Algorithmic Investigations in P-Adic Fields

Devdatt P. Dubhashi
Ph.D Thesis

92-1301
September 1992

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501
ALGORITHMIC INVESTIGATIONS IN P-ADIC FIELDS

A Dissertation
Presented to the Faculty of the Graduate School
of Cornell University
in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy

by
Devdatt P. Dubhashi
August 1992
ALGORITHMIC INVESTIGATIONS IN P-ADIC FIELDS

Devdatt P. Dubhashi, Ph.D.
Cornell University 1992

This thesis is concerned with algorithmic investigations in p-adically closed fields, of which Hensel’s field of p-adic numbers is prototypical. The well known analogies between the field of real numbers and the field of p-adic numbers are supplemented from a computational standpoint.

We resolve the complexity of the Decision Problem for Fields in the p-adic case. We work in the new nth power formalism for p-adic fields where the correspondence to the reals is most transparent. First we give an alternating exponential time algorithm for deciding linear sentences in the theory of p-adically closed fields. This also translates into a deterministic algorithm running in exponential space or double exponential time. A deterministic quantifier-elimination procedure for the linear fragment running in double exponential time and space is also presented. Next we employ a quantitative version of a Cell Decomposition Lemma due to Denef to give an alternating exponential time decision procedure for the full theory. As usual this also yields a deterministic decision procedure running in double exponential time or in exponential space, and a quantifier elimination procedure running in double
exponential time and space. These complexity bounds are demonstrated to be essentially optimal by proving matching lower bounds on the respective problems.

We give a simple algorithm to determine all roots among the p-adic integers of a given polynomial equation. This algorithm is a purely symbolic (as opposed to numerical) p-adic version of the classical Newton and Horner iteration methods and has a natural parallel implementation. We also give algorithms for some problems in valued fields and in p-adic semi-algebraic geometry.

Finally we give some additional elementary evidence to support the thesis that certain cosets of \( n \)th powers are the proper p-adic analogues to signs in the real case. This is done by showing that these coset representatives display similar behavior with respect to functions and their derivatives as do the signs in the real case.
Biographical Sketch

Devdatt was born April 27, 1965 in New Delhi, India. After several years of nomadic existence in various parts of India, he returned there, attending first, Delhi Public School and then earning a Bachelor of Technology degree in Computer Science from the Indian Institute of Technology (I.I.T.) Delhi. The tale of how from his adolescent dreams of consorting with the (heavenly) stars, he came to dabble in Computers, we shall leave for future chronicles. In quest of Turing and Tarski, he arrived at Cornell where he gleaned much from the vast storehouse of Knowledge he discovered (notwithstanding occasional disturbing diversions when it seemed doubtful if he was pursuing the higher quests in the spheres of Computer Science or in Tennis and Cooking!). He was awarded a Ph.D. degree for ascertaining upper and lower bounds on the complexities of abstruse mathematical problems. Applying this expertise to evaluate his own contribution, he knows that it is upper bounded by no more than a minuscule but entertains the fond hope that the lower bound is a non-zero constant. Through meeting different peoples and cultures at Cornell, he also learnt about Life and Living and it would probably have made Wittgenstein happy to hear that he comes away a “better” man rather than simply a “cleverer” one. For the next year, he has chosen to inflict himself upon the residents of the Max Planck Institut für Informatik, Saarbrücken, Germany.
To my Parents

For their boundless love, unstinting support and for their countless sacrifices so that I could have all the opportunities for Learning, culminating in this.
Acknowledgements

In the hoary Indian tradition, I start by paying tribute to my teachers: this is my \textit{Gurudakshina} \textsuperscript{1} to them.

First and foremost I thank Dexter Kozen for being my friend, philosopher and guide. In him I found a unique combination of youthful vitality and serene sagacity. It was through him and his work that I came to appreciate beauty and elegance in Mathematics, both for itself and in innovative applications to Computer Science. In particular he is principally responsible for my capitulation to the charms of the \textit{algebraic} mode of thought. I have to thank him for keeping me under his wing and yet allowing me all the freedom I desired and more. I would also like to thank him for being very kind, tolerant and indulgent to me through the many periods of aimless wanderings I was subject to.

Next I would like to thank the other members of my committee: Juris Hartmanis and Richard Shore. It would be a rare student indeed who could boast of so distinguished a committee! Each in his inimitable way, a superb master of the art of pedagogy, each a leader and pioneer in his field and each the most noble and warm of human beings, they set standards which were inspiring and yet very difficult to attain! I can only promise to try.

\textsuperscript{1}Literally translated, "Donation to the teacher"
From my undergraduate days at I.I.T. Delhi, I must record here the singular influence of S.N. Maheshwari whose exciting courses awakened my interest in Theoretical Computer Science.

I would also like to thank Prakash Panangaden who served on my committee until his departure from Cornell for always goading me on (though often without effect!). I would like to thank Moss Sweedler for always encouraging me in my work and for many delightful conversations. My conversion to algebra also owes much to the course I attended lectured by Stephen Chase.

Many thanks to the staff in the Computer Science Department, especially to Jan Batzer, Bekky Personius, Laurie Buck and Suzy Harris.

Next, I would like to thank all the friends and colleagues who contributed in one way or another to my sustenance. There are some insidious tendencies that a writer has to guard against at this stage, namely of omitting some names or favoring more recent memories over equally important but more distant ones. I will try my best below but apologize in advance for (the nevertheless inevitable) omissions.

First those who had to put up with me at home (at various times during six long years): Anant, Arun, Pierre, Samir, Shashank, Shankar and Vasant. Then those who had to do the same at school: Alessandro, Bill, Daniela, Desh, Ida, Suresh...

Some very special thanks: to Shyam, Shashank and Sanjeev (Sanghi) for enduring friendship that transcends the ordinary; to Marie for befriending a lonely Steppenwolf and to Alessandro ("Alenoigre!") for initiating me into Bach, Beethoven, Debussy ... and Cynicism.
For financial support, I am grateful to Cornell University (specifically the Computer Science Department) and to the National Science Foundation (through grants CCR 8806096 and CCR 8901061).

By far though, I am most grateful to my parents. To them I dedicate this thesis as a small token of my love and respect although it can make but the slightest dent in the overwhelming debt I owe them. I warmly thank also my sister Medha and my adorable niece Archana for keeping me entertained during (my rather infrequent) trips home.
# Table of Contents

## 1 Introduction
1.1 Brief History of the P-adics ............................................ 1
1.2 The P-adics in Algebraic Number Theory .......................... 2
  1.2.1 Class Field Theory .................................................. 2
  1.2.2 Diophantine Analysis .............................................. 3
1.3 Motivating Issues behind this Thesis .............................. 5
  1.3.1 Parallels Between the Reals and the P-adics ............... 5
  1.3.2 The Decision Problem for Fields: The P-adic Case ....... 6
1.4 Outline of the Thesis ................................................... 8

## 2 A P-adic Primer
2.1 The Field of p-adic Numbers: Construction and Basic Properties .. 10
  2.1.1 Valuations and Completions ..................................... 10
  2.1.2 The p-adic Numbers: Definition and Basic Properties .... 17
  2.1.3 Further Properties of the p-adics ............................... 19
2.2 The $P_n$-formalism ................................................... 22
  2.2.1 Motivation ....................................................... 22
  2.2.2 Structure of $Q_p^*$ .............................................. 23
  2.2.3 Valuation and $n$-th powers .................................. 26
2.3 The $R-Q_p$ Analogy .................................................. 29
  2.3.1 Algebra ......................................................... 29
  2.3.2 Model Theory .................................................... 31
  2.3.3 Semi-Algebraic Geometry ...................................... 32

## 3 Quantifier Elimination and Decision Procedures for Sentences in P-adic Fields
3.1 Introduction ........................................................... 36
3.2 Some Facts about $Q_p$ .............................................. 40
3.3 Linear Sentences in $Q_p$ ............................................ 41
  3.3.1 Denef's Lemma .................................................... 42
  3.3.2 A Decision Method .............................................. 44
  3.3.3 Complexity of the Decision method ........................... 44
Chapter 1

Introduction

1.1 Brief History of the P-adics

*God created the integers, all else is the work of man.*

Leopold Kronecker.

The p-adic numbers were invented at the turn of this century by the German mathematician Kurt Hensel (1861-1941),[Hen08]. His principal objective was to emulate methods of power series expansions, which play such a central role in the theory of functions, with numbers as well. The idea sprang from the observation that numbers behave in many ways like functions and in fact can be regarded as such on a certain topological space, [Neu90].

The appearance of the p-adics in Hensel’s book was the inspiration for a celebrated paper by E. Steinitz [Ste10] which appeared in Crelle’s Journal. The p-adics were until then regarded as strangers in the mathematical world because of their many unusual properties. A need was therefore felt for a general, abstract and axiomatic theory of fields as *algebraic* structures, into which the p-adics would fit in naturally. It is difficult today to appreciate the impact that this paper had on the mathematics of the day, but let it be noted that it was sufficient to warrant reprinting as a book some twenty years later as a “classic”. We can see its influ-
ence today, for instance, in the subject of *stability theory*, [Bal88] where Steinitz's program of classifying theories by their *invariants* is carried out in great detail for many different theories.

### 1.2 The P-adics in Algebraic Number Theory

In modern times, the p-adics (and, more generally, *valuation theory*) constitute a corner-stone of Algebraic Number Theory, [CF67,Cas86,Has80]. To quote one of the pioneers of the subject, Helmut Hasse, [Has80]:

> There are two quite distinct approaches, the *divisor-theoretic* and the *ideal-theoretic*, to the theory of algebraic numbers...

> It seemed at first that the ideal-theoretic approach was superior... More recently, however, it turned out, first in the theory of quadratic forms and then especially in the theory of hyper-complex numbers (algebras) not only that the division-theoretic or *valuation-theoretic* is capable of expressing the arithmetic structural laws more simply and naturally, by making it possible to carry over the well-known connection between local and global relations from function theory to arithmetic, but also that the true significance of class field theory and the general reciprocity law of algebraic numbers are revealed only through this approach. Thus the scales now tip in favor of the divisor-theoretic approach.

Indeed one may say without too much exaggeration, that the significance of the p-adics to algebraic number theory is comparable to that of the reals for analysis! We give below two representative samples in support of this statement.

#### 1.2.1 Class Field Theory

*Class Field Theory* is concerned with the study of the so-called *global* fields (such as the rationals) and *local* fields (such as the reals and the p-adics). The central
problem studied is to describe all the extensions of these fields, [CF67).

The central result of Global Class-Field Theory is the identification of the maximal abelian\(^1\) extension of the rationals, \(\mathbb{Q}\), [Iwa86,Cas86].

**Theorem 1.1 (Kronecker-Weber)** The maximal abelian extension \(\hat{\mathbb{Q}}_{ab}\) of \(\mathbb{Q}\) is the cyclotomic extension obtained by adjoining all roots of unity. Moreover,

\[
\text{Gal}(\hat{\mathbb{Q}}_{ab}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^*
\]

(where the product is over all primes, \(p\)).

Here, \(\mathbb{Z}_p^*\) is the group of units of the so-called \(p\)-adic integers, see Chapter 2.

In the local case, the fundamental result identifies the structure of all abelian extensions of a \(p\)-adic field by relating it to the multiplicative structure of the field itself, [Neu86]

### 1.2.2 Diophantine Analysis

The fact that they were originally inspired by the analogies of numbers to functions notwithstanding, it is in one of the classical subjects of arithmetic that the \(p\)-adics have had one of their most outstanding triumphs: *Diophantine Analysis*. In a Diophantine problem, we are given a polynomial equation in several variables,

\[
F(x_1, x_2, \ldots, x_n) = 0
\]

and are asked to find its solutions in integers. In general, this is a very difficult problem. In fact, this is the celebrated tenth problem of Hilbert and in a beautiful sequence of developments [Dav82], was shown to be recursively undecidable. Even in particular cases, the problem can be most intransigent. For instance, the famous last “theorem” of Fermat asserts that the Diophantine equation

\[
x^n + y^n = z^n
\]

\(^1\)The adjective refers to a property of the relevant Galois group
has no solution for $n > 2$, [Rib79]. However, to this day, the conjecture remains unresolved $^2$.

One may weaken the question by considering instead the congruences

$$F(x_1, \cdots, x_n) \equiv 0 \pmod{m}$$

for all $m$, or, equivalently, via the Chinese Remainder theorem, the set

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

for all prime powers. The existence or otherwise of solutions to these congruences might give some information on the original question. Through the $p$-adic numbers, this infinite set of congruences can be reduced to the study of a single equation:

**Theorem 1.2** Let $F(x_1, \cdots, x_n)$ be a polynomial with integer coefficients and $p$ a fixed prime. The congruences

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

are solvable for all $k \geq 1$ iff the equation

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

is solvable in the $p$-adic integers.

While the existence of a solution in the $p$-adics is a necessary condition for the existence of a rational solution, the reverse is very seldom true. In the case of quadratic forms however, the deduction can be made. Curiously, this is obtained through the solution of the eleventh problem of Hilbert which H. Hasse achieved with the “utmost of finality and elegance” [Kap77] $^3$. This is the local-global principle of Minkowski and Hasse, [Neu90,Cas86]:

$^2$Though an important breakthrough was made by G. Faltings through the proof of the Mordell conjecture.

$^3$Interestingly, Hasse tells of a postcard from Hensel dated October 2, 1920 that gave him the key idea!
Theorem 1.3 (Hasse-Minkowski) Let \( F(x_1, \cdots, x_n) \) be a quadratic form with rational coefficients. The equation

\[
F(x_1, \cdots, x_n) = 0
\]

has a non-trivial solution in \( \mathbb{Q} \) iff it has a non-trivial solution in \( \mathbb{R} \) and in \( \mathbb{Q}_p \) for all primes \( p \).

1.3 Motivating Issues behind this Thesis

There were two primary issues that motivated this thesis: first, to develop further the analogy between the reals and the p-adics, and second, to resolve quantitatively, the decision problem for the p-adics.

1.3.1 Parallels Between the Reals and the P-adics

As we shall describe in the next chapter, the reals and the p-adics are both natural completions of the rationals (and in fact the only ones). At first glance, though, they are radically different completions. The reals are archimedean completions, the p-adics are non-archimedean. Hence, as topological spaces, for instance, the two are antipodal – the reals are connected, the p-adics are totally disconnected. A reflection of this difference is the two totally different spheres in which they operate: the reals live in the realms of analysis, and the p-adics find their niche in algebraic number theory.

However, despite these contrasts, there are some deep underlying similarities between the two structures. In recent times, a fascinating pattern of analogies between the reals and the p-adics has been revealed to us with ramifications in algebra, logic (specifically model theory), algebraic-geometry and even analysis! In Chapter 2, we catalogue a representative sample of the most important of these analogies.

In this thesis, we hope to supplement this analogy from a computational standpoint. While the reals have been extensively studied algorithmically, there is vir-
tually no p-adic counterpart to this. We initiate a study of p-adic counterparts to well-known real algorithms, such as for finding roots of polynomial equations, [Usp48,BOFKT88] and for Cylindrical Algebraic Decomposition, [Col75].

1.3.2 The Decision Problem for Fields: The P-adic Case

The decision problem for fields has been a classical concern of mathematicians, especially among logicians and algebraists. More recently, concern for quantitative complexity issues has brought it to the forefront of research in theoretical computer science.

The decision problem for a class of fields consists in trying to decide whether a given first-order sentence in the language of fields (perhaps augmented by a certain additional vocabulary pertinent to the class under consideration) is true. Recall that such a sentence is built up from atomic predicates consisting of the field operations (and certain additional specific operations) by logical boolean connectives (\( \lor, \land, \neg \)) and by quantification (\( \exists, \forall \)), see Chapter 3.

The decision problem over the complexes, \( \mathbb{C} \), is essentially a question about the solvability of a system of polynomial equations in \( \mathbb{C} \), an issue addressed earlier this century in the work of mathematicians like Kronecker, Hermann, Macaulay and others, and constitutes the subject of elimination theory. Recently, quantitative complexity results have been obtained by, inter alia the following works: [Hei83, Gri87b, Jer89]. Essentially, these results show that the decision problem for \( \mathbb{C} \) can be solved in double exponential time.

The decision problem for \( \mathbb{R} \) was first studied in a classical work by Alfred Tarski, [Tar51]. Tarski gave an algorithm, but he paid no heed at all to complexity issues, and in fact was non-elementary. Elementary recursive solutions were subsequently found by Monk and Solovay, but the real breakthrough was the Cylindrical Algebraic Decomposition method of George Collins, [Col75], which gave a double-exponential time algorithm to decide the theory of reals. Subsequently,
the method was refined in several ways, [Arn89]. In a beautiful pioneering paper, Ben-Or, Kozen and Reif [BOKR86] developed an algorithm based on the classical theorem of Sturm, [Usp48], which ran in exponential space or parallel polynomial time. Other algorithms are presented in [Gri87a,Ren89].

Progress in the p-adic case has been much slower. In an award-winning series of papers, James Ax and Simon Kochen, [AK65,AK66], and independently, Ju. L. Ersöv, [Ers65], showed that the first-order theory of p-adic fields was decidable. They used the model-theoretic technique of ultraproducts and so their methods were not effective. Using ingenious but elementary arguments, Paul J. Cohen ⁴ [Coh69] gave the first effective decision procedure for the p-adics. Many of the key ideas in subsequent work including the present one, can be traced back to Cohen's paper ⁵. Subsequently, Weispfenning, [Wei76,Wei83], refined and extended these ideas and results. All this work was done in the setting of valued fields, with the valuation playing the role that order did in the real case.

However, the valued field setting required the use of a somewhat awkward two-sorted formalism (for the field itself and for the value group – see Chapter 2). In 1976, Angus Macintyre, [Mac76] in an insightful paper showed how one could work in a one-sorted formalism (the so-called “Pₙ-formalism”) by bringing the role of the “nth powers” to the forefront. Subsequently, the “nth power” formalism has proved to be a most fruitful one for the development of semi-algebraic geometry over the p-adics, for instance, and to develop the real-p-adic analogy in general, [Mac84, Rob87,SvdD88]. Macintyre's paper also demonstrated quantifier-elimination for the first-order theory of the p-adics in the new formalism. Denef, [Den84] gave a beautiful application of this quantifier elimination to counting p-adic points on varieties and in the process developed a cell decomposition for p-adic affine space.

