental unit ϵ of $K = \mathbb{Q}(\theta)$ has $\epsilon^m = \pm 1 + p(v_0 + v_1\theta + v_2\theta^2 + v_3\theta^3) := 1 + p\alpha$ with each $v_i \in \mathbb{Q}_p$ and $\mathrm{ord_p}\, \alpha \geq 0$. By abuse of notation, we also write θ for a root of g. Note that $s + t - 1 = 1$, so we again have one fundamental unit. By Theorem 2.42, we can find a unique prime ideal $\mathbf{p}$ above p in K that is equivalent to the p-adic norm we find from the inclusion of $\mathbb{Q}(\theta)$ into $\mathbb{Q}_p(\theta)$. The proof is now analogous to that of Theorem 3.4, where we only need to distinguish the cases $[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = 3$ and $[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = 4$. In both cases, we can use the fact that any set of four or five elements of the $\mathbb{Q}$-vector space spanned by $\{1, x, y\}$ is linearly dependent over $\mathbb{Q}$. The only other difference with the degree 3 case is that $\mathrm{N}(-1) = \mathrm{N}(1)$ since the degree is 4 and that we can have a third or fifth root of unity in $\mathbb{Q}(\theta)$. So instead of considering $\epsilon^l(x + y\theta)$, we consider $(-1)^i\epsilon^l(x + y\theta)$ when there are no roots of unity of order > 2 in $\mathbb{Q}(\theta)$, $(-1)^i\zeta_3^j\epsilon^l(x + y\theta)$ when $\zeta_3 \in \mathbb{Q}(\theta)$ is a third root of unity and $(-1)^i\zeta_5^k\epsilon^l(x - y\theta)$ when $\zeta_5 \in \mathbb{Q}(\theta)$ is a fifth root of unity, where $0 \leq i \leq 1$, $0 \leq j \leq 2$, $0 \leq k \leq 4$ and $0 \leq l < m$. □

In the below propositions in this section, we deal with equations of degree larger than 3. For number fields of this degree, we did not provide a way to find the fundamental unit, as was done in Theorem 1.82. Instead, we rely on the fact that algorithms to find the fundamental units exist and have been implemented in computer software, like *Mathematica*.

Proposition 3.11. *The only solutions for the Diophantine equation $f(x, y) = x^4 + 4x^3y + 2x^2y^2 - 4xy^3 + 3y^4 = 1$ are $(x, y) = (1, 0)$ and $(x, y) = (-1, 0)$.*

Proof. One can check that $\theta = \sqrt{2 + \sqrt{-2}} - 1$ is a root of $f(x, 1)$. Let $K = \mathbb{Q}(\theta)$. Also, one can check that the fundamental unit of K is equal to $\epsilon = 13 + 10\theta + 2\theta^2$ and that $\epsilon^2 = 157 + 276\theta + 144\theta^2 + 24\theta^3 = 1 + 3(52 + 92\theta + 48\theta^2 + 8\theta^3)$. Therefore, we take $m = 2$ and $p = 3$. From $\theta^4 + 4\theta^3 + 2\theta^2 - 4\theta = -3$, we find that $\min(\mathrm{ord}_3(\theta), \ldots, \mathrm{ord}_3(\theta^4)) = 1$, which implies that $\mathrm{ord}_3(\theta) = 1/4$. Since the ramification index of the extension $\mathbb{Q}_3 \subset \mathbb{Q}_3(\theta)$ is $e = 4$ and we know that $e \leq [\mathbb{Q}_3(\theta) : \mathbb{Q}_3] \leq 4$, we conclude that $[\mathbb{Q}_3(\theta) : \mathbb{Q}_3] = 4$, so

that $f(x,1)$ is irreducible in $\mathbb{Q}_3[x]$ and hence in $\mathbb{Q}[x]$ as well. Also, it is not difficult to see that K contains no third of fifth root of unity. We now compute that

$$\begin{aligned}
&\pm\epsilon^0(x-y\theta) = \pm(x-y\theta),\\
&\pm\epsilon^1(x-y\theta) \equiv \pm(-\theta-\theta^2-\theta^3) && \pmod{3\mathbb{Z}_3[\theta]},\\
&\pm\epsilon^2(x-y\theta) \equiv \pm(x+y+(x-y)\theta) && \pmod{3\mathbb{Z}_3[\theta]},\\
&\pm\epsilon^3(x-y\theta) \equiv \pm((1+y)\theta-\theta^2+y\theta^3) && \pmod{3\mathbb{Z}_3[\theta]}.
\end{aligned}$$

