P-ADIC GIBBS MEASURES ON CAYLEY TREES AND RELATED *P*-ADIC DYNAMICAL SYSTEMS

BY

MOHD ALI KHAMEINI BIN AHMAD

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy (Computational and Thereotical Sciences)

Kulliyyah of Science
International Islamic University Malaysia

SEPTEMBER 2019

ABSTRACT

This thesis is devoted to the study of the q-state Potts model over $\mathbb{Q}_p$ on Cayley trees. Specifically, we investigate the p-adic Gibbs measures of the Potts model on the Cayley trees of orders 3 and 4 and their related p-adic dynamical systems. In the first part, we describe the existence of the translation-invariant p-adic Gibbs measures of the Potts model on the Cayley tree of order 4. The existence of translation-invariant p-adic Gibbs measures is equivalent to the existence of fixed points of a rational map called Potts–Bethe mapping. The Potts–Bethe mapping is derived from the recurrent equation of a $\mathbb{Q}_p^q$-valued function in the construction of the p-adic Gibbs measures of the Potts model on Cayley trees. In order to describe the existence of these translation-invariant p-adic Gibbs measures, we find the solutions of some quartic equation in some domains $\mathcal{E}_p \subset \mathbb{Q}_p$. In general, we also provide some solvability conditions for the depressed quartic equation over $\mathbb{Q}_p$. In the second part, we study the dynamics of the Potts–Bethe mapping of degrees 3 and 4. First, we describe the Potts–Bethe mapping having good reduction. For a Potts–Bethe mapping with good reduction, the projective line $P^1(\mathbb{Q}_p)$ can be decomposed into minimal components and their attracting basins. However, the Potts–Bethe mapping associated to the Potts model on the Cayley trees of orders 3 and 4 have bad reduction. For many prime numbers p, such Potts–Bethe mappings are chaotic. In fact, for these primes p, we prove that restricted to their Julia sets, the Potts–Bethe mappings are topologically conjugate to the full shift dynamics. For other primes p, restricted to their Julia sets, the Potts–Bethe mappings are not topologically conjugate to the full shift dynamics. The chaotic property of the Potts-Bethe mapping implies the vastness of the set of the p-adic Gibbs measures, and hence implies the phase transition. As application, for many prime numbers p, the Potts models over $\mathbb{Q}_p$ on the Cayley trees of orders 3 and 4 have phase transition. We also remark the statement that phase transition implies chaos is not true.

خلاصة البحث

تم تكريس هذا البحث لدراسة q-state لنموذج بوتس على $\mathbb{Q}_p$ على أشجار كايلي. قمنا تحديدا بالتحقيق في p-adic لحسابات جيبس لنموذج بوتس على أشجار كايلي من الرتبة 3 و 4 والأنظمة الديناميكية لـــــ p-adic المتعلقة. قمنا في الجزء الأول بوصف وجود الترجمة–الثابتة لـــــ p-adic لحسابات جيبس لنموذج بوتس على أشجار كايلي من الرتبة 4. وجود الترجمة–الثابتة لـــــ p-adic لحسابات جيبس يعادل وجود نقاط محددة على الخريطة المنطقية المسماة بتخطيط بوتس و بيث. تم اشتقاق تخطيط بوتس و بيث من المعادلة التكرارية للدالة المقدرة بـــــ $\mathbb{Q}_p^q$ في بناء p-adic لحسابات جيبس لنموذج بوتس على أشجار كايلي. من أجل توصيف وجود الترجمة–الثابتة لـــــ p-adic لحسابات جيبس قمنا بالبحث عن حلول بعض المعادلات من الدرجة الرابعة في بعض مجالات $\mathcal{E}_p \subset \mathbb{Q}_p$. أعطينا بشكل عام بعض شروط قابلية الحل لمعادلات الدرجة الرابعة على $\mathbb{Q}_p$. قمنا في الجزء الثاني من البحث بدراسة ديناميكيات تخطيط بوتس و بيث للدرجة 3 و 4. تم توصيف تخطيط بوتس و بيث على احتوائها على تخفيض جيد .حتى يكون لتخطيط بوتس و بيث تخفيض جيد، بإمكان الخط الإسقاطي $\boldsymbol{P}^1(\mathbb{Q}_p)$ أن يحلل إلى أجزاء صغيرة وأحواضها الجاذبة. على الرغم من ذلك فقد كان لدى تخطيط بوتس و بيث لنموذج بوتس على أشجار كايلي من الرتبة 3 و 4 تخفيضا سيئا. لكل رقم أولي p ، كان تخطيط تخطيط بوتس و بيث سيئا، وفي الواقع هذه الأرقام الأولية p، محدودة لجموعات جوليا الخاصة بها، كانت تخطيطات بوتس و بيث مترافقة طبوغرافيا لديناميكيات التحول الكامل. أما بالنسبة للأرقام الأولية p فقد تكون مجموعات جوليا الخاصة بها خالية. تدل الخاصية الفوضوية لتخطيطات بوتس و بيث على وسع مجموعات p-adic لحسابات جيبس، وبالتالي تدل على الانتقالية الطورية. أما بالنسبة للتطبيقات، فكان للعديد من الأرقام الأولية p لنماذج بوتس على $\mathbb{Q}_p$ على أشجار كايلي من الرتبة 3 و 4 انتقالا طوريا، ونلاحظ أيضًا أن التعبير بأن الانتقال الطوري يدل على الفوضوية ليس صحيحا.