On of the aims of this thesis is to make these results quantitative.

⁴Of the Set Theory and Continuum Hypothesis Fame!
⁵Which, incidentally, is rather hard reading—his notation is rather idiosyncratic and at many points it is not clear what he is proving!
1.4 Outline of the Thesis

The rest of this thesis is organized as follows. In Chapter 2, we give a quick p-adic primer. A survey of the relevant definitions, constructions and properties of the p-adics encompassing their algebraic, geometric and topological facets is presented. Previously, this material was scattered throughout the (rather large) literature on the p-adics. Here we have attempted to summarize in one place, all the relevant material and make it easily accessible. In particular, we have given a succinct presentation of the structure theory of certain multiplicative subgroups of the p-adics and how they relate to the new $P_\pi$-formalism that we alluded to above. We hope that this survey will provide a convenient reference point for future studies on the p-adics.

In Chapter 4, we describe and analyze a simple algorithm for finding p-adic roots of polynomial equations. This algorithm is a symbolic p-adic version of a combination of the classical Newton and Horner numerical schemes [Usp48], for finding roots of polynomial equations over the reals. In this way, we contribute to the $\mathbb{R} - \mathbb{Q}_p$ analogy from a computational perspective.

In Chapter 3, we describe and analyze decision procedures and quantifier-elimination procedures for the first-order-theory of the p-adics. This is the first quantitative result of its kind in the new $P_\pi$-formalism. The problems for the p-adics are shown to be of the same complexity as the corresponding problems for the reals. However, the techniques used are significantly different\footnote{Indeed in many of the $\mathbb{R} - \mathbb{Q}_p$ analogies, this is the case, [Rob87].}. First we give a decision procedure and a quantifier-elimination procedure for the linear fragment of the theory. We then give algorithms to solve the corresponding problems for the full theory. In each case, the decision procedure takes the form of an alternating Turing machine algorithm running in exponential time and making a linear number of alternations. This can be converted into a deterministic procedure running in exponential space or in double exponential time. The quantifier-elimination proce-
dure, in each case, runs in double exponential time and space. Both these bounds are demonstrated to be essentially optimal by exhibiting matching lower bounds. The main tool we use is a Cell Decomposition Lemma due to Denef [Den86] which we use in a refined quantitative form.

In Chapter 5, we present work of a more speculative nature towards a possible p-adic analogue of the classical Sturm theory for the reals. Elementary evidence is given to show that cosets of $n$-th powers in the multiplicative subgroup display a behavior similar to that shown by signs for the reals.
Chapter 2

A P-adic Primer

Literature on the p-adics is scattered in many different places and their many different facets are never found together. In this chapter, we fill in this need by giving a survey of the p-adics that encompasses the algebraic, topological, logical, and algebro-geometric viewpoints. Hopefully this will serve as a convenient reference point for future studies.

2.1 The Field of p-adic Numbers: Construction and Basic Properties

2.1.1 Valuations and Completions

The concept of a valuation is of central importance in algebra, algebraic geometry and algebraic number theory. In algebraic geometry, valuations provide a clean algebraic way of describing the central notion of a birational isomorphism between varieties [Abh90,OO81]. In algebraic number theory, the completions of valued-fields are the central objects of study of the so-called class-field theory, see the introduction. In this section, we collect together central facts and results about valuations (mostly without proof) for convenient reference. We refer for instance, to [E.67,Has80,End72,CF67,Wei63,Cas86] for the details.
Definition 2.1 A valuation of a field $k$ is a map $\phi : k \to \mathbb{R}$ such that

1. $\phi(x) \geq 0$ for all $x \in k$.
2. $\phi(x) = 0$ iff $x = 0$.
3. (Homomorphy) $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ for all $x, y \in k$.
4. (Triangle Inequality) $\phi(x + y) \leq \phi(x) + \phi(y)$ for all $x, y \in k$.

Example 2.2 Any field $k$ has the trivial valuation, $\tau : k \to \{0, 1\}$. □

Example 2.3 The best known nontrivial valuations are the absolute values, $|\cdot|_\mathbb{R}, |\cdot|_\mathbb{C}$ of $\mathbb{R}, \mathbb{C}$, the field of real and complex numbers respectively. □

Example 2.4 Let $K := k(t)$ where $k$ is any field and $t$ is transcendental over $k$. We first define a valuation $\phi$ on the ring of polynomials, $k[t]$. Let $c > 1$ be fixed and then for

$$f = a_0 + \cdots + a_n \cdot t^n \in k[t], \quad a_n \neq 0$$

define $\phi(f) := c^n$. (By convention, $\phi(0) = 0$.)

For an element $h = \frac{f}{g} \in k(t)$, with $f, g \in k[t], g \neq 0$, set $\phi(h) := \phi(f)/\phi(g)$ to extend $\phi$ to a homomorphism. □

Example 2.5 With $K := k(t)$ as in the last example, let $p(t) \in k[t]$ be irreducible (over $k$) and let $0 < \gamma < 1$ be fixed. Every $h \in k(t)$ can be written in the form

$$h(t) = (p(t))^\rho \cdot \frac{f(t)}{g(t)}$$

where $f, g \in k[t]$ are not divisible by $p$, and $\rho \in \mathbb{Z}$ depends only on $h$ and $p$. Set $\phi_p(h) := \gamma^\rho$ (and by convention, $\phi_p(0) = 0$). □

The next proposition lists some elementary facts about valuations.

Proposition 2.6 Let $\phi$ be a valuation of a field $k$. Then:
1. If \( z \in k \) is a root of unity, then \( \phi(z) = 1 \). In particular, \( \phi(1) = \phi(-1) = 1 \).

2. \( \phi(x - y) \leq \phi(x) + \phi(y) \) for all \( x, y \in k \).

3. \( \phi(x \cdot y^{-1}) = \phi(x) \cdot (\phi(y))^{-1} \) for all \( x, y \in k, y \neq 0 \).

4. \( |\phi(x) - \phi(y)| \leq \phi(x - y) \) for all \( x, y \in k \).

5. If \( k \) is finite, then \( \phi \) is trivial.

Let \( \phi \) be a valuation of a field \( k \). The map \( d_\phi : k \times k \to \mathbb{R} \), defined by

\[
d_\phi(x, y) = \phi(x - y) \quad \text{for all } x, y \in k
\]

is a metric on \( k \). Let \( T_\phi \) denote the metric topology induced by \( d_\phi \) on \( k \).

We have the following fundamental topological facts:

**Proposition 2.7**

1. \( T_\phi \) satisfies the \( T_2 \) or Hausdorff axiom.

2. For any \( x \in k \), the sets \( V_\epsilon(x) = \{ y \in k : d_\phi(x, y) < \epsilon \}, (\epsilon > 0) \) constitute a basis of open neighborhoods of \( x \).

3. \( T_\phi \) is discrete iff \( \phi \) is trivial.

4. The map \( \phi : k \to \mathbb{R} \) is uniformly continuous, with respect to the metric topologies induced on \( k \) and \( \mathbb{R} \) by \( d_\phi \) and \( |\cdot| \) (the usual absolute value) respectively.

5. The field \( k \) with the topology \( T_\phi \) is a **topological field** \(^1\).

Two valuations \( \phi, \psi \) are equivalent iff \( \phi = \psi^\rho \) for some real number \( \rho > 0 \).

The trivial valuation is equivalent only to itself. For non-trivial valuations, the following proposition gives alternate characterizations:

**Proposition 2.8** Let \( \phi, \psi \) be valuations of a field \( k \). The following are equivalent:

1. \( \phi \) is equivalent to \( \psi \).

\(^1\)That is, all field operations are continuous with respect to the topology.
2. \( T_\phi = T_\psi. \)

3. \( T_\phi \) is stronger than \( T_\psi. \)

4. For all \( x \in k, \phi(x) < 1 \rightarrow \psi(x) < 1. \)

5. For all \( x \in k, \phi(x) \leq 1 \iff \psi(x) \leq 1. \)

The valuations in Examples 2.4 and 2.5 belong to a special class of valuations in which we are particularly interested:

**Definition 2.9** A valuation \( \phi : k \to \mathbb{R} \) is non-archimedean if

\[
\phi(x + y) \leq \max(\phi(x), \phi(y)) \quad \text{for all } x, y \in k.
\]

That is, \( \phi \) satisfies not merely the triangle inequality, but the stronger, so called, ultrametric inequality. A valuation which is not non-archimedean is said to be archimedean (what else ?!). The adjective also applies to the induced metrics. \( \square \)

Here are some equivalent characterizations of non-archimedean valuations:

**Proposition 2.10** Let \( \phi : k \to \mathbb{R} \) satisfy all the conditions on a valuation except the triangle inequality. Then the following are equivalent:

1. \( \phi \) is a non-archimedean valuation.

2. \( \phi \) satisfies the triangle inequality and \( \{\phi(m \cdot 1) : m \in \mathbb{N}\} \) is bounded.

3. For all \( m \in \mathbb{N}, \phi(m \cdot 1) \leq 1. \)

4. For all \( x \in k, \phi(x) \leq 1 \rightarrow \phi(x + 1) \leq 1. \)

5. For all \( \rho > 1, \phi^\rho \) is a valuation of \( k. \)

In view of the great importance of the following corollary, we provide the (rather simple) proof as well:

**Corollary 2.11** If \( \phi \) is a non-archimedean valuation of \( k, \) then for all \( x, y \in k, \)

\[
\phi(x) \neq \phi(y) \rightarrow \phi(x + y) = \max(\phi(x), \phi(y)).
\]
Proof. Suppose $\phi(x) < \phi(y)$. Then,

$$
\begin{align*}
\phi(y) &= \phi((x + y) - x) \\
&\leq \max(\phi(x + y), \phi(x)) \text{ by the ultrametric inequality} \\
&= \phi(x + y) \quad \text{since } \phi(x) < \phi(y)
\end{align*}
$$

Also $\phi(x + y) \leq \max(\phi(x), \phi(y))$ by the ultrametric inequality. Hence $\phi(x + y) = \phi(y)$. \qed

This corollary has an interesting geometric interpretation: Any triangle is isosceles (with respect to the $d_\phi$ metric)! Or, any point in a disc is a center of the disc (again in the $d_\phi$ metric)!

More generally, an easy induction shows that

**Proposition 2.12** If $\phi(x_k) > \phi(x_i)$ for some $k$ and all $i$, $1 \leq i, k \leq n$, then $\phi(\sum_{1 \leq i \leq n} x_i) = \phi(x_k)$.

Sometimes this is phrased in the contrapositive:

**Proposition 2.13** If $\sum_{1 \leq i \leq n} x_i = 0$, then $\phi(x_j) = \phi(x_k)$ for some $1 \leq j, k \leq n$.

It is sometimes more convenient to write non-archimedean valuations additively.

**Definition 2.14** An exponential valuation $v$ of $k$ is a map $v : k \to \mathbb{R} \cup \{\infty\}$ such that:

1. $v(x) = \infty$ iff $x = 0$.
2. $v(x \cdot y) = v(x) + v(y)$.
3. $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in k$.

\qed
The next proposition shows how this is related to our original definition of a valuation:

**Proposition 2.15** There is a one-to-one correspondence between the non-archimedean valuations \( \phi \) of \( k \) and exponential valuations \( v \) of \( k \) given by:

\[
v \mapsto \phi = e^{-v}, \quad \phi \mapsto v = -\log \phi
\]

(with the convention \( e^{-\infty} = 0, -\log 0 = \infty \)).

In terms of an exponential valuation (which we will frequently use), the ultrametric inequality and the corollary above read:

**Proposition 2.16**

1. **(Ultrametric Inequality)** \( v(x + y) \geq \min(v(x), v(y)) \) for all \( x, y \).

2. **(Ultrametric Equality)** If \( v(x_k) < v(x_i) \) for some \( k \) and all \( i \), \( 1 \leq i, k \leq n \), then \( v(\sum_{1 \leq i \leq n} x_i) = v(x_k) \).

Let \( \phi \) be a non-trivial valuation of \( k \). A sequence \( (x_i)_{i \in \mathbb{N}} \) of elements of \( k \) is \( \phi \)-convergent to \( x \in k \) if it converges to \( x \) in the metric topology \( T_\phi \). We write \( \lim_\phi (x_i) = x \). This occurs iff \( (\phi(x_i - x))_{i \in \mathbb{N}} \) converges to 0 in \( \mathbb{R} \) (with the usual topology). That is, \((\phi(x_i))\) is also convergent, and \( \lim(\phi(x_i)) = \phi(\lim_\phi (x_i)) \).

A sequence \( (x_i) \) is \( \phi \)-Cauchy if it is a Cauchy-sequence in the metric topology induced by \( d_\phi \). That is, for every \( \epsilon > 0 \), there is a \( n_0 \in \mathbb{N} \) such that \( d_\phi(x_n, x_m) = \phi(x_n - x_m) < \epsilon \) for all \( n, m \geq n_0 \).

Clearly any convergent sequence is \( \phi \)-Cauchy. If every \( \phi \)-Cauchy sequence is convergent, then \( k \) is said to be complete.

We shall now briefly sketch Cauchy’s method of completing a field with respect to a valuation, that is, of obtaining an extension field which is complete with respect to an extended valuation.

Abbreviate \((x_i), (y_i)\) etc. by \( X, Y \) etc. Then:
**Proposition 2.17** Let $\phi$ be a valuation of $k$. Then:

1. The set of all $\phi$-Cauchy sequences $(x_i)$ of elements of $k$ form a ring $C$ (with respect to component-wise addition and multiplication).

2. The set of all $\phi$-null sequences (that is, sequences that are $\phi$-convergent to 0) form a maximal ideal $I$ of $C$.

3. The map $\Phi : C \to R$ given by $\Phi(X) = \lim(\phi(x_i))$ is well-defined and has the following properties:

$$\Phi(X + Y) \leq \Phi(X) + \Phi(Y), \Phi(X \cdot Y) = \Phi(X) \cdot \Phi(Y), \Phi(X) = 0 \iff X \in I.$$ 

We introduce a few notations. By a valued field, we shall mean a pair $(k, \phi)$ where $k$ is a field and $\phi$ is a valuation on $k$. Write $(k, \phi) \subseteq (\tilde{k}, \tilde{\phi})$ if $k$ is a sub-field of $\tilde{k}$ and $\phi = \tilde{\phi}|k$. More generally, a monomorphism $\lambda$ from $k$ into a field $\tilde{k}$ is an embedding of $(k, \phi)$ into $(\tilde{k}, \tilde{\phi})$ if $\tilde{\phi} \circ \lambda = \phi$. In this case we write $\lambda : (k, \phi) \to (\tilde{k}, \tilde{\phi})$.

Clearly, $\lambda$ is a continuous map when $k, \tilde{k}$ are endowed with $T_{\phi}, T_{\tilde{\phi}}$ respectively. A bijective embedding is an isomorphism; its inverse is also an embedding.

A valued field $(k, \phi)$ is complete if $k$ is $\phi$-complete. A completion of a valued field $(k, \phi)$ is a complete valued field, $(\tilde{k}, \tilde{\phi}) \supseteq (k, \phi)$ such that $k$ is dense in $\tilde{k}$ with respect to $T_{\tilde{\phi}}$. More generally, a completion of $(k, \phi)$ is an embedding $\lambda : (k, \phi) \to (\tilde{k}, \tilde{\phi})$ such that $(\tilde{k}, \tilde{\phi})$ is complete and $\lambda(k)$ is dense in $\tilde{k}$. In this case there is an isomorphism $\vartheta : (\tilde{k}, \tilde{\phi}) \to (\tilde{k}, \tilde{\phi})$ such that $(\tilde{k}, \tilde{\phi})$ is a completion of $(k, \phi)$ in the usual sense.

Cauchy’s method to produce completions is reflected in the following

**Proposition 2.18** Let $(k, \phi)$ be a valued field and let $C$, $I$ and $\Phi$ be as defined above. Then $\Phi$ induces a valuation $\tilde{\phi}$ of the field $\tilde{k} = C/I$ and $\mu : (k, \phi) \to (\tilde{k}, \tilde{\phi})$ is a completion where $\mu(x) = (x_i = x) + I$ for all $x \in k$.

We give two important examples of this completion process in the next subsection. We first list a few general properties of completions. The first is a universal mapping property:
Proposition 2.19 Let μ : (k, φ) → (k̂, φ̂) be a completion\(^2\) and λ : (k, φ) → (k̂, φ̂) an embedding into a complete valued field, (k̂, φ̂). Then, there is a unique embedding ̂λ : (k̂, φ̂) → (k̂, φ̂) such that λ = ̂λ ◦ μ.

This yields the

Corollary 2.20 Let μ\(_i\) : (k, φ) → (k\(_i\), φ\(_i\)) be completions, i = 1, 2. Then there is a unique embedding λ : (k\(_1\), φ\(_1\)) → (k\(_2\), φ\(_2\)) such that μ\(_2\) = λ ◦ μ\(_1\) and this is an isomorphism.

The next proposition concerns extensions of valuations to field extensions:

Proposition 2.21 Let (k, φ) be complete and let k̂ be a finite extension of k. Then there is at most one valuation ̂φ of k̂ which extends φ and such that (k̂, ̂φ) is complete.

Given a valued field (k, φ), denote by φ(k), the image of k in R under the valuation φ; this is called the value group. The following is an important property of the value-groups of fields with non-archimedean valuations.

Proposition 2.22 If (k̂, ̂φ) is a completion of (k, φ), and if φ is non-archimedean, then φ(k) = ̂φ(k̂).

2.1.2 The p-adic Numbers: Definition and Basic Properties

Cauchy first applied his construction to produce the field R of real numbers as the completion of the field Q of rationals under the usual absolute value valuation. However the absolute value is not the only non-trivial valuation on Q.