For $l=1$ and $l=3$, the coefficient for 1 is constant and equal to 0 $\pmod{3\mathbb{Z}_3[\theta]}$, so we can always apply Strassmann with $N=0$ to the power series obtained from comparing the coefficient of 1. This yields no solutions for $l=1$ and $l=3$. For $l=2$, notice that we can only achieve that $x+y \equiv 1 \pmod{3\mathbb{Z}_3}$ and $x-y \equiv 0 \pmod{3\mathbb{Z}_3}$ when $(x,y) \equiv (-1,-1) \pmod 3$. However, this contradicts the restriction that $f(x,y) \equiv 1 \pmod 3$. Therefore, we can always apply Strassmann with $N=0$ to one of the coefficients and we do not find any solutions for $l=2$ either.

Lastly, we consider $l=0$. Comparing the coefficient for θ^3 gives, in the notation of Theorem 3.4, $\sum_j f_{3,j}k^j = 0$, where $f_{3,0}=0$, $f_{3,1} \equiv 24 \pmod{3^2\mathbb{Z}_3}$ and $f_{3,j} \equiv 0 \pmod{3^2\mathbb{Z}_3}$ for $j \geq 2$. Thus, applying Strassmann with $N=1$ gives at most one solution. This goes for both the plus and the minus case, so we find at most two solutions to the Diophantine equation $f(x,y)=1$. Since $(x,y)=(\pm 1,0)$ are solutions corresponding to $l=0$ and $k=0$, they must be all. □

Now that we have seen how the idea works for number fields with one fundamental unit, we can start to think about how this generalizes to arbitrary amounts of fundamental units. A difficulty that arises is that we would then like to consider p-adic power series in multiple variables $x_1,\ldots,x_r$. However, we did not study such power series in this thesis. Therefore, we will restrict ourselves to the easiest case, in which we are still able to work with one variable.

Theorem 3.12. *Suppose that $f(x,y) \in \mathbb{Z}[x,y]$ is an irreducible monic binary form of degree n and that θ is a root of $f(x,y)$. Let $\{\epsilon_1,\ldots,\epsilon_r\}$ be the set of all (distinct) fundamental units of $K=\mathbb{Q}(\theta)$. Also, assume we have $m_1,\ldots,m_r \in \mathbb{Z}$ and an odd prime p such that for each $0 \leq i \leq k$ we have that $\epsilon_i^{m_i} = \pm 1 + p(v_{i,0}+v_{i,1}\theta+\ldots+v_{i,n-1}\theta^{n-1})$ with each $v_{i,j} \in \mathbb{Z}_p$ and moreover $d=[\mathbb{Q}_p(\theta):\mathbb{Q}_p] \geq 3$ and there exists $k \geq 2$ and $1 \leq i \leq r$ such that $v_{i,k} \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Suppose that W is the (finite) set of roots of unity in K and for each $w \in W$ and $0 \leq l_i < |m_i|$, where $1 \leq i \leq r$ and not all l_i equal to 0 and $w=\pm 1$ simultaneously, we have that $w\epsilon_1^{l_1}\cdots\epsilon_r^{l_r}(x-y\theta) = a_0+a_1\theta+\ldots+a_{d-1}\theta^{d-1}$ with $a_0 \not\equiv 1 \pmod{p\mathbb{Z}_p}$ or $a_i \not\equiv 0 \pmod{p\mathbb{Z}_p}$ for some $i \geq 1$. Then the only solutions to the Diophantine equation $f(x,y)=1$ are $(x,y)=(\pm 1,0)$ when n is even and $(x,y)=(1,0)$ when n is odd.*

Proof. Again, we can write $f(x,y) = \mathrm{N}_{K/\mathbb{Q}}(x-y\theta)$. Define $\alpha_i = v_{i,0}+v_{i,1}\theta+\ldots+v_{i,n-1}\theta^{n-1}$ for each i. By the same reasoning as in the proof of Theorem 3.4, $(1+p\alpha_i)^{k_i}$ converges in $\mathbb{Q}_p(\theta)$ as a power series in k_i. Also, let $\mathbf{p}$ be the unique ideal in K above p.

If we have a solution (x, y), then there exist $w \in W$ and $0 \leq l_i < |m_i|$ such that

$$w\epsilon_1^{l_1} \cdots \epsilon_k^{l_r}(x - y\theta) = (1 + p\alpha_1)^{k_1} \cdots (1 + p\alpha_k)^{k_r}. \tag{3.2}$$

Since for each i, $(1 + p\alpha_i)^{k_i} = 1 + pz_i$ with $z_i \in \mathbb{Z}_p[\theta]$, we find that the right-hand side of 3.2 can be written as $1 + pz$ with $z \in \mathbb{Z}_p[\theta]$. However, by assumption, the left-hand side cannot, unless $0 = l_1 = \ldots = l_r$ and $w = \pm 1$. Consider i and k such that $v_{i,k} \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Then we write

$$\prod_{m \neq i}(1 + p\alpha_m)^{k_m} = 1 + pw_i \text{ where } w_i \in \mathbb{Z}_p$$

to conclude that the right-hand side of 3.2 is equal to $1+pz_i+p^2w_iz_i$. Comparing the coefficients for θ^k, we get the equation $0 = \pm \sum_j g_j k_i^j$, where $g_0 = 0$, $g_1 \equiv pv_{i,k} \pmod{p^2\mathbb{Z}_p}$ and $g_j \equiv 0 \pmod{p^2\mathbb{Z}_p}$ for $j \geq 2$. Thus, we may apply Strassmann with $N = 1$ to find at most one solution for this power series. Taking $w = 1$, we see that $k_i = 0$ gives this solution with $(x, y) = (1, 0)$. In the case that $w = -1$, $k_1 = 0$ yields $(x, y) = (-1, 0)$ as the only possibility. This is a solution to our Diophantine equation if and only if n is even. □

Despite the many assumptions we need to do to prove Theorem 3.10, the implications it has are certainly not trivial, as the following example illustrates.

Proposition 3.13. *The trivial solution is the only solution for the Diophantine equation* $f(x, y) = x^5 - 2y^5 = 1$.

Proof. The polynomial $f(x, 1)$ is Eisenstein with $p = 2$ so irreducible in $\mathbb{Q}[x]$. Also, $f(x, 1)$ has one real and four complex roots, so by Dirichlet's unit theorem there are two fundamental units, which turn out to be $\epsilon_1 = \theta - 1$ and $\epsilon_2 = 1 + \theta + \theta^3$. Computing their fifth powers yields

$$\begin{aligned}
\epsilon_1^5 &= 1 + 5\theta - 10\theta^2 + 10\theta^3 - 5\theta^4 &&= 1 + 5(\theta - 2\theta^2 + 2\theta 3 - \theta^4) \\
\epsilon_2^5 &= 151 + 105\theta + 100\theta^2 + 95\theta^3 + 65\theta^4 &&= 1 + 5(30 + 21\theta + 20\theta^2 + 19\theta^3 + 13\theta^4),
\end{aligned}$$

where θ is a root of $x^5 - 2$. We would like to apply Theorem 3.12 with $p = 5$. One can check that $f(x, y)$ is irreducible over $\mathbb{Z}/25\mathbb{Z}$ and hence over $\mathbb{Q}_5$ as well. Also, the only roots of unity in $\mathbb{Q}(\theta)$ are $W = \{\pm 1\}$. Using a programme like *Mathematica*, one can check that the 25 different expressions $\epsilon_1^{l_1}\epsilon_2^{l_2}(x - y\theta)$ are never of the form $a_0 + a_1\theta + \ldots + a_4\theta^4$, where $a_0 \equiv 1 \pmod{5\mathbb{Z}_5}$ and $a_i \equiv 0 \pmod{5\mathbb{Z}_5}$ for $1 \leq i \leq 4$. In order to see this, note that all solutions of $x^5 - 2y^2 \equiv 1 \pmod 5$ are $(x, y) \in \{(1, 0), (-1, -1), (0, 2), (2, -2), (-2, 1)\}$. Also, we see that $v_{1,2} = -2 \not\equiv 0 \pmod{5\mathbb{Z}_5}$. All conditions of Theorem 3.12 are now satisfied, so we conclude that $(x, y) = (1, 0)$ is the only solution to the Diophantine equation $f(x, y) = 1$. □

Note that Theorem 3.12 can also be applied to obtain Corollary 3.11.

In this section, we have applied Skolem's method to three specific kinds of Thue equations. It is possible to generalize Skolem's method in such a way that a general proof for the finiteness of solutions of Thue equations is obtained. Borevich and Shafarevich extended Skolem's ideas using p-adic manifolds to obtain the following result.