For every prime p, the field Q admits the p-adic valuation, φ\(_p\), obtained by setting φ\(_p\)(p) = \(p^{-1}\) and for every prime \(q \neq p\), φ\(_p\)(q) = 1 and extending φ\(_p\) to all of Q by the homomorphism condition. That is, write α ∈ Q as α = \(p^n \cdot (r/s)\) where

\(^2\)Not necessarily the completion provided by the previous proposition
\( p \nmid r, s \) and set \( \phi_p(\alpha) = p^{-n} \). We use the notation \( \phi_\infty \) to denote the usual absolute value. This gives the elegant formula

\[
\prod_p \phi_p(x) = 1 \quad \text{for all } x \in \mathbb{Q}
\]

where the product runs over all prime \( p \) and \( \infty \). (Some authors define \( \phi_p(p) = c \) for some fixed \( c < 1 \), but this entails losing the above formula, for instance.)

The following is a famous theorem that specifies all the valuations on \( \mathbb{Q} \):

**Proposition 2.23 (Ostrowski)** Any non-trivial valuation of \( \mathbb{Q} \) is equivalent to \( \phi_p \) for exactly one \( p \), \( p \) a prime, or \( \infty \).

**Definition 2.24** The field of \( p \)-adic numbers, \((\mathbb{Q}_p, \hat{\phi}_p)\) is the completion of \((\mathbb{Q}, \phi_p)\).

It is instructive to see what the abstract completion process described above amounts to in this specific situation. A \( p \)-adic number \( a \) is represented by the equivalence class of a \( \phi_p \)-Cauchy sequence of rationals, \( \{a_i\} \) where two \( \phi_p \)-Cauchy sequences, \( \{b_i\}, \{c_i\} \) are equivalent iff the sequence \( \{b_i - c_i\} \) is a \( \phi_p \)-null sequence, that is, iff \( \lim \phi_p(b_i - c_i) = 0 \). Moreover, if the sequence \( \{a_i\} \) is \( \phi_p \)-Cauchy, then \( \{\phi_p(a_i)\} \) is a Cauchy sequence of real numbers and has a limit, \( c \). Then the extended valuation \( \hat{\phi}_p \) satisfies \( \hat{\phi}_p(a) = c \). Also, the ultrametric inequality implies that the sequence \( \phi_p(a_i) \) is eventually constant and takes the value \( c \).

Sequences of \( p \)-adic numbers do not show the subtleties of behavior that sequences of reals do:

**Proposition 2.25** 1. For a sequence of \( p \)-adic numbers, \( \{a_n\} \) to be convergent, it is necessary and sufficient that

\[
\lim_n (a_n - a_{n+1}) = 0.
\]

2. For a series \( \sum_{n \geq 1} a_n \) of \( p \)-adics to be convergent, it is necessary and sufficient that

\[
\lim_n a_n = 0.
\]
As a consequence, we get a nice representation of p-adics which resembles the usual decimal representation of reals and is the source of formal similarities to \textit{Laurent} series:

\textbf{Proposition 2.26} Every non-zero p-adic $a$, can be expressed uniquely in the form

$$\sum_{n \geq N} a_n p^n$$

where $0 \leq a_n < p$ are integers and $a_N \neq 0$. The integer $N$ is determined by the condition $\hat{\phi}_p(a) = p^{-N}$.

\textbf{Example 2.27} [P-adic Arithmetic] Arithmetic in the p-adics is carried out as one would expect, digit-by-digit with carries, see [Kob84, Mah81]. A curiosity is that $-1$ has the p-adic expansion:

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

consisting of an infinite sequence of the digit $p-1$. This is easy to see by noting that one indeed obtains 0 on addition with 1. \(\square\)

\subsection*{2.1.3 Further Properties of the p-adics}

In this sub-section, we collect together some useful facts about the structure of the field $\mathbb{Q}_p$.

\textbf{Algebra of the p-adics}

Recall that to every valuation corresponds an exponential valuation. For the p-adic valuation, $\phi_p$, there corresponds the exponential valuation $v_p$ such that $\phi_p(x) = p^{-n}$ iff $v_p(x) = n$.

Define $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : \hat{\phi}_p(a) \geq 0\}$; this is the ring of $p$-adic integers.

\textbf{Proposition 2.28} The ring $\mathbb{Z}_p$ is the closure of the ring $\mathbb{Z}$ of integers in the field $\mathbb{Q}_p$. $\mathbb{Z}_p$ is a principal ideal ring, a Dedekind domain and a ring with unique factorization.
The following proposition describes the multiplicative structure of the ring $\mathbb{Z}_p$:

**Proposition 2.29**  
1. The set $U_p = \{ a \in \mathbb{Q}_p : v_p(a) = 1 \}$ is the set of all invertible elements of $\mathbb{Z}_p$.  
2. The set $\mathcal{P} = \{ a \in \mathbb{Q}_p : v_p(a) > 0 \}$ is the unique maximal ideal in $\mathbb{Z}_p$. Every non-zero ideal of this ring is of the form $\mathfrak{l} = p^n\mathbb{Z}_p = \mathcal{P}^n$ for some $n \geq 0$. Here, $\mathcal{P}^0 = \mathbb{Z}_p$ and $\mathcal{P}^n = \{ a \in \mathbb{Q}_p : v_p(a) \geq n \}$.  
3. The canonical embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induces an isomorphism of $\mathbb{Z}/p^n\mathbb{Z}$ onto $\mathbb{Z}_p/\mathcal{P}^n$.

The last statement leads to yet another illuminating characterization of the p-adics:

**Proposition 2.30**  
1.  
   
   $$\mathbb{Z}_p = \lim_{\rightarrow} \mathbb{Z}/p^n\mathbb{Z}$$

2. There are canonical projection homomorphisms, $\text{res}_k : \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}, k \geq 1$.  
3. $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$.

The key technical tool for handling the p-adics is the following algebraic-topological criterion for roots of polynomials in $\mathbb{Z}_p[x]$. It relates roots in the finite residue rings to roots in the inverse limit.

**Lemma 2.31 (Hensel’s Lemma)**  
1. Let $f \in \mathbb{Z}[x]$ and let $a_0$ be a root of $f$ in $\mathbb{Z}/p\mathbb{Z}$. If $f'(a_0) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, then $a_0$ can be lifted to a unique root $\xi \in \mathbb{Z}_p$ of $f$ such that $\text{res}_1(\xi) = a_0$.
2. More generally, if $\alpha$ is a root of $f$ in a finite ring $\mathbb{Z}/p^n\mathbb{Z}$ and if $n > 2r$ where $r = v(f'(\alpha))$, then $\alpha$ can be lifted to a unique root $\xi \in \mathbb{Z}_p$ of $f$ such that $\text{res}_{n-r}(\xi) = \text{res}_{n-r}(\alpha)$.

An algorithmic proof of this lemma may be found in Chapter 4.

The last fact we record is about how the p-adic completions for different primes relate to each other as rings:
Proposition 2.32 $\mathbb{Q}_p, \mathbb{Q}_q$ for $p \neq q$ are not isomorphic as rings.

Topology of the $p$-adics

We noted earlier that any completion has an induced topology from the valuation metric and hence is Hausdorff.

Let

$$V_\epsilon(x) = \{ y \in \mathbb{Q}_p : \hat{\phi}_p(y - x) \leq \epsilon \}$$

and

$$V'_\epsilon(x) = \{ y \in \mathbb{Q}_p : \hat{\phi}_p(y - x) < \epsilon \}.$$

Then:

Proposition 2.33 $V_\epsilon(x), V'_\epsilon(x)$ are clopen neighborhoods of $x$.

Furthermore:

Proposition 2.34 1. The topological field $\mathbb{Q}_p$ is totally disconnected.

2. The topological field $\mathbb{Q}_p$ is separable.

3. The topological field $\mathbb{Q}_p$ is locally compact.

How do the topological fields $\mathbb{Q}_p, \mathbb{Q}_q$ compare for $p \neq q$?

Proposition 2.35 The topological fields $\mathbb{Q}_p, \mathbb{Q}_q$ for $p \neq q$ are homeomorphic.

The next proposition describes the topological properties of important functions on the $p$-adics:

Proposition 2.36 1. Let $\mathbb{R}_{disc}$ be the reals endowed with the discrete topology.

Then the restriction of $\hat{\phi}_p$ to $k \setminus \{0\}$ is continuous.

2. Let $f(x_1, \cdots, x_n) \in \mathbb{Q}_p[x_1, \cdots, x_n]$. Then, regarded as a function, $f : \mathbb{Q}_p^n \to \mathbb{Q}_p$, $f$ is continuous.
Finally we give the topological properties of the ideals described in the previous sub-section:

**Proposition 2.37**  1. The ideals $P^n$ are compact and open sets in $Q_p$.

2. The ideal $P^n$ is the closure of $p^n\mathbb{Z}$.

3. If $a \in Q_p$, then the family $\{a + P^n\}$ is a basis of neighborhoods of $a$.

### 2.2 The $P_n$-formalism

#### 2.2.1 Motivation

We would like to develop the theory in an analogous manner to the reals. However, at first glance, there is no immediate counterpart in the p-adics, to the order structure in the reals. Traditionally, people have attempted to use the valuation structure to get such a counterpart: the relation $x \geq 0$ in the reals was sought to be replaced by $v(x) \geq 0$ in the p-adics. There are many reasons why this is not satisfactory, for instance while in the reals the group of signs is finite of order 3, the value group in the p-adics is infinite (isomorphic to $\mathbb{Z}$).

A more natural replacement for the order relation comes from Artin's theory of real-closed fields developed in order to solve *Hilbert's 17th Problem*, [Kap77]. This asks whether a polynomial $f \in R[x_1, \ldots, x_n]$ which is positive definite \(^3\) can be represented as the sum of squares of rational functions over the reals, that is, as the sum of squares of elements in $R(x_1, \ldots, x_n)$. In his celebrated affirmative solution, [Lam84], Artin brought to the forefront, the crucial role of the subgroup, $R^*(2)$ of the multiplicative group, $R^*$, consisting of those elements that are squares. Seen in this way, the signs of real numbers have the following interpretation independent of the order structure: $[R^* : R^*(2)] = 2$, we have coset representatives $+1, -1$ and the natural homomorphism $sgn : R^* \rightarrow R^*/R^*(2)$ giving the coset representative is the familiar and all-important sign homomorphism.

\(^3\)That is, $f(a_1, \ldots, a_n) \geq 0$ for all $(a_1, \ldots, a_n) \in R^n$
There is a certain technical complication in carrying this over to the p-adic case. It turns out that the p-adic closure (see § 2.3.1) of a p-valued field is not unique. Every p-adic closure of a p-valued field, $k$, is, however, obtained by adjoining radicals, i.e. roots of binomials of the form $x^n - a$, $a \in k$. Consequently, two p-adic closures, $\hat{k}_1, \hat{k}_2$ are isomorphic precisely when

$$\hat{k}_1^{(n)} \cap k = \hat{k}_2^{(n)} \cap k$$

for each $n \geq 2$, where $\hat{k}_i^{(n)}$ denotes the set of $n$-th powers of elements in $\hat{k}_i$. It is for this reason that one has to consider all $n$-th powers, not only squares, for the p-adics.

### 2.2.2 Structure of $\mathbb{Q}_p^*$

In this subsection, we will describe the structure of the multiplicative group $\mathbb{Q}_p^*$ and of the subgroups $\mathbb{Q}_p^{*(n)}$ for all $n \geq 2$, [Ser73,Has80,Coh89].

Let $U := \mathbb{Z}_p^*$ be the group of p-adic units. For every $n \geq 1$, put $U_n := 1 + p^n \mathbb{Z}_p$; this is the kernel of the homomorphism $\epsilon_n : U \to (\mathbb{Z} / p^n \mathbb{Z})^*$ obtained in the obvious way. The $U_n, n \geq 1$ form a descending sequence of open subgroups of $U$, and $U = \lim_\to U / U_n$. $U_1$ is called the group of 1-units ("Einseinheiten"). Since any unit $u \in U$ can be written as $u = a_0 + a_1 p + \cdots$ with $1 \leq a_0 < p$, it is clear that

$$U \cong \mathbb{F}_p \times U_1$$

Now any $x \in \mathbb{Q}_p^*$ may be written as $x = p^n \cdot u$ for some $n \in \mathbb{Z}$, and $u$ a unit, so $\mathbb{Q}_p^* \cong \mathbb{Z} \times U$ (where the first factor refers to the additive group of integers). Hence we obtain the following structure theorem:

**Theorem 2.38**

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{F}_p^* \times U_1.$$ 

One can get a more perspicuous description via the following
Lemma 2.39

\[ U_1 \cong \mathbb{Z}_p. \]

\textit{Proof.} The map

\[ Z_p \to U_1 \]

\[ x \mapsto (1 + p)^x \]

is clearly an injective homomorphism from the additive group \( Z_p \) to the multiplicative group \( U_1 \). In [Ser73, Coh89], it is shown that in fact this is also surjective for \( p > 2 \). \( \square \)

Combining the previous two results, we get the structure theorem:

Theorem 2.40

\[ Q_p^* \cong \mathbb{Z} \times F_p^* \times Z_p. \]

This structure theorem easily enables us to determine the structure of the subgroup of nth powers. Clearly,

Proposition 2.41

\[ Q_p^{*(n)} \cong n\mathbb{Z} \times F_p^{*(n)} \times n\mathbb{Z}_p. \]

To get a more explicit description of the quotient group than this proposition would yield, we need a few lemmas.

Lemma 2.42

\[ n\mathbb{Z}_p \cong U_{v(n)+1}. \]

\textit{Proof.} The image of \( n\mathbb{Z}_p \) under the map

\[ Z_p \to U_1 \]

\[ x \mapsto (1 + p)^x \]

is easily verified to be \( U_{v(n)+1}. \) \( \square \)

\(^4\)For \( p = 2, U_1 \approx \{ \pm 1 \} \times U_2 \) and \( U_2 \approx \mathbb{Z}_2. \)
Lemma 2.43 For $k \geq 1$,

$$U_1/U_k \cong (1 + p\mathbb{Z}/p^{k-1}\mathbb{Z}).$$

Proof. The homomorphism

$$U_1 \rightarrow \mathbb{Z}/p^k\mathbb{Z}$$

$$x \mapsto (1 + px) \pmod{p^k}$$

has kernel $U_k$ and image $(1 + p\mathbb{Z}/p^{k-1}\mathbb{Z})$. □

Combining the previous three propositions, we obtain

Proposition 2.44

$$Q_p^{*\langle n \rangle} \cong n\mathbb{Z} \times F_p^{*\langle n \rangle} \times U_{v(n)+1}.$$  

Proposition 2.45

$$Q_p^{*}/Q_p^{*\langle n \rangle} \cong \mathbb{Z}/n\mathbb{Z} \times F_p^{*}/F_p^{*\langle n \rangle} \times 1 + p\mathbb{Z}/p^{v(n)}\mathbb{Z}.$$  

By a simple computation, see [HK86,IR90], $|F_p^{n}| = \frac{p-1}{\gcd(n,p-1)}$, so we deduce:

Corollary 2.46 For any $n \geq 2$,

$$[Q_p^{*}:Q_p^{*\langle n \rangle}] = n \cdot \gcd(n,p-1) \cdot p^{v(n)}.$$  

The next proposition gives a canonical set of coset representatives for $Q_p^{*}$ in $Q_p^{*\langle n \rangle}$.

If $n = md$ for integers $n, m, d$, then of course $Q_p^{*\langle n \rangle} \subseteq Q_p^{*\langle m \rangle}$, and from the above characterization,

Proposition 2.47

$$Q_p^{*\langle m \rangle}/Q_p^{*\langle n \rangle} \cong \mathbb{Z}/d\mathbb{Z} \times F_p^{*}/F_p^{*\langle d \rangle}.$$  

We will denote the canonical projection homomorphism by $\rho_n : Q_p^{*} \rightarrow Q_p^{*\langle n \rangle}.$
2.2.3 Valuation and $n$-th powers

Macintyre, [Mac76], first suggested that the $p$-adics be studied in the “$P_n$-formalism” to pursue the analogy to the reals, with the coset representatives taking the place of sign conditions. In this formalism, there are unary predicates, $P_n$ for each $n \geq 2$ standing for the $n$-th powers, so

$$P_n(x) \leftrightarrow \exists y(y^n = x)$$

(Here $x$ and $y$ refer to field elements.) In Section 2.3, we will give a sampler of how some natural analogies obtain between the reals and the $p$-adics in this formalism.

In the meanwhile, we will relate it to the more conventional valuation formalism. In fact, the valuation is definable in terms of the $n$-th power predicates.

**Proposition 2.48** 1. If $p \neq 2$, then for any $a, b \in k$,

$$v(a) \leq v(b) \iff P_2(a^2 + p \cdot b^2)$$

2. If $p = 2$, then for any $a, b \in k$,

$$v(a) \leq v(b) \iff P_3(a^3 + p \cdot b^3)$$

*Proof.* We will sketch the proof for $p \neq 2$. If $P_2(a^2 + p \cdot b^2)$ then there exists a $y \in k$ such that

$$y^2 = a^2 + p \cdot b^2$$

Now,

$$2v(y) = v(a^2 + p \cdot b^2) \geq \min(2v(a), 2v(b) + 1) \quad \text{by the ultrametric inequality}$$

$$= 2v(a) \quad \text{by parity}$$

Hence, $v(a) \leq v(b)$. 
Conversely, suppose \( v(a) \leq v(b) \), and consider the equation (in \( y \)):

\[
f(y) := y^2 - (a^2 + p \cdot b^2)
\]

Now \( v(f(a)) = 2v(b) + 1 > 2v(a) = 2v(f'(a)) \), (in the last step, we need \( p > 2 \)). Hence by the Hensel lemma, there is a root of the polynomial, and so \( P_2(a^2 + p \cdot b^2) \).

Conversely, the \( P_n \) predicates define clopen sets in the valuation topology. First we need a key lemma apparently due to Robinson, [Rob87]:

**Lemma 2.49** If \( v(y - x) > 2(v(x) + v(n)) \) for \( x, y \in k \), then \( \rho_n(x) = \rho_n(y) \).

**Proof.** Let \( x = \rho_n(x) \cdot z_1^n \). Now apply Hensel's lemma to the polynomial \( f(z) := \rho_n(x) \cdot z^n - y \). We have \( f'(z) = n \cdot \rho_n(x) z^{n-1} \). So

\[
v(f(z_1)) = v(x - y) \\
> 2(v(x) + v(n)) \\
> 2((n - 1) \cdot v(z_1) + v(n)) \\
= 2 \cdot f'(z_1)
\]

(Note that we can assume \( v(z_1) \geq 0 \), else apply the argument to \( \frac{1}{x}, \frac{1}{y} \)). Hence there exists a \( z_2 \in k \) such that \( y = \rho_n(x) \cdot z_2^n \), that is, \( \rho_n(x) = \rho_n(y) \). \( \Box \)

**Corollary 2.50** There is a function \( \lambda(n) \), such that if \( v(x) > \lambda(n) \), then \( P_n(1+x) \).

**Proof.** Apply the lemma to 1 and note that \( v(1) = 0 \). We can take \( \lambda(n) := 2 \cdot v(n) \). \( \Box \)

This corollary actually enables one to weaken somewhat the assumptions of the original lemma and should be compared with the Ultrametric equality, Proposition 2.16.

**Proposition 2.51** 1. If \( v(y - x) > v(x) + \lambda(n) \), then \( \rho_n(x) = \rho_n(y) \).
2. If \( v(x_k) + \lambda(n) < v(x_i) \) for some \( k \) and all \( i \neq k, 1 \leq i, k \leq m \), then

\[
\rho_n \left( \sum_{1 \leq i \leq m} x_i \right) = \rho(x_k)
\]

*Proof.* Observe that

\[
y = x + (y - x) = x \left(1 + \frac{y - x}{x} \right)
\]

So by the corollary above, if \( v(y - x) > v(x) + \lambda(n) \), then \( \rho_n(1 + \frac{y - x}{x}) = 1 \) and hence \( \rho_n(x) = \rho_n(y) \).

The second part now follows easily taking \( y := \sum_{1 \leq i \leq m} x_i \) and \( x := x_k \). \( \square \)

Finally we can show that the \( P_n \) sets are clopen:

**Proposition 2.52** For each \( n \geq 2 \), the sets

\[
\{ x \in k^* : P_n(x) \}
\]

are closed and open in the valuation topology.

*Proof.* The open covering is obtained by taking the open sets \( \{ y : v(y - x) > v(x) + \lambda(n) \} \) for each \( x \in \{ x \in k^* : P_n(x) \} \). The complement is obtained by taking the union of the sets \( \{ x \in k^* : P_n(\rho \cdot x) \} \) for \( \rho \) running over all the coset representatives other than 1. \( \square \)

Another useful property of the \( P_n \) predicate is its ability to define equalities.

**Proposition 2.53** Let \( a \in k \). Then

\[
a = 0 \leftrightarrow P_2(p \cdot a^2)
\]

*Proof.* Clearly if \( a = 0 \) then \( P_2(p \cdot a^2) \). Conversely, suppose \( a \neq 0 \), and then \( v(a) < \infty \). But then if there exists a \( y \in k \) with \( y^2 = p \cdot a^2 \), we have \( y \neq 0 \) and the computation \( 2v(y) = 2v(a) + 1 \) results in a contradiction. \( \square \)
2.3 The $\mathbb{R}$-$\mathbb{Q}_p$ Analogy

2.3.1 Algebra

The Artin-Schreier theory of real-closed-fields, [Jac85,Coh89], gave the first purely algebraic account of the theory of reals. There is a corresponding Prestel-Rocquette theory of p-adically closed fields, [PP84]. In this subsection, we outline the main correspondences.

A field is said to be real if $-1$ cannot be expressed as the sum of squares \(^5\). The Artin-Schreier theory shows that an field is real iff there is an ordering on it. A maximal algebraic extension, $L$, of a real field, $K$, which is also real is called the real-closure of $K$. A real field which is its own real-closure is called real-closed.

In [Rob87,Bel88], an analogous notion of a p-adic field is defined by giving an explicit axiomatization. Then one defines the p-adic closure of a p-adic field $K$ to be a maximal algebraic extension which is also p-adic. A p-adic field which is its own p-adic closure is called p-adically closed.

There is in fact an intrinsic characterization of real-closed and p-adically closed fields given by certain canonical completeness schemas.

**Proposition 2.54** 1. A real field is real-closed iff (a) every odd degree polynomial over the field has a root in the field and (b) every element or its negative is a square in the field.

2. A p-adic field is p-adically closed iff (a) Hensel’s lemma holds, (see § 2.1.1) and (b) for each $n \geq 2$, there exist a set of integers, $b_1, \ldots, b_{k(n)}$ such that for each $x$ in the field, $P_n(b_i \cdot x)$ for some $i$.

Sometimes, the p-adic counterpart is stated in the form: A field is p-adically closed if it is henselian and has value group elementarily equivalent to $\mathbb{Z}$ (such a group is called a integers-group). (The last stated property in the proposition is in fact simply a reflection of this fact about the value group.)

\(^5\)Equivalently, iff 0 cannot be so expressed.
Proposition 2.55 1. (Artin-Schreier) Every real field has a real-closure which is unique up to isomorphism.

2. (Prestel-Rocquette, Robinson, Belair) Every p-adic field has a p-adic closure which is unique up to isomorphism.

By the Artin-Schreier theory, we know that a positive definite rational function \( f \in \mathbb{R}(x_1, \cdots, x_n) \)\(^6\) can be represented as a sum of squares of rational functions, \( g_1^2 + \cdots + g_k^2, k \geq 1 \), where \( g_1, \cdots, g_k \in \mathbb{R}(x_1, \cdots, x_n) \).

In the p-adic case, a rational function \( f \in \mathbb{Q}_p(x_1, \cdots, x_n) \) is said to be \( p \)-integral definite — if \( f(a_1, \cdots, a_n) \in \mathbb{Z}_p \) for all \( a_1, \cdots, a_n \in \mathbb{Q}_p \) provided \( f(a_1, \cdots, a_n) \) is defined (i.e. its denominator does not vanish)\(^7\). To get the analogous characterization of \( p \)-integral functions, Kochen replaced the square operator by

\[
\gamma_p(x) := \frac{1}{p} \left( \kappa(x) - \frac{1}{\kappa(x)} \right)^{-1}
\]

with \( \kappa(x) := x^p - x \), the Artin-Schreier operator. Now we have the following analogue to Hilbert’s 17th Problem in the p-adics (we suppress the subscript on the Kochen operator):

Proposition 2.56 (Kochen, [Koc67]) A rational function \( f \in \mathbb{Q}_p(x_1, \cdots, x_n) \) is \( p \)-integral definite iff

\[
f = \frac{\Psi(\gamma(g_1), \cdots, \gamma(g_k))}{1 + p\Phi(\gamma(g_1), \cdots, \gamma(g_k))}
\]

where \( \Phi, \Psi \in \mathbb{Z}[y_1, \cdots, y_k], k \geq 1 \) and \( g_1, \cdots, g_k \in \mathbb{Q}_p(x_1, \cdots, x_n) \).

\(^6\)One may replace \( \mathbb{R} \) by any real-closed field.

\(^7\)Equivalently, iff \( v(f(a_1, \cdots, a_n)) \geq 0 \), so the analogy to order is clear.
2.3.2 Model Theory

The model-theory of real-closed and p-adically-closed fields shows remarkable similarities.

The reals are usually viewed as the structure \((R, +, *, 0, 1, <)\) and as such are studied in the language of ordered fields, i.e. in the language of field theory augmented with a relation for order. Traditionally, the p-adics have been viewed as valued fields, and as such studied in a 2-sorted language for valued fields. Specifically, there are two sorts, one for the field elements and one for the elements of the value group (which is an ordered abelian group). So, the p-adics have been viewed as structures of the type \((k, \Gamma, +_k, *_k, 0_k, 1_k, +_\Gamma, 0_\Gamma, <_\Gamma)\) which is a combination of the language of fields and the language of ordered abelian groups.

In the \(P_n\)-formalism of § 2.2, we can uniformly view both the reals and the p-adics as structures of a common type, namely fields with an \(n\)-th power structure.

The first main model-theoretic result is regarding model-completeness, [Mac77]:

**Proposition 2.57 (Model-Completeness)**

1. \(R\) The theory of real-closed fields is model-complete. That is, let \(K \subseteq L\) be real-closed. Then a first-order sentence in the language of ordered fields with parameters from \(K\) holds in \(L\) iff it holds in \(K\). The same is true in the language of fields augmented with the \(P_2\)-predicate.

2. \(Q_p\) The theory of p-adically closed fields is model-complete. That is, let \(K \subseteq L\) be p-adically closed. Then a first-order sentence in the language of valued fields with parameters from \(K\) is true in \(L\) iff it is true in \(L\). The same holds in the language of fields augmented with all the predicates \(P_n, n \geq 2\).

A consequence of this result are the following transfer principles:

**Proposition 2.58 (Transfer Principles)**

1. *(Tarski’s transfer principle for \(R\))* A first-order sentence is true in all real-closed fields iff it is true in \(R\).
2. (Ax-Kochen-Ersov transfer principle for $\mathbb{Q}_p$) A first-order sentence is true in all $p$-adically closed fields iff it is true in $\mathbb{Q}_p$.

This can also be deduced from the following important property of the two theories:

**Theorem 2.59 (Quantifier-Elimination)**

1. $\mathbb{R}$ (Tarski, [Tar51], also [Col75,BOKR86]) The theory of real-closed fields admits elimination of quantifiers in the language of ordered fields, or in the language of field theory augmented with the predicate $P_2$.

2. $\mathbb{Q}_p$ (Macintyre, [Mac76], also [Den86]) The theory of $p$-adically closed fields admits elimination of quantifiers in the language of fields augmented with all the predicates $P_n, n \geq 2$. We do not get elimination of quantifiers in the pure language of valued fields.

The last statement is a notable advantage of the $P_n$-formalism over the traditional valuation formalism.

A nice converse to the above is

**Proposition 2.60 (Macintyre, McKenna, and van den Dries, [MMvdD83])**

*In the $P_n$-formalism:*

1. $\mathbb{R}$ An ordered field that admits elimination of quantifiers is real-closed.

2. $\mathbb{Q}_p$ A “Belair-Robinson” field (see § 2.3.1) that admits elimination of quantifiers is $p$-adically closed.

### 2.3.3 Semi-Algebraic Geometry

A semi-algebraic set in $\mathbb{R}^n$ is one that is specified by a set of polynomial equations and inequalities. Thus a semi-algebraic set in $\mathbb{R}^n$ has the form:

$$\{x \in \mathbb{R}^n : f(x) = 0, g_1(x) \sim 0, \ldots, g_k(x) \sim 0\}$$
where \( f, g_1, \cdots, g_k \in \mathbb{R}[x] \) and \( \sim \) is one of the two order relations, \(<, >\). Real semi-algebraic geometry comprises the study of these semi-algebraic sets and their morphisms.

At first sight there is no immediate analogue for the order relation \(<\) over the \( p \)-adics. However the "\( n \)-th power" formalism from § 2.2 and the Artin-Schreier/Prestel-Roquette theory from § 2.3.1 provides the appropriate analogue. Thus, we view the (real) semi-algebraic set

\[
\{ x \in \mathbb{R}^n : f(x) = 0, g_1(x) > 0, g_2(x) < 0 \}
\]

as the set

\[
\{ x \in \mathbb{R}^n : f(x) = 0, \text{sgn}(g_1(x)) = +1, \text{sgn}(g_2(x)) = -1 \}
\]

and this suggests that we define a \( p \)-adic semi-algebraic set to be one of the form

\[
\{ x \in \mathbb{Q}_p^n : f(x) = 0, \rho_{n_1}(g_1(x)) = b_{n_1}, \cdots, \rho_{n_k}(g_k(x)) = b_{n_k} \}
\]

where \( f, g_1, \cdots, g_k \in \mathbb{Q}_p[x], \) the \( \rho \)s are the canonical homomorphisms, \( \rho_n : \mathbb{Q}_p^* \to \mathbb{Q}_p^*/\mathbb{Q}_p^{*(n)} \), \( n \geq 2 \), and the \( b_n \)s are canonical integer coset representatives, from § 2.2.

There are some simplifications one can make. First, by allowing integers in the language, one can write a condition of the form \( \rho_n(g_k(x)) = b_n \) as \( P_n(h(x)) \) in the formalism introduced in § 2.2 and § 2.3.2. Second, from § 2.2, we can always express an equation \( f(x) = 0 \) as \( P_2(p \cdot f(x))^2 \). Lastly, one can do by considering only one \( n \) by the following lemma which obtains from Proposition 2.47 in § 2.2.2.

**Lemma 2.61** If \( m|n \), then there exist an (explicitly given) set of integers, \( b_1, \cdots, b_k \) such that

\[
P_m(f(x)) \leftrightarrow \bigwedge_{b_i} P_n(b_i \cdot f(x))
\]

Hence, by taking the least common multiple of the different powers occurring in the formula, finally, we define a semi-algebraic set over the \( p \)-adics as a boolean combination of sets of the form:
\{x \in \mathbb{Q}_p^n : P_n(f_1(x)) \land \cdots \land P_n(f_k(x))\}

In Real semi-algebraic geometry, one has a strengthened form of the quantifier-elimination theorem called the “finiteness theorem”, [vdD82]: a definable open subset of \(\mathbb{R}^n\) can be defined using only positive boolean operations\(^8\) and strict polynomial inequalities. Introduce the notation, as in [Rob87], \(R_n(x) \iff x \neq 0 \land P_n(x)\). One can of course express the condition \(f(x_1, \cdots, x_n) > 0\) by \(R_2(f(x_1, \cdots, x_n))\) in the reals. In [Rob87], an exact p-adic analog is obtained:

**Theorem 2.62 (“Finiteness” Theorem)** \((k := \mathbb{R} \text{ or } \mathbb{Q}_p)\) Any definable open subset of \(k^n\) can be defined using only \(\lor, \land\) and the \(R_n, n \geq 2\).

On definable sets, one has the following further analogies from [SvdD88]. The first can be thought of as a “formal Baire theorem” and the second leads to a sensible notion of dimension.

**Proposition 2.63** \((k := \mathbb{R} \text{ or } \mathbb{Q}_p)\)

1. Suppose \(S \subseteq k^m\) has non-empty interior, and \(S = \cup_i S_i\), with each \(S_i\) definable. Then some \(S_i\) has non-empty interior.

2. Let \(S \subseteq k^m\) be definable. then \(S = \cup_i S_i\) where each \(S_i\) is definable and for each \(i\), either \(S_i\) is open, or has no interior and is homeomorphic by a bi-analytic projection along certain co-ordinate axes to an open subset of some \(k^d\) where \(d < m\).

The promised notion of dimension obtains as follows: define the dimension of \(S \subseteq k^m\) as the largest \(d\) such that \(S = \cup_i S_i\), each \(S_i\) is definable and for some \(i\), \(S_i\) is homeomorphic by a bi-analytic projection along certain co-ordinate axes to an open subset of some \(k^d\) where \(d < m\)\(^9\). Then, [SvdD88]:

---

\(^8\)i.e. no negations.

\(^9\)Put \(\text{dim}(\emptyset) := -\infty\)
Proposition 2.64 \((k := \mathbb{R} \text{ or } \mathbb{Q}_p)\)

1. \(\dim(k^m) = m.\)

2. If \(X, Y\) are definable subsets of \(k^m\), then

\[
\dim(X \cup Y) = \max(\dim(X), \dim(Y))
\]

and \(\dim(X) \leq \dim(Y)\) if \(X \subseteq Y.\)

3. If \(X\) is definable, then \(\dim(X)\) is equal to the algebro-geometric dimension of the Zariski closure of \(X.\)
Chapter 3

Quantifier Elimination and Decision Procedures for Sentences in P-adic Fields

3.1 Introduction

The decision problem for fields, namely, the problem of deciding the truth of first-order sentences in the language of fields for various classes of fields has been a classical concern of mathematicians, especially among logicians and algebraists. Recently, this has also been studied by computer scientists from a complexity theoretic perspective. In particular, the decision problems for the complexes, $\mathbb{C}$ and for the reals, $\mathbb{R}$, have been very well studied, [Hei83,Gri87b,Ier89,Col75,BOKR86, Gri87a,Ren89]. In this chapter we give quantifier elimination and decision procedures for the theory of $p$-adically closed fields (of which the canonical representative is Hensel’s field of $p$-adic numbers, $\mathbb{Q}_p$). Our main results show that these problems are of essentially the same complexity as the corresponding problems for the theory of real addition and for the theories of various classes of Boolean algebras.

The decision problem for $\mathbb{C}$ (or for any algebraically-closed field) is essentially
concerned with the solvability of systems of polynomial equations. This issue was addressed extensively earlier this century by mathematicians like Hermann and Kronecker and constitutes the classical area called *Elimination Theory*. The decision problem for the reals, $\mathbb{R}$, was first addressed in the celebrated work of Alfred Tarski, [Tar51] where it was viewed as constituting the foundations of elementary algebra and geometry. None of these investigations pay any heed to quantitative complexity issues.

More recently, these problems have attracted the attention of computer scientists. The goal is to obtain a *precise quantitative* classification of the computational complexities of the decision problem for various classes of fields. For $C$ (or any algebraically closed field), the results of, *inter alia* [Hei83,Gri87b,Ier89]. show in essence, that the decision problem can be solved in double exponential space. Similar advances were made with regard to the decision problem for $\mathbb{R}$, culminating in the works [Col75,BOKR86,Gri87a,REN89], which show, in essence, that the decision problem for $\mathbb{R}$ can be solved in double exponential time or in exponential space.