Theorem 3.14. *If $f \in \mathbb{Z}[x,y]$ is an irreducible form of degree at least 3 such that $f(x,1)$ has at least one complex root and $c \in \mathbb{Z} \setminus \{0\}$, then the equation $f(x,y) = c$ has a finite number of integer solutions.*

A proof can be found in [1]. The theory behind the proof goes beyond the scope of this thesis. We can describe the intuition behind the condition that $f(x,1)$ needs to have at least one complex root. Suppose that θ is a root of $f(x,1)$ and that we have r fundamental units in the ring of integers of $K = \mathbb{Q}(\theta)$. Applying the same ideas as in Theorem 3.4, we get finitely many equations similar to (3.1) that look like this:

$$p(x,y) = \sum_{j_i \geq 0} f_{0,j_1,\ldots,j_r} k_1^{j_1} \cdots k_r^{j_r} + \sum_{j_i \geq 0} f_{1,j_1,\ldots,j_r} k_1^{j_1} \cdots k_r^{j_r} \theta + \ldots + \sum_{j_i \geq 0} f_{n-1,j_1,\ldots,j_r} k_1^{j_1} \cdots k_r^{j_r} \theta^{n-1},$$

where k_i is a variable power of the i-th fundamental unit ϵ_i and p is a polynomial in $\mathbb{Q}[\theta][x,y]$. If we write $p(x,y) = a_0 + a_1\theta + \ldots + a_{n-1}\theta^n$, this amounts to solving the n equations $\sum_{j_i \geq 0} f_{m,j_1,\ldots,j_r} k_1^{j_1} \cdots k_r^{j_r} = a_m$, where $m \in \{0,\ldots,n-1\}$ for the $r+2$ variables $x, y, k_1, \ldots, k_r$. Therefore, naively, one would expect such a system of equations to have finitely many solutions only when $r+2 \leq n$, or $r+1 \leq n-1$. This is only the case when $f(x,1)$ has at least one complex root.

3.2 Skolem's equations $x^3 + dy^3 = 1$

In this section we prove a theorem by Skolem on the Diophantine equations $x^3 + dy^3 = 1$ for $d \in \mathbb{Z}$ and we consider some of its implications. The idea behind the proof of the theorem is similar to the idea behind the theorems in Section 3.1. It relies on p-adic power series and Strassmann's Theorem. We present a proof inspired by [2].

Theorem 3.15 (Skolem)**.** *For any $d \in \mathbb{Z}$ there exists at most one non-trivial solution (x,y) to the Diophantine equation $f(x,y) = x^3 + dy^3 = 1$.*

Proof. First we deal with the case $d = \pm 1$. Since we can replace y by $-y$ in a solution, the cases $d = 1$ and $d = -1$ are equivalent, so we consider $d = -1$. Then $x^3 - y^3 = (x-y)(x^2+xy+y^2) = 1$, so we have that $x - y = x^2 + xy + y^2 = \pm 1$. Substituting $x = y \pm 1$ in the quadratic part, we find that $3y(y \pm 1) + 1 = \pm 1$. Looking modulo 3, we find $1 \equiv \pm 1 \pmod 3$, so we get $3y(y+1) = 0$, giving $y = 0$ or $y = -1$. Hence $(x,y) \in \{(1,0),(0,-1)\}$ are all the solutions. Now assume $d \neq \pm 1$. We may suppose that d is cube-free. Otherwise, we could write $d = ac^3$ with a cube-free or equal to ± 1. If (x,y) is a solution to $x^3 + dy^3 = 1$, then (x, cy) is a solution to $x^3 + ay^3 = 1$, so we are left with the cube-free case. Therefore, if θ is a root of $x^3 - d$ and $K = \mathbb{Q}(\theta)$, we have that $[K : \mathbb{Q}] = 3$. By Lemma 3.2 and because $-\theta$ is a root of $x^3 + d$, we can write the equation as $f(x,y) = \mathrm{N}_{K/Q}(x + y\theta) = 1$.

Now suppose we have two units of $x_1 + y_1\theta$ and $x_2 + y_2\theta$ of K, both with norm 1. Since $f(x,1)$ has two complex and one real root, we have one fundamental unit ϵ by Dirichlet's unit theorem. We may assume that $\mathrm{N}_{K/\mathbb{Q}}(\epsilon) = 1$, otherwise we take $-\epsilon$. Hence there exist $m_1, m_2 \in \mathbb{Z}$ such that $x_1 + y_1\theta = \epsilon^{m_1}$ and $x_2 + y_2\theta = \epsilon^{m_2}$. Suppose that (x_1, y_1)

and(x_2, y_2) are not the trivial solution, i.e. $m_1, m_2 \neq 0$. Then we can define $N = m_1/m_2$. Also, we can simplify m_1/m_2 such that $m_1/m_2 = n_1/n_2$ with $\gcd(n_1, n_2) = 1$ and we may suppose that $3 \nmid n_2$; otherwise we consider n_2/n_1. This means that $N \in \mathbb{Z}_3$. Since one of $n_1, n_1 - n_2, n_1 + n_2$ is divisible by 3, we may write $N = 3M + r$ with $M \in \mathbb{Z}_3$ and $r \in \{0, 1, 2\}$. We compute that

$$(x_1 + y_1\theta)^3 = 1 + 3x_1y_1(x_1\theta + y_1\theta^2) =: 1 + 3\alpha.$$

Therefore, we can use Lemma 2.51 to write

$$x_2 + y_2\theta = (1 + 3\alpha)^M(x_1 + y_1\theta)^r$$

where $(1+3\alpha)^M = \exp_3(M \log_3(1+3\alpha)) = \sum_{j\geq 0} c_j M^j$ is a power series in M. Just like in the proof of Theorem 3.4, we find that $c_0 = 0$, $c_1 = 3\alpha + 3^2x_1^2y_1^2A$ for $A \in \mathbb{Z}_3[\theta]$ and $c_j \in 3^2x_1^2y_1^2\mathbb{Z}_3[\theta]$. Hence we find that

$$x_2 + y_2\theta = (1 + 3Mx_1y_1(x\theta + y\theta^2) + 9Mx^2y^2C)(x + y\theta)^r \text{ for some } C \in \mathbb{Z}_3[\theta].$$

If we write $C = C_0 + C_1\theta + C_2\theta$ and collect the coefficients for θ^2 in this expression, we find that

$$0 = \begin{cases} 3Mx_1y_1^2(1 + 3x_1C_2) & \text{if } r = 0 \\ 3Mx_1^2y_1^2(2 + 3(y_1C_1 + x_1C_2)) & \text{if } r = 1 \\ y_1^2(1 + 9Mx_1^2(x_1 + C_2x_1^2 + 2C_1x_1y_1 + C_0y_1^2)) & \text{if } r = 2. \end{cases}$$

Since $y_1 \neq 0$, we can divide by y^2 in the case $r = 2$ to obtain a contradiction modulo 3. Since $d \neq \pm 1$ there are no solutions to $x^3 + dy^3 = 1$ with $x = 0$, so $x_1 \neq 0$. Therefore, in the other cases, we can divide by $3Mx_1y_1^2$ ($r = 0$) and $3Mx_1^2y_1^2$ ($r = 1$) when $M \neq 0$ to again obtain a contradiction modulo 3. If $M = 0$ and $r = 0$, we have that $N = 0$ and hence $n_2 = 0$, a contradiction. Hence we must have $M = 0$ and $r = 1$, which gives $N = 1$ and $n_1 = n_2$, implying that $(x_1, y_1) = (x_2, y_2)$ as desired. □

Example 3.16. The Diophantine equation $x^3 + 2y^3 = 1$, which we solved in Corollary 3.8, can now be solved in a much easier way. We see that $(1, 0)$ and $(-1, 1)$ are two solutions, so by Theorem 3.15, they are the only ones. We can do the same for $d = 7$, since $(2, -1)$ is a non-trivial solution of $x^3 + 7y^3 = 1$. In general, for any $n \in \mathbb{Z}_{>0}$, the Diophantine $x^3 + (n^3 - 1)y^3 = 1$ has as the non-trivial solution the pair $(x, y) = (n, -1)$.

This example demonstrates the power of Theorem 3.15 and therefore of Skolem's p-adic method for solving Thue equations, which now allows us to solve an entire class of Diophantine equations in a single blow.

The Russian mathematician Boris Delone (1890-1980) proved the following theorem, which shows exactly when the non-trivial solution mentioned in Theorem 3.15 exists for positive cube-free $d \in \mathbb{Z}$. When Delone proved his theorem, he was not (yet) familiar with p-adic numbers, so his approach could be considered ad hoc. However, from modern perspective, the ideas behind his approach show similarities with Skolem's p-adic method.

Theorem 3.17 (Delone)**.** *For $d \in \mathbb{Z}_{>0}$ cube-free, the Diophantine equation $x^3 + dy^3 = 1$ has a non-trivial solution if and only if the fundamental unit ϵ of the ring $\mathbb{Z}[d^{1/3}]$ such that $0 < \epsilon < 1$ is of the form $x + yd^{1/3}$ wity $x, y \in \mathbb{Z}$.*

Delone's proof can be found in [3]. Note that for any fundamental unit ϵ, one of the fundamental units $\epsilon, -\epsilon, \epsilon^{-1}$ and $-\epsilon^{-1}$ lies in the interval $(0, 1) \subset \mathbb{R}$. Also note that $\mathbb{Z}[d^{1/3}]$ is an order by the remarks above Theorem 1.80 and that this theorem shows the existence of the fundamental unit ϵ in $\mathbb{Z}[d^{1/3}]$.