The decision problem for $\mathbb{Q}_p$ was shown to be decidable in an influential series of papers by James Ax and Simon Kochen, [AK65,AK66], and also independently by Ersov,[Ers65]. However, their methods were model-theoretic and not effective. Paul Cohen ¹, [Coh69] gave an explicit, elementary Primitive recursive decision procedure which was subsequently refined and generalized by Volker Weispfenning, [Wei76,Wei83]. However, none of these works give any quantitative complexity bounds. Weispfenning, [Wei88] restricts attention to certain linear (divisibility) sentences to obtain the first precise quantitative bounds.

To start, we resolve the complexity of the decision problem for a certain fragment of the first order theory of the $p$-adics in the new $n$-th power formalism. The fragment we consider consists of *linear sentences* in the language of fields

¹Of the Continuum Hypothesis fame!
augmented by Macintyre's \( n \)-th power predicates. An alternate way to say this is that we are considering only the restricted theory \( \text{Th}((\mathbb{Q}_p, +, 0, 1, (P_k)_{k \geq 2})) \) of \( \mathbb{Q}_p \) without multiplication. This is parallel to the work of Ferrante and Rackoff, [FR75], and also [Ber80,Fö82] for the theory of real addition with order. It is also related to the work of Weispfenning,[Wei88] cited above; but we work in the language of the new formalism of \( n \)-th powers whereas Weispfenning works in the traditional formalism of valued fields. Via the fact that the valuation is definable in terms of the new formalism, our work encompasses that of Weispfenning. Furthermore, we obtain very similar complexity results. However the techniques we use are completely different – the Ferrante-Rackoff method is applicable only to ordered, divisible, abelian groups, while Weispfenning's ideas are applicable only in a valued field setting.

In essence, we show that the decision problem for linear sentences in \( \mathbb{Q}_p \) is computationally equivalent to the decision problem for real addition, [Ber80] and to the theories of various classes of Boolean algebras, [Koz80]. We employ a lemma of Denef, [Den84,Den86], to obtain the first quantitative bounds for quantifier elimination and decision procedures in the \( P_n \)-formalism of Macintyre. Our decision procedure for linear sentences in \( \mathbb{Q}_p \) is in the form of an alternating Turing machine algorithm that runs in exponential time and makes as many alternations as there are quantifiers in the input formula. This places the decision problem in the alternating Berman complexity class \( \cup_n \mathcal{ST}(\exists, 2^n, n) \). Further, we observe that previous results yield in fact, that the decision problem is complete for this class, so we determine the precise complexity of the decision problem. In particular, the decision problem can be solved in exponential space.

Another important and related problem over fields is that of quantifier-elimination: Given a formula \( F := (Q_1 x_1)(Q_2 x_2) \cdots (Q_n x_n)(E(x_1, \cdots x_n)) \), where \( Q_i \) is either \( \exists \) or \( \forall \) for each \( i \), produce a quantifier free formula \( F' \) equivalent to \( F \) (over the class of fields under consideration). While it has been known that \( \mathbb{Q}_p \) admits elimination
of quantifiers in the new formalism (as opposed to the pure valued field formalism), [Mac76,Den86], we present the first explicit quantifier elimination procedure (for the linear fragment) of $\mathbb{Q}_p$ with precise quantitative complexity bounds. We give a quantifier elimination procedure running in double exponential time and space. This is shown to be essentially optimal by exhibiting a family of linear formulas for which any such procedure must take exponential space. In fact, any quantifier free equivalents to the formulas in this family are shown to have size at least double exponential in the size of the original formulas. So the linear elimination problem for $\mathbb{Q}_p$ is of the same complexity as the quantifier elimination problem for torsion-free abelian groups, for algebraically closed fields, [Hei83,Ier89] and for real-closed fields, [DJ88].

Next we extend these results to cover the full theory. The main tools we use are the Cell Decomposition Lemmas of Denef, [Den86]. We give explicit bounds for the number of cells and the size of various parameters produced by the decomposition and use these bounds to give an alternating exponential time algorithm for the full theory. This implies that the complexity of the decision problem for $p$-adic fields is the same as the complexity of the corresponding problem for the reals. We also give an explicit quantifier-elimination procedure for the full theory which runs in double-exponential time and space which is optimal and of the same complexity as the corresponding optimal procedure for the reals. This is a pleasant augmentation of the well known $\mathbb{R}$-$\mathbb{Q}_p$ analogy from a computational viewpoint.

This chapter is organized as follows. In § 3.2, we briefly give some background material on the $p$-adics. In § 3.3, we describe our decision procedure and quantifier elimination procedure, and give a precise quantitative analysis of these algorithms. In § 3.4, we show that these bounds are in fact optimal by giving lower bounds on the complexities of these problems. In § 3.5, we apply the Denef Cell Decomposition Lemmas to give optimal decision and quantifier-elimination procedures for the full theory.
3.2 Some Facts about $Q_p$

We recall some basic facts about $Q_p$ from Chapter 2. For a prime $p$ and an integer $m$, define $v_p(m)$ \(^2\), to be the highest power of $p$ dividing $m$. Extending this to the rationals by setting $v(m/n) := v(m) - v(n)$, we obtain the $p$-adic valuation on $Q$. The function $\phi(x) := p^{-v(x)}$ defines the $p$-adic metric on the rationals. The field of $p$-adic numbers, $Q_p$, is obtained by completing the rationals with respect to this metric.

In $R$, the subgroup of the multiplicative group of units, $R^*$ consisting of the squares, $R^{*2}$ plays an important role. The following are familiar facts: $[R^* : R^{*2}] = 2$ and $\pm 1$ are a set of coset representatives (in fact these are simply the signs of real numbers). In the $p$-adics, subgroups of $n$-th powers play a similar role. However, for $Q_p$, it is necessary, in general, to consider all $n$-th powers, not simply squares, [Mac76,PP84]. We have the following

FACTS [Bel88,PP84]: For each $k \geq 2$, $[Q_p^* : Q_p^{*k}]$ is finite and there is a set of integer coset representatives, $B_k := \{b_1^{(k)}, \ldots, b_l^{(k)}\}$.

There is a nice structure theorem describing these subgroups and quotient groups, see Chapter 2. Important consequences are the following two propositions.

**Proposition 3.1**

$$Q_p^{*n} \cong nZ \times F_p^{*n} \times U_{v(n)+1}$$

(Here $U_k := \{1 + p^k \cdot x : x \in Q_p, v(x) \geq 0\}$.)

**Proposition 3.2** If $m|n$, then there exist an (explicitly given) set of integers, $b_1, \ldots, b_k$ such that

$$P_m(f(x)) \leftrightarrow \lor_{b_i} P_n(b_i \cdot f(x)).$$

Macintyre introduced his $n$-th power formalism into the study of $Q_p$ to exploit the analogy between squares in the reals and $n$-th powers in the $p$-adics. This

\(^2\)We will omit the subscript $p$ in the future having fixed a prime $p$
formalism has turned out to be a fecund source of analogies between the two structure, see § 2.3. In this so-called $P_n$-formalism, we augment the language of rings to include predicates $P_k$, $k \geq 2$ whose interpretations in the structure $Q_p$ will be the subgroups of $k$-th powers. Precisely, $P_k(x) \leftrightarrow \exists y(x = y^n)$. An advantage of this formalism over the traditional valuation formalism is that one can define the valuation in terms of the $P_k$-predicates:

**Proposition 3.3** 1. If $p \neq 2$, then for any $a, b \in k$,

$$v(a) \leq v(b) \leftrightarrow P_2(a^2 + p \cdot b^2).$$

2. If $p = 2$, then for any $a, b \in k$,

$$v(a) \leq v(b) \leftrightarrow P_3(a^3 + p \cdot b^3).$$

One can also define equality via:

**Proposition 3.4** Let $a \in k$. Then

$$a = 0 \leftrightarrow P_2(p \cdot a^2).$$

$Q_p$ is typical of a class of fields axiomatized by a set of algebraic sentences called the $p$-adically closed fields [PP84]. These are the analogues to the real-closed fields. As in the real case, all the $p$-adically closed fields are elementarily equivalent to $Q_p$, that is, they satisfy the same sentences.

### 3.3 Linear Sentences in $Q_p$

As mentioned briefly in the last section, it is fruitful to consider $Q_p$ as a structure for the language of rings augmented by the predicates $P_k$, $k \geq 2$. We define a linear term as in [Wei88] as one of the form $a_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n$ where $a_0, \cdots a_n \in Q$. Atomic formulas are of the type $t = 0$ or $P_k(t)$, $k \geq 2$ where $t$ is

\footnote{More generally, one can allow these to be algebraic $p$-adic numbers}
a linear term. As in § 3.2, it suffices to consider atomic formulas of the latter type since \( t = 0 \) is equivalent to \( P_2(p \cdot t) \). Summarizing, a linear atomic formula is of the form \( P_k(a_0 + a_1 \cdot x_1 + \cdots + a_m \cdot x_m) \) where \( a_0, \cdots, a_m \in Q, m \geq 0 \) and \( k \geq 2 \). Closing under boolean operations and quantifiers gives us all the linear formulas. An alternate way to say this is that we are considering only the restricted theory \( \text{Th}((Q_p, +, 0, 1, (P_k)_{k \geq 2})) \), i.e. \( Q_p \) without multiplication.

Given a linear formula,

\[
F := (Q_1 x_1)(Q_2 x_2) \cdots (Q_n x_n)(E(x_1, x_2, \cdots, x_n)
\]

(where each \( Q_i \) is \( \exists \) or \( \forall \)) we will give a decision procedure to test if \( Q_p \models F \). By the fact that all \( p \)-adically closed fields are elementarily equivalent to \( Q_p \), this in fact gives a decision procedure for the class of all \( p \)-adically closed fields. We also give a quantifier elimination procedure to produce a quantifier free formula \( f' \) such that \( Q_p \models (F \iff F') \).

We start with a simple observations. First, for an atomic formula

\[
a_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n
\]

and for \( k \geq 2 \),

\[
P_k(a_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n) \iff P_k(b^{(k)} \cdot (x_n - c(x_1, \cdots, x_{n-1})))
\]

where \( c(x_1, \cdots, x_{n-1}) = -(\frac{a_1}{a_n} \cdot x_1 + \cdots + \frac{a_{n-1}}{a_n} \cdot x_{n-1}) \) and \( b^{(k)} \) is an integer (coset representative) chosen such that \( P_k(b^{(k)} \cdot a^{-1}) \). (The integer \( b^{(k)} \) is bounded independent of the size of the coefficient \( a_n \); it depends only on \( k \).) Next, we may assume that all the atomic formulas occurring in a formula have the form \( P_k(t) \) for a fixed \( k \). By Proposition 3.2, we can do this by considering the least common multiple of all the \( k \)s such that a predicate \( P_k \) occurs in the formula.

### 3.3.1 Denef's Lemma

The main ingredient in our proof is the following refinement of a lemma due to Denef, [Den84,Den86]. The construction is due entirely to Denef, and the lemma
is proved by simply analyzing his construction. For a formula \( F \), let \( l(F) \) denote the length and let \( s(F) \) denote the largest absolute value of any integral constant appearing in any rational constant in \( F \).

**Lemma 3.5** Let \( x := (x_1, \ldots, x_m) \) and let \( c_1(x), c_2(x) \) be two linear terms. For some fixed \( n \geq 2 \), let \( b_1^{(k)}, b_2^{(k)} \) be two integer coset representatives of \( n \)-th powers. Then there exists a set \( D \) of linear terms \( c(x) \) (which can be explicitly computed in time polynomial in \( l(c_1) + l(c_2) \)) such that

1. The formula \( \exists t(P_k(b_1^{(k)} \cdot (t - c_1(x))) \land P_k(b_2^{(k)} \cdot (t - c_2(x))) \) is equivalent to the formula \( \forall t(P_k(b_1^{(k)} \cdot (t - c_1(x))) \land P_k(b_2^{(k)} \cdot (t - c_2(x)))) \) is equivalent to the formula \( \land_{c(x) \in D} c(x) \).

2. For each \( c(x) \in D \), \( l(c) \leq \gamma \cdot (l(c_1) + l(c_2)) \) for some constant \( \gamma \) (depending only on \( n \) but not on the terms themselves).

3. For each \( c(x) \in D \), \( s(c) \leq (\max(s(c_1), s(b_1^{(k)}), s(c_2), s(b_2^{(k)})))^{\gamma'} \) where \( \gamma' \) is a constant depending only on \( n \) but not on the individual terms.

By a repeated application of Denef’s Lemma, we obtain:

**Proposition 3.6** Given a linear formula \( F := Qt(E(x, t)) \), one can obtain an equivalent formula \( F'(x) \) in which each term \( P_k(c(x), t) \) in the original formula is replaced by a disjunction (if \( Q \) is \( \exists \)) or a conjunction (if \( Q \) is \( \forall \)) of a constant number of formulas \( P_k(c'(x)) \). Moreover \( l(F') \leq (l(F))^{\gamma} \), and \( s(F') \leq (s(F))^{\gamma'} \) for some constants \( \gamma \) and \( \gamma' \).

**Sketch of Proof:** The first statement and the bound on length follow immediately from the construction. To analyze the size bound, let us say, as in [FR75], that a rational number \( r \) is limited by a positive integer \( k \), and write \( r \leq k \) if there exist integers \( a, b \) such that \( r = a/b \) and \( |a|, |b| \leq k \). Next we observe that if \( r_1 \leq w_1, \ldots, r_k \leq w_k, \) then \( r_1 + \cdots + r_k \leq k \cdot w_1 \cdots w_k, \) and \( r_1 \cdots r_k \leq w_1 \cdots w_k. \)

---

\(^4\)For simplicity, we will always assume \( l(F), s(F) \geq 2 \)
Now the bounds follow by straightforward computations on the formulas produced by Denef's construction. □

3.3.2 A Decision Method

The corollary immediately allows us to give an alternating Turing machine algorithm to decide a sentence in our language. At an existential quantifier, we make an existential branch over all the disjuncts produced by Denef's construction. At a universal quantifier, we similarly make a universal branch. At the bottom, we can decide an atomic formula $P_k(a)$ where $a \in Q$ by using the criterion in Proposition 3.1.

3.3.3 Complexity of the Decision method

To analyze the complexity of the algorithm, we need to bound the size of the rational numbers produced during its course. From Proposition 3.6, it follows that the largest constant produced is at most $2^{2^n}$ on a formula with $n$ variables, for some constant $\gamma$. Hence the bottom level computation takes time $O(2^{\gamma n})$. All the other computations involved take polynomial time and we make $n$ alternations. We conclude that

**Theorem 3.7 (Decision Procedure for Linear Sentences in $Q_p$)** The decision problem for linear sentences over $Q_p$ is in the Berman complexity class $\cup_\gamma \mathcal{ST}_A(\ast, 2^{\gamma n}, n)$. In particular it can be solved in $\mathcal{EXPSPACE}$ and in double exponential time.

3.3.4 Quantifier Elimination

One can in fact extract an explicit quantifier-free formula equivalent to $F$. First we put $F$ in prenex normal form in the standard way. Next, to eliminate an existential quantifier, we replace the formula with the conjunction or disjunction, as appropriate, produced by Denef's construction.
3.3.5 Complexity of Quantifier Elimination

Let us compute the space needed to eliminate quantifiers in a formula $F$ with $l(F) := l_0$ and $s(F) = s_0$. Putting it into prenex normal form produces a formula of length at most $l_0 \log l_0$, taking into account even variable subscripts. From Proposition 3.6, it follows that the largest formula produced in the course of quantifier elimination is at most $(l_0 \log l_0)^{\gamma n_0}$ where $F$ has $n_0$ quantifiers, for some constant $\gamma$. This is bounded by $2^{2^{\gamma n}}$ for some constant $\gamma'$. Hence,

**Theorem 3.8 (Quantifier Elimination for Linear Sentences in $Q_p$)** There is a quantifier elimination procedure for the theory of linear sentences in $Q_p$. Given a formula $F$, this produces a quantifier-free formula $F'$ equivalent to $F$ in double exponential time. Moreover, $l(F') \leq 2^{2^{\gamma (F)}}$ for some constant $\gamma$.

Weispfenning, [Wei88], employs a language with a divisibility predicate so that his atomic formulas have the form $t = 0$ or $t_1 \div t_2$. In the $P_k$-formalism this is expressible as $P_2(t_1^2 + p \cdot t_2^2)$. This formula is not linear, but via the Cell Decomposition method of Denef, [Den84,Den86], we can express it in terms of other linear formulas. Thus our results encompass those of Weispfenning, [Wei88].

3.4 Lower Bounds

In this section, we show that the upper bounds on complexity in § 3.3 are tight, in that,

1. The decision problem for linear sentences in $p$-adically closed fields is hard for $\cup_c STA(\varepsilon, 2^c n, n)$ under polynomial-time reductions.

2. Any quantifier elimination procedure for linear sentences in $p$-adically closed fields requires double exponential space on an explicit (infinite) family of linear sentences of linear length.
The first assertion was essentially proved by Berman, [Ber80], by analyzing the original argument of Fischer and Rabin, [FR74]. Berman showed that $\cup_{c} STA(*, 2^{cn}, n)$ is polynomial-time reducible to the theory of $R$. It was observed by, *inter alia*, Weispfenning [Wei88] and F"{u}rer [F"{u}82], that this reduction (and in fact the original one of [FR74]) makes no essential use of the order relation. In fact, it holds for any theory in the language $L_{G1} := (0, 1, +)$ of abelian groups, such that all its models are groups, and in one model, an element (for instance, 1) of infinite order exists. More precisely,

**Proposition 3.9 (Fischer-Rabin, Berman)** Let $G$ be a torsion-free abelian group with distinguished element $0 \neq 1$. $G$ may carry additional structure for a language $L$ extending $L_{G1}$. Then, the decision problem for first order sentences in the $L$-theory of $G$ is hard for $\cup_{c} STA(*, 2^{cn}, n)$ under polynomial time reductions.