Reflection

In one of the first meeting with my supervisor-to-be, I was given three possible subjects for my bachelor's thesis. I had come to Sander Dahmen and Rob de Jeu with the request to help me to find a subject for my bachelor's thesis that "had something to do with number theory". The first options they came up with were

1. Diophantine equations,
2. p-adic numbers and p-adic zeta functions and
3. dessins d'enfants.

The p-adic zeta functions are a p-adic generalization of the Riemann zeta function. More information about p-adic zeta functions can be found in [9]. A dessin d'enfant (French for " children's drawing") is a graph with vertices alternatingly coloured black and white that can be assigned to holomorphic functions from a Riemann surface to the Riemann sphere.

Before doing any research on these subjects, Diophantine equations would have been my first choice. This, because I have always been more than others interested in the integers and their properties. I believe that in its essence, mathematics is a theory that has been developed in order to understand the properties of the natural numbers. Therefore I first looked at the book *Diophantine equations* by Louis Mordell [14], but I returned it to the library after just half an hour of scanning its content. Mordell presents in his book many ad hoc solutions to Diophantine equations and many of these solutions involve (large amounts of) calculations. I, however, preferred to be working in a more abstract and algebraic setting.

Secondly, I scanned *p-adic Numbers, p-adic Analysis and Zeta-Functions* by Neil Koblitz [9]. On one hand, I became enthusiastic about the idea of the p-adic numbers and because of my interest in the integers, I liked the idea of generalized zeta-functions. On the other, I thought that a choice for option 2 would result in too many p-adic analysis. Lastly, I read about dessins d'enfants, which I also found an interesting topic.

In the end, I am happy that dr. Dahmen proposed a more theoretic approach towards solving Diophantine equations that also required the knowledge of the p-adic numbers. I was immediately convinced by this combination of subjects, because it allowed me to immerse myself into new mathematical theory, while it also gave me the opportunity to do research on Diophantine equations myself.

In retrospect, I think that I made an excellent choice, because I very much enjoyed writing this thesis. I studied most of the algebraic number theory from [16], which is a very well written and accessible textbook for bachelor students who have had a first

course in ring and field theory. I would very much advise this book to any third-year bachelor student with an interest in algebra or number theory. Thanks to this book, I was able to study all the number theory that I needed relatively quickly and without any major problems.

For studying the p-adic number theory, I used a combination of [9] and [7]. In [9], Koblitz presents a short and direct path towards the p-adic Weierstrass preparation theorem. At times, however, it was more difficult to read, often because proofs were left to the reader. In addition, I used [7] to fill the gaps and to provide additional information. Gouvea explains the p-adic theory in [7] in a more elaborate way, which makes the book more accessible. However, I found that this went at the expense of the general overview of the theory. Together, the books were an excellent way to study the p-adic numbers and I encountered no major difficulties while studing this piece of the theory.

Furthermore, even though Chapter 3 is based on [2], I formulated and proved all the lemma's and theorems in Section 3.1 myself. Despite that fact that it was much harder than studying from textbooks, I enjoyed doing some mathematical research myself. Once, after having written about seven pages of Section 3.1, I discovered a crucial error in all the proofs and examples I had written down, which caused me to rewrite most of this section. In spite of the time this cost, it was satisfying to be presented with a problem and to be able to solve it all by yourself.

Lastly, I would like to thank my supervisor dr. Sander Dahmen for all of his help during this project. I am especially greatful for the way he encouraged me to investigate many loose ends into detail, even though that resulted in a lenghty thesis for him to read.

Populaire samenvatting

De stelling van Pythagoras is waarschijnlijk de meest bekende wiskundige stelling van allemaal. Iedere vwo-leerling leert tegenwoordig al in de tweede klas dat voor een rechthoekige driehoek met zijden a, b en c, waar c de lange zijde is, geldt dat

$$a^2 + b^2 = c^2.$$

Het klassieke voorbeeld van zo'n driehoek heeft zijden met lengtes 3, 4 en 5. Inderdaad, $3^2+4^2 = 5^2$. Misschien ben je ooit ook wel een voorbeeld tegengekomen, waar de driehoek zijden had met lengtes 5, 12 en 13. Nu kun je je afvragen: voor welke gehele getallen a, b en c geldt er nog meer dat $a^2 + b^2 = c^2$? Dit is een voorbeeld van een diofantische vergelijking, een vergelijking in meerdere variabelen met gehele coëfficiënten waar je gehele oplossingen voor zoekt. De variabelen in de stelling van Pythagoras zijn a, b en c en de cofficiënten voor al die variabelen zijn gelijk aan 1.

Een ander voorbeeld van een diofantische vergelijking is nu snel gevonden: $a^3+b^3 = c^3$. We zien meteen dat er gehele oplossingen zijn wanneer a, b of c gelijk is aan nul. Andere oplossingen lijken minder gemakkelijk te vinden. In 1621 viel het de Franse wiskundige Pierre de Fermat op dat voor iedere gehele n groter dan 2 de vergelijking $a^n + b^n = c^n$ geen gehele oplossingen leek te hebben. Dit vermoeden werd bekend als 'de Laatste Stelling van Fermat' en sindsdien hebben velen geprobeerd het te bewijzen. Dit lukte pas in 1995, toen de Brit Andrew Wiles een bewijs presenteerde.

Dit verslag staat in het teken van het ontwikkelen van een methode die het mogelijk maakt om een speciaal soort diofantische vergelijkingen op een relatief eenvoudige manier op te lossen. Deze methode maakt gebruik van wiskundige theorie die ook Andrew Wiles gebruikte voor zijn bewijs van de Laatste Stelling van Fermat.

De algebraïsche getaltheorie is één van deze theorieën en misschien wel de meest fundamentele. Deze wordt beschreven in Hoofdstuk 1. Kort gezegd is getaltheorie de studie van de gehele getallen $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$. Aangezien diofantische vergelijkingen gekarakteriseerd worden door gehele coëficienten en we op zoek zijn naar gehele oplossingen, is het niet verwonderlijk dat we eerst wat meer over de gehele getallen willen weten. In het bijzonder bestudeert de getaltheorie de breuken $\mathbb{Q}$, de verzameling van alle getallen $\frac{a}{b}$, waar a en b gehele getallen zijn. De verzameling breuken vormt een *lichaam*, wat betekent dat de som en het product van breuken nog steeds een breuk is en dat er voor iedere breuk $\frac{a}{b}$ een additieve inverse $-\frac{a}{b}$en een multiplicatieve inverse $\frac{b}{a}$ bestaat. Door aan $\mathbb{Q}$ een getal toe te voegen dat geen breuk is (bijvoorbeeld wortel twee) verkrijgen we een nieuw lichaam K. In het geval van wortel twee schrijven we dan $K = \mathbb{Q}(\sqrt{2})$. In zo'n lichaam K kunnen we kijken naar de *ring van gehelen*, de verzameling getallen in K die een nulpunt zijn van een polynoom $a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$,

waar alle a_i gehele getallen zijn. Het is hier belangrijk dat de coëfficiënt van de grootste macht van x gelijk is aan 1. Deze ring van gehelen kun je zien als een veralgemenisering naar K van de gehele getallen in $\mathbb{Q}$. De getaltheorie bestudeert uitbreidingen K van $\mathbb{Q}$ en hun ringen van gehelen.

Vervolgens wordt in Hoofdstuk 2 de theorie van de p-adische getallen bestudeerd. Als je op een klok de tijd 23:00 ziet staan, dan interpreteer je dat als 'elf uur'. Eigenlijk reken je dan *modulo* 12. Dat betekent dat je alle getallen bekijkt ten opzichte van het getal 12. Dus 34 wordt 10, 55 wordt 7 en 48 wordt 0. Het kan soms handig zijn om een diofantische vergelijking modulo een priemgetal te bekijken. Bijvoorbeeld, als je wil inzien dat de vergelijking $5a^2+10b^2 = 4$ geen gehele oplossingen heeft, dan kun je kijken modulo 5. Je ziet dat $5a^2+10b^2$ deelbaar is door 5, ongeacht de waardes van a en b. Dat betekent dat $5a^2 + 10b^2$ gelijk is aan 0 modulo 5 voor alle waardes van a en b. Echter, 4 is niet gelijk aan 0 modulo 5, dus er kunnen geen oplossingen bestaan. Je zou kunnen zeggen dat de p-adische getallen bedacht zijn om modulo p, p^2, p^3 etcetera tegelijk te kunnen kijken, waar p een priemgetal is. Net zoals de reële getallen, zijn de p-adische getallen een uitbreiding van de breuken $\mathbb{Q}$. In de p-adische getallen liggen twee getallen dicht bij elkaar als hun verschil deelbaar is door een hoge macht van p.