Combining this with the result of § 3.3, we obtain

**Corollary 3.10** The decision problem for linear sentences in the theory of $p$-adically closed fields is complete for $\cup_{c} STA(*, 2^{cn}, n)$ under polynomial time reductions.

For the lower bound on explicit quantifier elimination, we combine two ingredients. The first is a construction of Fischer and Rabin ([FR74], Th.8, Cor.9), slightly extended as in [Wei88]:

**Lemma 3.11 (Fischer-Rabin)** There is a positive constant $c$, and a sequence $\mu_{n}, n \geq 1$ of $L_{G1}$-formulas with one free variable $x$, such that

1. If $G$ is an abelian group in which 1 is an element of infinite order, then

$$\mu_{n}^{G} := \{a \in G : G \models \mu_{n}(a)\} = \{0, 1, \ldots, 2^{2n} - 1\}$$

2. If $G$ is an abelian group with distinguished element $1 \neq 0$, then

$$\mu_{n}^{G} \supseteq \{0, 1, \ldots, 2^{2n} - 1\}$$
3. \( l(\mu_n) \leq c \cdot n \).

The second ingredient is a general technical lemma due to Weispfenning, [Wei88], relating the geometry of definable sets to their sizes. A non-empty set \( \mathsf{Top} \) of topologies \( \tau \), on a set \( G \) are said to be independent, if whenever \( \mathcal{U} \) is a set of non-empty subsets of \( G \) such that there is an injective map \( \mathcal{U} \hookrightarrow \tau \), such that \( \mathcal{U} \) is \( \tau \)-open, then \( \cap \mathcal{U} \neq \emptyset \). For \( A \subseteq G \), and \( \tau \in \mathsf{Top} \), let \( \delta_\tau(A) := \text{Cl}_\tau(A) \cap \text{Cl}_\tau(G - A) \) denote the \( \tau \)-boundary of \( A \).

**Proposition 3.12 (Weispfenning)** Let \( G \) be an abelian group with distinguished element \( 1 \) of infinite order. (\( G \) may carry additional structure for a language \( L \) extending \( L_{G1} \).) Let \( \mathsf{Top} \) be a finite independent set of \( T_1 \)-topologies on \( G \) such that for any \( \tau \in \mathsf{Top} \), no \( a \in G \) is \( \tau \)-isolated. Assume further, that there is a constant \( d > 0 \), and a map \( \psi(x) \mapsto \tau_\psi \) from the set of atomic, 1-variable \( L \)-formulas to \( \mathsf{Top} \) such that \( |\delta_\tau(\psi^G)| \leq d \cdot l(\psi) \). Let \( c, \mu_n \) be as in lemma 3.11. Then, for any sequence \( \sigma_n(x)n \geq 1 \), of quantifier-free \( L \)-formulas, with \( G \models \mu_n \leftrightarrow \sigma_n \) for all \( n \geq 1 \), we have that \( d \cdot l(\sigma_n) \geq 2^{2^{\frac{1}{2} \cdot l(\mu_n)}} \) for all \( n \geq 1 \).

We apply this for \( \mathbb{Q}_p \) with \( \mathsf{Top} \) containing just the valuation topology. From §3.2, we have that \( P_k^{\mathbb{Q}_p}(f(x)) \) is closed for any polynomial \( f \) and all \( k \geq 2 \), so \( \text{Cl}(P_k^{\mathbb{Q}_p}(f(x))) = P_k^{\mathbb{Q}_p}(f(x)) \). Also,

\[
\text{Cl}(Q_p - P_k^{\mathbb{Q}_p}(f(x))) = \text{Cl}(\bigcup_{b \in B_k} P_k^{\mathbb{Q}_p}(bf(x))) = \bigcup_{b \in B_k} \text{Cl}(P_k^{\mathbb{Q}_p}(bf(x))) = \bigcup_{b \in B_k} P_k^{\mathbb{Q}_p}(bf(x))
\]

where \( B_k \) is a set of integer coset representatives of \( n \)-th powers excluding \( 1 \). Hence,

\[
\text{Cl}(P_k^{\mathbb{Q}_p}(f(x))) \cap \text{Cl}(Q_p - P_k^{\mathbb{Q}_p}(f(x))) = \bigcap_{b \in B_k} P_k^{\mathbb{Q}_p}(f(x)) \cap P_k^{\mathbb{Q}_p}(bf(x)) = (f(x) = 0)^{\mathbb{Q}_p}
\]

So we may take \( d = 1 \), and obtain
Corollary 3.13  Any quantifier-free formula $\sigma_n$ equivalent to $\mu_n$ over $Q_p$ has $l(\sigma_n) \geq 2^n$ for $n \geq 1$. Hence any quantifier elimination procedure for $Q_p$ requires at least double exponential space.

3.5  Algorithms and Analysis for the Full Theory

In this section, we give quantifier elimination and decision procedures for the full theory. To handle the more complicated non-linear sentences involved, we invoke certain Cell Decomposition Lemmas due to Denef, [Den86]. In order to give quantitative complexity bounds, we refine the lemmas by giving explicit bounds on the number of cells and the sizes of the various parameters produced. In this form, we are able to use the decomposition to give an alternating exponential time decision procedure. We also give a deterministic quantifier elimination procedure running in double exponential time or in exponential space. By the results of the last section, these bounds are essentially optimal.

We remark also that these results show that

- The decision problem and the quantifier-elimination problems for the full theory are of the same complexity as those for the linear fragment, and

- The complexities of the two problems are the same as the corresponding ones for the reals and for various classes of Boolean algebras.

In the rest of this section, we will denote by $k$ a $p$-adically closed field such as $Q_p$.

3.5.1  Denef’s Cell Decomposition Lemmas: Quantitative Versions

The basic intent behind a Cell Decomposition is to partition affine space into “cells” in each of which a given set of polynomials “behaves well”. In the well-known
Cylindrical Algebraic Decomposition algorithm over the reals, for instance [Col75], real affine space is partitioned into cells delineated by polynomial inequalities such that in each cell a given set of polynomials maintains constant sign. The natural analogue over the p-adics would be to partition p-adic affine space into cells in each of which a given set of polynomials maintains fixed coset representatives of certain $n$th powers. In this section, we describe and refine a Cell Decomposition lemma due to Denef, [Den84,Den86], that meets these requirements. In order to obtain this decomposition, an auxiliary decomposition is needed that partitions p-adic affine space into cells in each of which given polynomials are well behaved with respect to their valuations, in a sense which is made precise below.

First we need some preliminary definitions. Recall the following definition motivated in Chapter 2.

**Definition 3.14** A subset of $k^m, m \geq 1$ is semi-algebraic if it is a boolean combination of subsets of the form

$$\{ x \in k^m : P_n(f(x)) \}$$

where $f \in k[x_1, \ldots, x_m]$ and $n \geq 2$. $\square$

We extend this notion to functions as follows, [Den86]:

**Definition 3.15** A function $f : k^m \to k, m \geq 1$ is semi-algebraic if for every semi-algebraic subset $S \subseteq k \times k^r, r \geq 1$, the set

$$\{(x, y) \in k^{m+r} : (f(x), y) \in S\}$$

is semi-algebraic. $\square$

**Remarks:**

1. The graph of a semi-algebraic function is semi-algebraic.
2. A polynomial is a semi-algebraic function.

3. The class of semi-algebraic functions is closed under composition, addition and multiplication.

From Chapter 2, we know that sets defined by polynomial equalities and inequalities between valuations of polynomials are semi-algebraic. In [Den86], it is proved that sets defined by congruences are also semi-algebraic.

Now we can define the p-adic analog of a cell:

**Definition 3.16** A *cell* in $k^m \times k$ is a set of the form

$$\{(x, t) : x \in C \land \nu(a_1(x)) \sqcap_1 \nu(t - c(x)) \sqcap_2 \nu(a_2(x))\}$$

where $C \subseteq k^m$ is semi-algebraic, $a_1, a_2$ and $c$ are semi-algebraic functions and $\sqcap_1, \sqcap_2$ denotes either $\leq, <$ or no condition. The cell is said to have center $c(x)$. □

The next proposition gives a decomposition of p-adic affine space into cells such that in each cell, the valuation of a given polynomial is bounded near the valuation of an individual term. The idea of this decomposition goes back to Cohen, [Coh69] and the key tools used are the Ultrametric Equality and Hensel's Lemma. We use the construction as in Denef, [Den86], but supplement it with quantitative information which bounds its size.

**Proposition 3.17** (Cohen, Denef, [Coh69, Den86]) [Cell Decomposition Lemma: Valuation Version] Let $f(x, t)$ be a polynomial in $t$ with coefficients which are semi-algebraic functions of $x \in k^m$. Then, there exists a finite partition of $k^m \times k$ into cells $A$ such that each cell has associated with it a center, $c(x)$ (where $c(x)$ is semi-algebraic) and a bound $e \in \mathbb{N}$ such that if we write

$$f(x, t) := \sum_{i \geq 0} a_i(x)(t - c(x))^i$$

then

$$\nu(f(x, t)) \leq \min_{i} \nu(a_i(x)(t - c(x))^i) + e$$
In particular, let \( f \in \mathbb{Z}[x_1, \ldots, x_n] \) and suppose the degrees of \( f \) in \( x_1 \ldots x_n \) are bounded by \( d_1, \ldots, d_n \) and that the coefficients are bounded in size by \( L \). (Denote \( \sum_i d_i \) by \( D \).) Then there exists a partition of size \( O(2^{c \cdot 2^{D+L+n}}) \) and the constant \( e = O(2^{D+L+n}) \) for each such cell.

The proof of the first part of this proposition is identical to that in Denef, [Den86]. To get the bounds of the second part, we need a few lemmas.

**Lemma 3.18 (Legendre)** For a prime \( p \) and \( n \geq 1 \),

\[
v_p(n!) = \frac{n - (a_0 + \cdots + a_k)}{p - 1}
\]

where \( n := a_0 + \cdots + a_k \cdot p^k \) is the \( p \)-adic expansion of \( n \). In particular,

\[
v_p(n!) < \frac{n}{p - 1}
\]

For a proof, see [Rib89], p.22 or [GKP89], p.114.

**Lemma 3.19** For each cell in the decomposition of \( f \) as in the second part of the Cell Decomposition Lemma 3.17, the constant \( e = O(L \cdot 2^{D+N}) \).

**Proof.** We estimate this as \( 2^{D+n} \) times the constant produced by a chain of (partial) differentiations with respect to successive variables. The final constant produced is at most \( d_1! \cdot d_2! \cdots d_n! \cdot \prod_i a_i \) where the \( a_i \) are the coefficients of \( f \). Now

\[
v(d_1! \cdot d_2! \cdots d_n! \cdot \prod_i a_i) = \sum_i (v(d_i!) + v(a_i)) \leq \frac{1}{p - 1} \cdot \sum_i d_i + \sum_i a_i \leq \frac{1}{p - 1} \cdot D + n \cdot 2^L
\]

Hence we get the bound \( e = O(L \cdot 2^{D+n}) \). \( \square \)

**Lemma 3.20** The total number of cells produced in the decomposition is \( O(2^{c \cdot L \cdot 2^{D+n}}) \) for some constant \( c \).
Proof. By examining Denef’s construction, it can be seen that the number of cells produced in the decomposition is bounded by $O(p^e)$ where $e$ is the largest constant produced in the decomposition of $f'$. Combined with the previous lemma, this yields the bound stated. □

The next proposition is a $p$-adic analog of Cylindrical Algebraic Decomposition for the reals \textsuperscript{5}. The key idea is to use Proposition 2.51 to convert the valuation decomposition into a decomposition for $n$th powers.

Proposition 3.21 (Denef) [Cell Decomposition Lemma: $n$th Powers version] Let $f_i(x,t), 1 \leq i \leq r$ be polynomials in $t$ with coefficients which are semi-algebraic functions of $x \in k^n$, and let $n > 1$ be fixed. Then there exists a finite partition of $k^n \times k$ into cells $A$, such that each cell has a center $c(x)$ (which is semi-algebraic), such that for all $(x,t) \in A$, we have,

$$f_i(x,t) = u_i(x,t)^n \cdot h_i(x) \cdot (t - c(x))^{\nu_i}, \quad 1 \leq i \leq r$$

with $v(u_i(x,t)) = 0$, $h_i(x)$ a semi-algebraic function of $x$ and $\nu_i \in \mathbb{N}$ for each $1 \leq i \leq r$.

In particular, if applied to $r$ polynomials with degrees bounded by $d_1, \ldots, d_n$ (with $D := d_1 + \cdots + d_n$) and coefficient size bounded by $L$, it yields a decomposition into at most $O(2^{c_rL}2^{D+n})$ such cells for some constant $c$.

Proof. An examination of Denef’s construction reveals that it partitions each cell produced in the valuation decomposition into at most $p^{r2^{e+n}}$ cells where $e$ is the largest constant produced in the valuation decomposition. using the estimates above, we get the stated bound. □

3.5.2 A Decision Procedure

In this subsection, we use the quantitative version of the Cell Decomposition lemma, Proposition 3.21 to give a decision procedure for the full theory, $\text{Th}(\mathbb{Q}_p, +, \times, 0, 1, \{P_n\}_{n \geq 2})$

\textsuperscript{5}As stated, it is not a cylindrical decomposition as usually understood, but can be made such, [SvdD88]
in the form of an alternating Turing machine algorithm running in exponential
time. This also yields a deterministic decision procedure running in exponential
space or in double exponential time.

We describe an alternating Turing machine algorithm to decide sentences of the
theory of p-adically-closed fields. At any point in the computation, a processor is
attempting to verify a statement of the form

\[ Q_p^k \models (Qx_1) \cdots (Qx_k) \varphi(f_1(x_1, \cdots, x_k), \cdots, f_r(x_1, \cdots, x_k)) \]

where \( \varphi \) is a boolean combination of sentences of the form \( P_n(f_i(x_1, \cdots, x_k)) \).
(Assume, without loss of generality, that the last quantifier is \( \exists \).) By computing
the Cell Decomposition (Nth powers version) for the polynomials involved, this
amounts to verifying several condition of the form

\[
Q_p^k \models (Qx_1) \cdots (Qx_{k-1}) \varphi'(g_1(x_1, \cdots, x_{k-1}), \cdots, g_s(x_1, \cdots, x_{k-1})) \\
\wedge v(a_1(x_1, \cdots, x_{k-1})) \Box_1 v(t - c(x_1, \cdots, x_{k-1})) \Box_2 v(a_2(x_1, \cdots, x_{k-1})) \\
\wedge P_n(\rho \cdot (t - c(x_1, \cdots, x_{k-1})))
\]

The processor activates several child processors, one for each cell, each attempting
to verify such a condition. If the quantifier is \( \exists \), these are generated using V-
branching, if it is \( \forall \), \( \wedge \)-branching is used. As in [Den86], or otherwise, one can
eliminate the \( x_k \) variable at this stage and so each child processor is reduced to
verifying a condition of the form

\[ Q_p \models (Qx_1) \cdots (Qx_{k-1}) \varphi(g_1(x_1, \cdots, x_{k-1}), \cdots, g_s(x_1, \cdots, x_{k-1})) \]

Finally a (super-exponential) number of processors, each attempting to verify a
quantifier-free statement can all use the criterion in Proposition 3.1 from Chapter 2.

To analyze the complexity of the decision procedure, we note from Proposition
3.21 that there are approximately \( 2^{c \alpha \cdot L} \cdot 2^{D+N} \) cells that need to be generated.
However, the alternating machine can generate them in time \( O(\alpha \cdot L \cdot 2^{D+N}) \) by
its parallel branching capability. So there will be a double exponential number of processes running concurrently to verify their respective conditions. At the bottom it is clear that the criterion of Proposition 3.1 can be used to verify the quantifier-free condition in exponential time. Thus the overall alternating algorithm runs in time $O(r \cdot L \cdot 2^{D+N})$ i.e. in double exponential time. Moreover, the machine clearly makes at most $n$ alternations.

This analysis combined with results from the last section yield:

**Theorem 3.22 (Decision Problem for $Q_p$)** The decision problem for linear sentences over $Q_p$ is complete for the Berman complexity class $\cup_{\gamma} \text{STA}(\cdot, 2^\gamma, n)$. In particular it can be solved in $\text{EXPSPACE}$ and in double exponential time.

### 3.5.3 A Quantifier-Elimination Procedure

The decision problem of the last section can actually be converted into a deterministic quantifier-elimination algorithm in the straightforward way, eliminating one variable at a time by taking a disjunction over all the cells produced in the decomposition. To analyze the complexity of the algorithm, we merely note that the size of the constants involved in the formulas can at most increase by a constant, and that the number of polynomials produced to replace a given polynomial in a cell is at most four times the original. This yields

**Theorem 3.23 (Quantifier-Elimination for $Q_p$)** There is a quantifier elimination procedure for the theory of linear sentences in $Q_p$. Given a formula $F$, this produces a quantifier-free formula $F'$ equivalent to $F$ in double exponential time. Moreover, $l(F') \leq 2^{2^{\gamma |F|}}$ for some constant $\gamma$. 

Chapter 4

Representing and Computing p-adic Roots of Polynomial Equations

4.1 Introduction

In Computer Science, p-adic methods are often of use in accurate and efficient computations, [Yun76,Lip76,Lau82].

Solving polynomial equations over the real and complex numbers is a classical endeavor, [Usp48]. Recently, efficient algorithms have been developed to symbolically compute zeroes of polynomials over the reals, [BOFKT88]. This was subsequently extended to the complex numbers, [Nef90]. In a different vein, an unusual representation of real algebraic numbers (derived from a remarkable proposition called Thom’s lemma in real algebraic geometry, [Dic85]) and algorithms for computing such representations are found in [BOKR86,CR88].

In this chapter, we introduce a succinct representation for p-adic algebraic numbers. We show how to compute such succinct representations of roots of polynomials using symbolic p-adic versions of the well-known Newton and Horner numerical
iteration methods. One motivation for solving polynomial equations over the p-adics comes from *diophantine analysis*, [Lew69]. For instance, the *Hasse-Minkowski local-global principle* [Sil86,Cas86], asserts that a rational binary quadratic form has a rational zero iff it has a zero over $\mathbb{R}$, and over $\mathbb{Q}_p$ for every prime $p$, see Chapter 1.

The rest of this chapter is organized as follows. An efficient algorithmic version of a key technical fact about the p-adics called Hensel's lemma is presented in § 4.2. Here we also make an easy observation that gives a fast parallel algorithm for division in the p-adic numbers, which may be of independent interest. In § 4.3, we introduce a succinct representation for p-adic algebraic numbers, and in § 4.4, we describe a conceptually simple algorithm to compute such representations. This algorithm can be seen as a combination of p-adic versions of the classical Newton and Horner iterations for solving polynomial equations numerically. In § 4.5, we analyze the complexity of the algorithm. In the process we also give some (p-adic) bounds on the discriminant of a polynomial that may be of interest in themselves.

### 4.2 Zassenhaus Lifting in Residue Rings and Fast Parallel Division in the P-adics

The quadratically convergent Zassenhaus lifting algorithm is well-known in the context of lifting factorizations of polynomials over residue rings, [Zas69,Zas78, DST88]. It appears less known in the number-fields context, so we present the algorithm here.

**Algorithm 4.1** **INPUT:** A polynomial $f \in \mathbb{Z}[x]$ \footnote{Actually the algorithm will work for a polynomial with p-adic coefficients, but we consider integral coefficients for simplicity. There is nothing essentially different needed in the other case.}, $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(a_0) = 0$, $f'(a_0) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ and an integer $k \geq 2$.

**OUTPUT:** $\xi_k \in \mathbb{Z}/p^k\mathbb{Z}$ such that $f(\xi_k) = 0$ in $\mathbb{Z}/p^k\mathbb{Z}$ and $res_1(\xi_k) = a_0$. 
1. Set $\xi_0 := a_0$ and let $\beta_0$ be the multiplicative inverse of $f'(\xi_0)$ in $\mathbb{Z}/p\mathbb{Z}$. (At each stage, the multiplicative inverse of $f'(\xi_i)$ in the current residue ring will be maintained as $\beta_i$.) To start let $i := 0$.

2. Repeat the following lifting step for $\lfloor \log k \rfloor$ stages:

   (a) Compute $\zeta_i$ such that $f(\xi_i) = p^{2^i} \cdot \zeta_i$ and set $\Delta_i := -\beta_i \cdot \zeta_i$.

   (b) Compute $\eta_i$ such that $1 - \beta_i \cdot f'(\xi_i) = p^{2^i} \cdot \eta_i$ and set $\delta_i := -\beta_i \cdot \eta_i$.

   (c) Set $\xi_{i+1} := \xi_i + p^{2^i} \cdot \Delta_i$ and $\beta_{i+1} := \beta_i + p^{2^i} \cdot \delta_i$.

   (d) Set $i := i + 1$.

Essentially the algorithm interleaves a Newton iteration for a zero of $f$ with one for a multiplicative inverse of $f'$. Clearly each individual stage can be executed efficiently in parallel and so the whole algorithm is an $\mathcal{NC}$-algorithm.

In fact, the iteration for the inverse can be seen to yield a fast parallel algorithm for computing a multiplicative inverse in $\mathbb{Z}_p$ when possible, and we get an algorithmic version of a well known fact about the p-adic integers in the bargain:

**Proposition 4.2** A p-adic integer $\alpha := a_0 + a_1 p + \cdots$ is a unit in $\mathbb{Z}_p$ iff $a_0 \neq 0$. In that case, moreover, an inverse can be computed in $\mathcal{NC}$. Consequently, there is an $\mathcal{NC}$-algorithm for p-adic division.

### 4.3 Succinct Representations of p-adic Algebraic Numbers

While an arbitrary p-adic integer has an infinite-series representation, we give a succinct representation of algebraic p-adic integers. Attempts to secure a p-adic version of Thom's lemma by carrying over the formal analogies between $\mathbb{R}$ and $\mathbb{Q}_p$ in the obvious way do not seem to work. However we do obtain succinct representations via the following proposition (which is inspired by a property of connected sets in $\mathbb{R}$, namely that such sets are either empty, singletons or infinite).
Proposition 4.3 Let \( f \in \mathbb{Z}[x] \) and let \( \mathcal{V}(f, r) := \{ x \in \mathbb{Z}_p : v(f(x)) = \infty, v(f'(x)) = r \} \) for \( r \geq 0 \). Then for each basic open set, \( \mathcal{B}(\alpha, k) := \{ x \in \mathbb{Z}_p : v(x - \alpha) > k \}, \) \( k \geq r \), we have \( \mathcal{V}(f, r) \cap \mathcal{B}(\alpha, k) \) is either empty or a singleton.

Proof. Follows from Hensel's lemma. \( \square \)

In other words, a root \( \xi \) of a polynomial, \( f \) is uniquely determined by the pair \((r, \alpha)\), where \( r = v(f'(\xi)) \) and \( \alpha = res_r(\xi) \), and consequently, can be succinctly represented in that form. Actually, in order to be able to use the Zassenhaus lifting algorithm from the previous section, we will represent a root, \( \xi \) of \( f \) by the pair \((r, res_{2r+1}(\xi))\) where \( r = v(f'(\xi)) \).

Not every pair \((r, \alpha)\) where \( \alpha \in \mathbb{Z}/p^{2r+1}\mathbb{Z} \) represents a root, of course. To see if such a pair \((r, \alpha)\) in fact represents a root of \( f \), check if \( f(\alpha) = 0 \) in \( \mathbb{Z}/p^{2r+1}\mathbb{Z} \) and if so, whether \( res_r(\alpha) \) lifts up to \( \alpha \). By Hensel's lemma, it is clear that \((r, \alpha)\) represents a root \( \xi \) just if this is the case and that then, \( \alpha = res_{2r+1}(\xi) \).

4.4 Computing Roots of Polynomials in \( \mathbb{Z}_p \)

In this section we give a simple algorithm to find succinct representations for all roots of a given polynomial \( f \in \mathbb{Z}[x] \) in \( \mathbb{Z}_p \). The algorithm combines symbolic \( p \)-adic versions of Newton's Method and Horner’s method and has a natural parallel implementation.

Let \( f \in \mathbb{Z}[x] \) be given and suppose \( f(a_0) = 0 \) but \( f'(a_0) \neq 0 \) in \( \mathbb{Z}/p\mathbb{Z} \). Then by Hensel’s lemma it follows that \( a_0 \) lifts to a unique root \( \xi \in \mathbb{Z}_p \) and that the succinct representation for \( \xi \) is \((0, a_0)\).

If \( f(a_0) = 0 \) and \( f'(a_0) = 0 \) as well in \( \mathbb{Z}/p\mathbb{Z} \), then Hensel's lemma gives no information about whether \( a_0 \) can be lifted to a root. In this case we apply a Horner iteration. Define a polynomial \( F \) by

\[
p^s F(x) := f(a_0 + px) \text{ where } s \text{ is maximal}
\]
(This essentially corresponds to the Horner step: diminish the root by \( a_0 \) and scale by \( p \). The extraction of the power of \( p \) is for reasons that will become clear below; it does not affect the relationship between the roots of \( f \) and \( F' \).)

**Lemma 4.4** Let \( \xi, \xi' \in \mathbb{Z}_p \). Then, \( \xi \) is a root of \( f \) iff \( \xi = a_0 + p\xi' \) and \( \xi' \) is a root of \( F' \). Moreover, in that case, if \( (r, \alpha) \), and \( (r', \alpha') \) are the succinct representations of \( \xi \) and \( \xi' \) respectively, then \( r = r' + s - 1 \) and \( \alpha = res_{2r+1}(a_0 + p\xi') \) can be computed by lifting \( \alpha' \) to the ring \( \mathbb{Z}/p^k\mathbb{Z} \) for \( k = 2r - 1 \).

**Proof.** Observe that
\[
p^sF'(x) = pf'(a_0 + px)
\]
so
\[
p^sF'(\xi') = pf'(a_0 + p\xi')
\]
\[
= pf'(\xi)
\]
and hence
\[
v(f'(\xi)) = v(F'(\xi')) + s - 1
\]
The second part of the assertion now follows from Zassenhaus lifting. \( \square \)

This lemma allows us to synthesize the following straightforward algorithm to compute succinct representations of all roots of \( f \) in \( \mathbb{Z}_p \).

**Algorithm 4.5**

1. Compute all roots of \( f \) in \( \mathbb{Z}/p\mathbb{Z} \).

2. For a root \( a_0 \) such that \( f'(a_0) \neq 0 \), the unique corresponding root is represented by \( (0, a_0) \).

3. For a root \( a_0 \) such that \( f'(a_0) = 0 \), recursively compute the roots of \( F' \) where \( p^sF(x) := f(a_0 + px) \) with \( s \) maximal. For a root \( (r', \alpha') \) of \( F' \), the corresponding root of \( f \) is represented by \( (r, \alpha) \) where \( r := r' + s - 1 \), \( \alpha := a_0 + p\alpha'' \) and \( \alpha'' \) is obtained by lifting \( \alpha' \) to \( \mathbb{Z}/p^{2r}\mathbb{Z} \).
4.5 Complexity Analysis

To show that this algorithm actually terminates and to analyze its complexity we need to bound the number of Horner steps required before we arrive at a polynomial whose root we can compute by a single Newton step. We need the following preliminary lemma.

Lemma 4.6 Let $\mathcal{D}(f)$ denote the discriminant of $f$. If $v(f(\xi)) > 2v(\mathcal{D}(f))$, then $v(f'(\xi)) \leq v(\mathcal{D}(f))$.

Proof. See [Cas86] \Box

Now let $f_0 := f$, and given $f_i(i \geq 0)$ and $a_i \in \mathbb{Z}/p\mathbb{Z}$ such that $f_i(a_i) = 0 = f'(a_i)$ in $\mathbb{Z}/p\mathbb{Z}$, define $f_{i+1}$ by

$$p^{s_{i+1}} f_{i+1}(x) := f_i(a_i + px) \text{ where } s_{i+1} \text{ is maximal}$$

Lemma 4.7 For the sequences $f_i, s_i, i \geq 0$ as above, $s_i \geq 2$ for all $i > 0$.

Proof. First, from the Taylor expansion,

$$f_i(a_i + px) = f_i(a_i) + (px)f_i'(a_i) + \cdots$$

and the fact that $f_i(a_i) = 0 \pmod{p}$, it follows that $s_{i+1} \geq 1$. Now if $f_{i+1}(a_{i+1}) = 0 \pmod{p}$, then from

$$p^{s_{i+1}} f_{i+1}(a_{i+1}) = f_i(a_i + pa_{i+1})$$

it follows that $f_i(a_i + pa_{i+1}) = 0 \pmod{p^2}$. Finally, substituting $x := a_{i+1}$ in the first Taylor expansion shows that $f_i(a_i) = 0 \pmod{p^2}$. This, together with $f_i'(a_i) = 0 \pmod{p}$ shows that $s_{i+1} \geq 2$. \Box

Lemma 4.8 There is an $i_0 < v(\mathcal{D}(f))$ such that either $f_{i_0}(b) \neq 0$ for all $b \in \mathbb{Z}/p\mathbb{Z}$ or for each $b \in \mathbb{Z}/p\mathbb{Z}$ such that $f_{i_0}(b) = 0$, $f'_{i_0}(b) \neq 0$. 
Proof. Suppose otherwise; then one can define the sequence \( f_0, \ldots, f_k \) for some \( k \geq v(D(f)) \).

By induction it can be shown that for each \( i, 0 \leq i < k \),

\[
p^{s_1 + \cdots + s_{i+1}} f_{i+1}(x) = f(a_0 + \cdots + a_i p^i + p^{i+1}x)
\]

and so

\[
p^{(s_1 + \cdots + s_{i+1})-(i+1)} f_{i+1}'(x) = f'(a_0 + \cdots + a_i p^i + p^{i+1}x)
\]

If \( f_k(a_k) = 0 \pmod{p} \) for some \( a_k \in \mathbb{Z}/p\mathbb{Z} \), then

\[
f(a_0 + \cdots + a_k p^k) = 0 \pmod{p^{(s_1 + \cdots + s_k)+1}}
\]

and if \( f_k'(a_k) = 0 \pmod{p} \) also, then

\[
f'(a_0 + \cdots + a_k p^k) = 0 \pmod{p^{(s_1 + \cdots + s_k)-k+1}}
\]

Since \( k \geq v(D(f)) \), it follows from the previous lemma that \((s_1 + \cdots + s_k) + 1 > 2k \geq 2v(D(f))\) and \((s_1 + \cdots + s_k) - k + 1 > v(D(f))\). This contradicts lemma 4.6

\[\Box\]

We now wish to bound \( v(D(f)) \) from above. A rough estimate can be obtained via Mahler's inequality for the discriminant \(^2\):

**Proposition 4.9 (Mahler,[Mah64])** Let \( f := a_0 + \cdots + a_n x^n \). Then

\[
|D(f)| < n^n (|a_0| + \cdots + |a_n|)
\]

**Corollary 4.10** With \( f \) as above,

\[
v(D(f)) < n \log_p(n) + \log_p (a_0 + \cdots + a_n)
\]

With a view to giving more direct bounds, we now prove a few bounds on the valuations of roots and root-separations which may be of independent interest. Let

\[
f = a_0 + \cdots + a_n x^n = a_n \prod_{1 \leq i \leq n} (x - \xi_i)
\]

\(^2\)Thanks to Rich Zippel for pointing this out.
Proposition 4.11 For each $1 \leq i \leq n$,

$$v(\xi_i) \leq v(a_0/a_n) = v(a_0) - v(a_n)$$

Proof. We have for each $1 \leq i \leq n$,

$$v(\xi_i) \leq \sum_j v(\xi_j) = v(a_0/a_n)$$

□

Proposition 4.12 For any two distinct roots, $\xi_i, \xi_j$,

$$v(\xi_i - \xi_j) \leq \min\{v(f'(\xi_i)), v(f'(\xi_j))\}$$

Proof. From the Taylor expansion,

$$f(\xi_i) = f(\xi_j) + (\xi_i - \xi_j)f'(\xi_j) + (\xi_i - \xi_j)^2 g(\xi_j)$$

(where $g$ is an integral polynomial), it follows, using the ultra-metric inequality from Chapter 2, that $v(\xi_i - \xi_j) \leq v(f'(\xi_j))$. Interchanging $\xi_i, \xi_j$, the result follows. □

This proposition allows us to deduce a bound for $v(D(f))$.

Proposition 4.13 For a polynomial $f$ as above,

$$v(D(f)) \leq (2n - 1)v(a_n) + n(n - 1) \max_{1 \leq i \leq n} (v(f'(\alpha_i)))$$

Proof. Recall that

$$D(f) = a_n^{2n-1} \cdot (\prod_{i \neq j} (\alpha_i - \alpha_j))^2$$

and use the previous proposition. □

Another bound in a special case is the following:
Proposition 4.14 For $f$ as above, suppose

$$v(\alpha_1) < v(\alpha_2) < \cdots < v(\alpha_n)$$

Then

$$v(D(f)) \leq v(a_n) + 2n^2v(a_0/a_n)$$

Proof. This follows by noting that

$$v(\alpha_i - \alpha_j) = v(\alpha_i)$$

if $i < j$, by the ultametic inequality. □

Let us return to the equation corresponding to the Horner iteration:

$$p^{s_{i+1}} f_{i+1}(x) := f_i(a_i + px)$$

where $s_{i+1}$ is maximal $i \geq 0$

Lemma 4.15 Let $f = a_0 + \cdots + a_n \cdot x^n \in k[x]$, $a_n \neq 0$ for any field $k$ and let

$$F_1(x) := f(a + b \cdot x)$$

$a, b \in k$

Then $D(F_1) = D(f)$.

Proof. Observe that $\xi_i$ is a root of $f$ (in the algebraic closure of $k$) iff $\eta_i := a + b \cdot \xi$ is a root of $F$ for $1 \leq i \leq n$. Now noting that if the leading coefficient of $F_1$ is $a_n \cdot b^n$, we compute

$$D(F_1) = b^{n(2n-2)} \cdot a_n^{2n-2} \cdot \left[ \prod_{i \neq j} (\eta_i - \eta_j) \right]^2$$

$$= b^{n(2n-2)} \cdot a_n^{2n-2} \cdot b^{-2n(n-1)} \cdot \left[ \prod_{i \neq j} (\xi_i - \xi_j) \right]^2$$

$$= D(f)$$

□

Corollary 4.16 With the $f_i$ $i \geq 0$ as above,

$$D(f_{i+1}) \leq D(f_i) - (2n - 2)$$

$i \geq 0$
Proof. Recall that for each $i \geq 0$, we have $s_i \geq 2$ and observe that if $p^s \cdot F(x) := F_1(x)$, then $\mathcal{D}(F) = \mathcal{D}(F_1) - s$. □

Now using Lemma 4.6, the above corollary and the bound on $\mathcal{D}(v(f))$ in proposition 4.13, we get the following complexity result on Algorithm 4.5:

**Theorem 4.17** Algorithm 4.5 computes all $p$-adic integral roots of a polynomial. Given a polynomial of degree $n$ and whose coefficients are bounded (in terms of bit complexity) by $b$, it runs in sequential time $O(n \cdot p^b)$. It can be implemented to run in parallel time $O(\log n + b)$ with $O(n \cdot p^b)$ processors.

Unfortunately, none of these bounds is good enough to ensure polynomial sequential time or parallel polylog time. So although the algorithm is conceptually simple and easy to implement, at this point we can only prove its termination and bound its (sequential) complexity by an exponential. The algorithm is also naturally susceptible to parallelization, but again no good bounds are available at this point.