Tenslotte is de opgedane kennis van de eerste twee hoofsdstukken in Hoofdstuk 3 toegepast om een speciaal soort diofantische vergelijkingen op te lossen. Dit zijn vergelijkingen van de vorm $f(x, y) = 1$, waar f een *binaire vorm* is. Binair slaat op het feit dat f afhangt van twee variabelen, x en y. Een binaire vorm is een polynoom in x en y, zodat de machten van x en y in de lossen termen altijd optellen tot hetzelfde getal. Een voorbeeld van een binaire vorm is $x^3+6xy^2-y^3$. Je ziet dat de som van de machten van x en y van iedere term gelijk is aan drie. De manier waarop zo'n diofantische vergelijking wordt opgelost is als volgt. Je ziet vrij snel dat $(x, y) = (1, 0), (0, -1), (1, 6)$ drie oplossingen zijn van $x^3 + 6xy^2 - y^3 = 1$. Vervolgens is er met behulp van de kennis uit de eerste twee hoofdstukken een stelling bewezen, waaruit je kan afleiden dat het onmogelijk is dat deze diofantische vergelijking meer dan drie oplossingen heeft. We weten dan met zekerheid dat we alle oplossingen hebben gevonden. De moeilijkheid schuilt in het bewijzen van stellingen die grenzen aangeven voor het aantal oplossingen van diofantische vergelijkingen.

Terug naar de diofantische vergelijking van Pythagoras: $a^2 + b^2 = c^2$. We zagen al oplossingen $(a, b, c) = (3, 4, 5)$ en $(a, b, c) = (5, 12, 13)$. Zijn dit ze dan allemaal? Nee, dit is een voorbeeld van een diofantische vergelijking met oneindig veel oplossingen. Immers, als (a, b, c) een oplossing is, dan is $(a \cdot n, b \cdot n, c \cdot n)$ dat ook voor ieder geheel getal n.

Bibliography

[1] Z.I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press Inc., 1966, http://www.maths.ed.ac.uk/~aar/papers/borevich.pdf

[2] Henri Cohen, *Number Theory Volume I: Tools and Diophantine Equations*, Springer, 2007

[3] B.N. Delone and D.K. Faddeev, *The theory of irrationalities of the third degree*, American Mathematical Society, second printing 1978

[4] Gerard van der Geer, *Syllabus algebra I voorlopige versie*, dictate for the course Algebra 1 at the University of Amsterdam, http://gerard.vdgeer.net/algebra-input.pdf

[5] Gerard van der Geer, *Syllabus algebra IIa voorlopige versie*, dictate for the course Algebra 2 at the University of Amsterdam, http://gerard.vdgeer.net/algebra2-input.pdf

[6] Gerard van der Geer, *Syllabus algebra 3 voorlopige versie*, dictate for the course Galois Theory at the University of Amsterdam, http://www.science.uva.nl/~geer/alg3.pdf

[7] Fernando Q. Gouvêa, *p-Adic Numbers: An Introduction*, Springer, second edition 1997

[8] Robert Guralnick, Murray M. Schacher and Jack Sonn, *Irreducible polynomials which are locally reducible everywhere*, http://www.math.ucla.edu/~mms/poly.pdf

[9] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 1977

[10] T.H. Koornwinder en Jan Wiegerinck, *Analyse: van $\mathbb{R}$ naar $\mathbb{R}^n$*, dictate for the course Analyse: van $\mathbb{R}$ naar $\mathbb{R}^n$ at the University of Amsterdam, http://staff.science.uva.nl/~janwieg/edu/analyse1/AnalyseRRn-input.pdf

[11] H.W. Lenstra and P. Stevenhagen, *Chebotarëv and his Density Theorem*, EBSCO Publishing, 2002, http://www.math.leidenuniv.nl/~reinier/ant/chebotarev.pdf

[12] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, http://www-math.mit.edu/~poonen/papers/chabauty.pdf

[13] B.J.J. Moonen, *Topologie*, dictate for the course Topologie at the University of Amsterdam, http://staff.science.uva.nl/~bmoonen/Topologie/topo.pdf

[14] L.J. Mordell, *Diophantine equations*, Academic Press Inc, 1969

[15] J. Neukirch, *Algebraic number theory*, Springer-Verlag Berlin Heidelberg, 1999

[16] Ian Stewart and David Tall, *Algebraic Number Theory and Fermat's Last Theorem*, CRC Press, third edition 2002

[17] N. Tzanakis and B.M.M. de Weger, *On the Practical Solution of the Thue Equation*, Journal of Number Theory 31, 1989, http://deweger.xs4all.nl/papers/[6]TzdW-Thue-JNumTh[1989].pdf