### 4.6 Arithmetic on $p$-adic Algebraic Numbers

In this section we describe algorithms to manipulate succinct representations of $p$-adic algebraic numbers in standard arithmetic operations. Assume $(r, \alpha)$ and $(s, \beta)$ are succinct representations for two $p$-adic algebraic numbers, $\xi$ and $\eta$ and suppose $f$ and $g$ are polynomials (in $\mathbb{Z}[x]$) such that $f(\xi) = 0 = g(\eta)$.

#### 4.6.1 Succinct representation for $-\xi$

If $\xi$ is a root of $f(x)$, then $-\xi$ is a root of $f_1(x) := f(-x)$. Further, $f'(-x) = -f'(x)$, and so $v(f_1(-\xi)) = v(f'(\xi)) = r$. So the succinct representation for $-\xi$ is $(r, -\alpha)$. 
4.6.2 Succinct representation for $\frac{1}{\xi}$

If $\xi \neq 0$, then $\frac{1}{\xi}$ is a root of the polynomial $f_1(x) := x^m \cdot f\left(\frac{1}{x}\right)$ where $m = \partial f$. Taking the derivative, we see that $v(f_1(\frac{1}{x})) = -(m - 2)v(\xi) + v(f'(\xi))$. Assume that $\xi$ is invertible in $\mathbb{Z}_p$, so that $v(\xi) = 0$, see Proposition 4.2. Then, $v(f_1(\frac{1}{x})) = r$ and by the algorithm of Proposition 4.2, we get a succinct representation for $\frac{1}{\xi}$.

4.6.3 Succinct representation for $u + \xi, u \cdot \xi$

It is easy to see that $u + \xi$, (where $u \in \mathbb{Z}$) is a root of the polynomial $f_1(x) := f(x - u)$. Since $f_1'(x) = f'(x)$, we get a succinct representation for $u + \xi$ by a simple addition of p-adic expansion.

It is also clear that $u \cdot \xi$ is a root of the polynomial $f_2(x) := u^m \cdot f(x/u)$. Taking derivatives, $v(f_2'(u \cdot \xi)) = (m - 1) \cdot v(u) + v(f'(\xi)) = (m - 1)v(u) + r$. So we first lift $\xi$ into the ring $\mathbb{Z}/p^k\mathbb{Z}$ where $k = (m - 1)v(u) + r$, then multiply by $u$ to get the succinct representation for $u \cdot \xi$.

4.6.4 Succinct representation for $\xi + \eta$

The polynomial $\text{Res}_y(f(x - y), g(y))$, namely the resultant with respect to $y$ of $f(x - y)$ and $g(y)$ has $\xi + \eta$ as one of its roots. By applying the algorithm of § 4.4, we can compute a succinct representation for $\xi + \eta$.

4.6.5 Succinct representation for $\xi \cdot \eta$

The polynomial $\text{Res}_y(y^m f(x/y), g(y))$ has $\xi \cdot \eta$ as one of its roots. By applying the algorithm of § 4.4, we can compute a succinct representation for $\xi \cdot \eta$.

4.7 Prospectus

We hope to significantly improve the complexity of the algorithm by finding a more efficient replacement of the Horner iterations (which dominate the cost of the above algorithm). The algorithms of [BOFKT88] and [Nef90] achieve performance
in the class $\mathcal{NC}$. In our case, the sequential Horner steps are the bottleneck. We would also like to extend the idea to multivariate polynomials.
Chapter 5

Towards a p-adic Sturm Theory

5.1 Introduction

The p-adic metric has quite different properties from the usual absolute value, [Kob84]. Naturally then, \( \mathbb{Q}_p \) has certain diametrically opposite topological and algebraic properties compared to \( \mathbb{R} \). Nevertheless, beginning with the pioneering work of Ax and Kochen, [AK65,AK66] and particularly after the introduction of the “n-th power” formalism by Macintyre [Mac76], we have witnessed some striking similarities between \( \mathbb{R} \) and \( \mathbb{Q}_p \), from model-theoretic [Mac76,Den86,Mac84], algebraic [PP84], and algebro-geometric angles[Rob87], see the summary in Chapter:padicprimer.

In [Rob87], [Den86] and in [SvdD88] we find the suggestion that in order to obtain the correct analogue of semi-algebraic geometry over the p-adics, one must replace signs by cosets of \( n^{th} \)-powers. In this chapter we add some more “elementary” evidence in favor of this suggestion. In § 5.2 we show how cosets of \( n^{th} \)-powers play a role in the p-adics similar to the role signs play for the reals, in particular in the behavior of polynomials and their derivatives. In § 5.3 we show how these concepts give short proofs of a result relating to quadratic extensions of \( \mathbb{Q}_p \), and a result about p-adic algebraic numbers.

For the reals, there is a beautiful “Sturm theory” that gives information on the
number of roots of a polynomial in an interval that satisfy certain sign-conditions
(this forms a key ingredient of some central algorithms in real (semi)-algebraic
geometry), [BOKR86,CR88]). Towards the end, in § 5.4 and in § 5.5 we make
some speculations on how a possible p-adic analog could be achieved; such a result
would be very fascinating indeed!

5.2 Signs versus Cosets

A key observation due to Edmund Robinson, [Rob87], is that the sets defined by
the $P_n$-predicates are well-behaved with respect to the underlying metric topology
induced by the valuation, in that they are “effectively open”.

**Proposition 5.1**  \( R \) Let \( x \in \mathbb{R}^* \). Then for all \( y \) in the open set, \( \{ w : |x - w| < |x| \} \), we have \( P_2(x) \leftrightarrow P_2(y) \).

\( p \) Let \( x \in \mathbb{Q}_p^* \) an \( n \geq 2 \). Then for all \( y \) in the open set, \( \{ w : |x - w|_p < p^{-2(v(x) + v_p(n))} \} \), we have, \( P_n(x) \leftrightarrow P_n(y) \).

**Proof.** The real part is obvious, the p-adic part follows from Hensel’s lemma.
\[ \square \]

We immediately make a few observations from this (that appear to have been
missed in the literature) which gives very simple but compelling evidence that the
nth power cosets behave analogously to signs:

**Corollary 5.2**  \( R \) Let \( x \in \mathbb{R}, x \neq 0 \). Then for all \( y \) in the open set, \( \{ w : |x - w| < |x| \} \), we have, \( sgn(w) = sgn(x) \).

\( p \) Let \( x \in \mathbb{Q}_p, x \neq 0 \) and \( n \geq 2 \). Then for all \( y \) in the open set, \( \{ w : |x - w|_p < p^{-(v(x)) + 2v_p(n)} \} \), \( coset_n(y) = coset_n(x) \).

**Proof.** Apply the previous proposition to \( x p^{-1} \), where \( coset_n(x) = coset_n(\rho) \).
\[ \square \]
The first part of this corollary is the familiar fact that for a nonzero real $x$, all points sufficiently close to it have the same sign as $x$. The second part is the $p$-adic analogue of this statement.

For a continuous function, $f$, this implies:

**Proposition 5.3**  \( R \) Let $x \in \mathbb{R}, f(x) \neq 0$. Then in all sufficiently small neighborhoods around $x$, $f$ takes the same sign as $f(x)$.

\( p \) Let $x \in \mathbb{Q}_p, f(x) \neq 0$. Then in all sufficiently small neighborhoods around $x$, $f$ takes values in the same coset as $f(x)$.

What about neighborhoods of zero?

**Proposition 5.4**  \( R \) In all neighborhoods of 0, there are points taking both signs.

\( p \) In all neighborhoods of 0, there are points belonging to each coset of $n$th powers for each $n \geq 2$.

Proof. Simply observe that by taking $\rho' := \rho \cdot p^{kn}$ for a sufficiently large $k$, we obtain an element belonging to the same coset as $\rho$, but with arbitrarily small norm. \( \Box \)

For differentiable $f$, the values of $f$ in a neighborhood of a zero lie in a coset determined by that of the first non-zero derivative and that of the arbitrarily small increment:

**Proposition 5.5** Let $f$ be differentiable $n$ times and suppose $f^n(\xi) \neq 0$ while $f^i(\xi) = 0$ for all $i < n$. (In particular $\xi$ is a zero of $f$.)

\( R \) For all sufficiently small $\epsilon$, we have

$$\text{sgn}(f(\xi + \epsilon)) = (\text{sgn}(\epsilon)^n) \cdot \text{sgn}(f^n(\xi))$$

In particular, if $f'(\xi) \neq 0$, then

$$\text{sgn}(f(\xi + \epsilon)) = \text{sgn}(\epsilon) \cdot \text{sgn}(f'(\xi))$$
p. Let \( m \geq 2 \). For all \( \epsilon \) such that \( |\epsilon| < p^{-2(v(f^n(\xi)) + v(m))} \), we have

\[
coset_m(f(\xi + \epsilon)) = (coset_m(\epsilon))^n \cdot coset_m(f^n(\xi))
\]

In particular if \( f'(\xi) \neq 0 \), then

\[
coset_m(f(\xi + \epsilon)) = coset_m(\epsilon) \cdot coset_m(f'(\xi))
\]

Proof. The real part follows by taking a one-term approximation of the Taylor series for \( f \). For the p-adic case we have from the Taylor expansion,

\[
f(\xi + \epsilon) = f(\xi) + \epsilon f'(\xi) + \cdots
\]

\[
= \epsilon^n (f^n(\xi) + \epsilon f^{n+1}(\xi) + \cdots)
\]

Now,

\[
|\epsilon f^{n+1}(\xi) + \cdots| \leq |\epsilon| < p^{-2(v(f^n(\xi)) + v(n))}
\]

and so,

\[
coset(f^n(\xi) + \epsilon f^{n+1}(\xi) + \cdots) = coset(f^n(\xi))
\]

So finally,

\[
coset(f(\xi + \epsilon)) = (coset(\epsilon))^n \cdot coset(f^n(\xi)).
\]

\[\square\]

5.3 Applications

We give a short proof of Mahler’s “Main Lemma”, [Mah81], p.71, used to study quadratic extension fields of \( \mathbb{Q}_p \).

Proposition 5.6 Let \( S_p \) be the set of p-adic numbers \( \Delta \) satisfying

\[
|\Delta - 1|_p \leq \begin{cases} 
1/8 & \text{if } p = 2 \\
1/p & \text{if } p \geq 3 
\end{cases}
\]

Then for all \( \Delta \in S_p \), we have \( P_2(\Delta) \), that is, \( S_p \subseteq \mathbb{Q}_p^2 \).
Proof. Simply observe that 1 is a square and use Robinson’s lemma, noting that $2(v_2(2) + v_2(1)) < 3$ in the first case and $2(v_p(2) + v_p(1)) < 1$ in the second. □

For the reals, the remarkable Thom’s lemma [Dic85], gives a coding of real algebraic numbers via certain sign sequences, [CR88]. We have a partial p-adic analogue which we list along with the classical version for the reals.

**Proposition 5.7** Let $f$ be a polynomial of degree $n$, and suppose $f(\alpha) = 0 = f(\beta)$. Let $f^{(1)}, \ldots, f^{(n)}$ be the successive derivatives of $f$.

$R$ If $\text{sgn}(f'(\alpha)) = \text{sgn}(f'(\beta)), \ldots, \text{sgn}(f^n(\alpha)) = \text{sgn}(f^n(\beta))$, then $\alpha = \beta$.

$p$ If $coset_m(f^{n-1}(\alpha)) = coset_m(f^{n-1}(\beta))$ for all $m \geq 2$, then $\alpha = \beta$.

Proof. For the real part, see [Dic85,CR88]. For the p-adic statement, we have

$$f^{n-1}(\beta) = f^{n-1}(\alpha) + (\beta - \alpha)f^n(\alpha)$$

However, if $coset_m(f^{n-1}(\alpha)) = coset_m(f^{n-1}(\beta))$ for all $m \geq 2$, then $f^{n-1}(\alpha) = f^{n-1}(\beta)$, [Mac76]. Since $f^n$ is a non-zero constant, $\alpha = \beta$. □

### 5.4 Euclidean Sequences and Cosets

Our goal is to eventually obtain a p-adic version of Sturm’s theorem. A reason to believe this is possible comes from the behavior of the nth power cosets with respect to the standard Euclidean remainder sequence:

**Proposition 5.8** Let $f = f_0, f_1, \ldots, f_n$ be the Euclidean remainder sequence for a polynomial $f$.

$R$ (a) For sufficiently small $\epsilon$, $\text{sgn}(f_0(\xi - \epsilon)/f_1(\xi - \epsilon)) = -1$ and $\text{sgn}(f_0(\xi + \epsilon)/f_1(\xi + \epsilon)) = +1$, where $f(\xi) = 0$. That is, $\text{sgn}(f/f')$ changes sign from -1 to +1 as one passes through a root, $\xi$ of $f$, from $\xi - \epsilon$ to $\xi + \epsilon$. 
(b) Let \( 0 < i < n \) and let \( f_i(\xi) = 0 \). For sufficiently small \( \epsilon \), \( sgn(f_{i-1}(\xi \pm \epsilon)) = -sgn(f_{i+1}(\xi \pm \epsilon)). \)

(c) \( f_n \) has constant sign.

\( p \)

(a) For a fixed \( n \), let \( \epsilon_i \) be sufficiently small coset representatives ranging over all cosets. Then \( \text{coset}_n(f_0(\xi + \epsilon_k)/f_1(\xi + \epsilon_k)) = \text{coset}_n(\epsilon_k), \) where \( f(\xi) = 0 \). That is, \( \text{coset}_n(f/f') \) changes cosets from that of \( \epsilon_i \) to that of \( \epsilon_j \) as we pass through a root \( \xi \) of \( f \) from \( \xi + \epsilon_i \) to \( \xi + \epsilon_j \).

(b) Let \( 0 < i < n \) and let \( f_i(\xi) = 0 \). For sufficiently small \( \epsilon \), \( \text{coset}_n(f_{i-1}(\xi + \epsilon) = \text{coset}_n(-1) * \text{coset}_n(f_{i+1}(\xi + \epsilon)). \)

(c) \( f_n \) has constant coset representative.

5.5 Speculations towards a \( p \)-adic Sturm Theory

To this end, we would like to define a function \( v \) on "balls" of the form \( B = B(\alpha, r) := \{ x : \vert x - \alpha \vert_p < p^{-r} \} \), that is additive on balls and for all sufficiently small balls, satisfies:

\[
v(B) = \begin{cases} 
0 & \text{if } B \text{ has no zeroes} \\
1 & \text{if } B \text{ has exactly 1 zero.}
\end{cases}
\]

Proposition 5.8 suggests this is possible. However, while in the real case such a function, namely the difference in the sign variation count at the endpoints, is defined taking into account points obtained by adding to the center, two appropriate coset representatives, in the \( p \)-adic case one should consider points obtained by adding to the center, appropriate representatives of all cosets.
As a preliminary, consider the converse to Proposition 5.3 in the real case – the useful \textit{intermediate value theorem}:

**Proposition 5.9 (Intermediate Value Theorem)** Let $f$ be continuous.

\textbf{R} If $f$ takes on both signs in an interval $a \leq x \leq b$, then $f$ has a zero, $\xi$ in the interval.

We would like a $p$-adic analogue to this. However at the moment, we can only show that a weaker version of the intermediate value property implies this stronger statement. We conjecture that this weaker statement and hence, the stronger one hold for the $p$-adics.

**Proposition 5.10** The weak version of the intermediate value property for the $p$-adics implies the strong version:

\textbf{Weak} If $f$ takes values in two different cosets over all $Q_p$, then $f$ has a zero somewhere in $Q_p$.

\textbf{Strong} If $f$ takes values in two cosets in an interval, $\{x : v(x - \alpha) > s\}$, then $f$ has a zero $\xi$ in the interval.

\textit{Proof.} Define

$$g(x) := f(\alpha + p^s x).$$

Then a zero of $g$ corresponds to a zero of $f$ in the given interval; so the weak statement applied to $g$ yields the strong one for $f$. $\square$
Chapter 6

Conclusions and Future Directions

6.1 Conclusions

In this thesis, we have resolved the precise computational complexity of the Decision Problem for Fields in the p-adic case. This is the first quantitative result on the complexity of the decision problem for the full theory of $\mathbb{Q}_p$ although it was first shown to be decidable by Ax, Kochen and Ersöv in the mid 1960’s, and subsequently investigated by many authors.

First we gave an alternating exponential time algorithm for deciding linear sentences in the theory of p-adically closed fields. This also translates into a deterministic algorithm running in exponential space or double exponential time. A deterministic quantifier-elimination procedure for the linear fragment running in double exponential time and space was also presented. Next we employed a quantitative version of a Cell Decomposition Lemma due to Denef to give an alternating exponential time decision procedure for the full theory. As usual this also yields a deterministic decision procedure running in double exponential time or in exponential space, and a quantifier elimination procedure running in double
exponential time and space. These complexity bounds were demonstrated to be essentially optimal by proving matching lower bounds on the respective problems.

Next we gave a simple algorithm to determine all roots among the $p$-adic integers of a given polynomial equation. This algorithm was a purely symbolic (as opposed to numerical) $p$-adic version of the classical Newton and Horner iteration methods and has a natural parallel implementation. We also described algorithms for some problems in valued fields and in $p$-adic semi-algebraic geometry.

Finally we gave some additional elementary evidence to support the thesis that certain cosets of $n$th powers are the proper $p$-adic analogues to signs in the real case. This was done by showing that these coset representatives display similar behavior with respect to functions and their derivatives as do the signs in the real case. We also made some speculative remarks about a possible approach to a "$p$-adic Sturm Theory".

### 6.2 Future Directions

We were able to prove the termination of the algorithm in Chapter 4 but we gave only an exponential bound on the running time of the algorithm. We conjecture that the algorithm can be made to run in polynomial sequential time or in parallel polylogarithmic time.

The speculative remarks in Chapter 5 opened up an intriguing possibility for a $p$-adic version of Sturm Theory. It would be truly wonderful if a precise result could be established enabling one to count roots of a polynomial in a given interval in terms of variations of cosets or something along those lines. One could then even hope to obtain completely different algorithms for the decision problem as with the Ben-Or-Kozen-Reif algorithm for the reals.
Bibliography