APPROVAL PAGE

The thesis of Mohd Ali Khameini Bin Ahmad has been approved by the following:

Pah Chin Hee
Supervisor

Mansoor Saburov
Co-supervisor

Arnaud Le Ny
Co-supervisor

Lingmin Liao
Co-supervisor

Abdumalik Rakhimov
Internal Examiner

Utkir Rozikov
External Examiner

Mohd Salmi Md Noorani
External Examiner

Jamalludin Ab. Rahman
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Mohd Ali Khameini Bin Ahmad

Signature .... Date ....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

***P*-ADIC GIBBS MEASURES ON CAYLEY TREES AND RELATED *P*-ADIC DYNAMICAL SYSTEMS**

I declare that the copyright holders of this thesis is jointly owned by Mohd Ali Khameini Bin Ahmad and IIUM.

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Mohd Ali Khameini Bin Ahmad

……..…………………….. ……………………….

Signature Date

ACKNOWLEDGEMENTS

To start with The Name of Allah, The Most Beneficent, The Most Merciful. The Perfect Praise to Allah, I am able to finish my degree in PhD. There are no other powers giving me the directions, patience and guidance in order to finish this thesis. In addition, may blessing and peace be upon Prophet Muhammad who was sent for mercy to the world.

A special thanks goes to my supervisors Arnaud Le Ny, Pah Chin Hee, Mansoor Saburov and Lingmin Liao for their full commitment in guiding me during the completion of this thesis. My discussion with Arnaud Le Ny really opens up my view on my research area. Meanwhile, Mansoor Saburov always encourage me during the completion of this thesis. He has always remind me to continue working hard especially in mathematics. On the other hand, I am really thankful to have Lingmin Liao as my supervisor. During my stay in France, he is always there to guide me, both in life and mathematics.

I am thankful to the examiners of my thesis, Utkir Rozikov, Mohd Salmi Md Noorani and Abdumalik Rakhimov, for their thorough reading of my thesis. Their unusually careful readings and thoughtful suggestions have resulted in improvements in this thesis. Not forget to Ai-Hua Fan and Teo Lee Peng for their good assessement and sharing during my thesis's defense. I am indebted to the Embassy of France in Malaysia and Labex Bézout for their financial support. Their support really ease me during my one and the half year staying in France. Moreover, I am also extremely acknowledge the financial support from Pah Chin Hee by MOHE Fundamental Research Grant Scheme FRGS17-027-0593 for my remaining one and the half year of my study in Malaysia.

On top of that, I am grateful especially to my beloved wife, Nur Atikah Binti Yusof for her understanding and support in many ways to finish this thesis. I am also grateful to my parents, Khadijah Binti Halim and Ahmad Bin Katimon, for their prayers and support. Last but not least, this thesis would not be impossible without the help of my friends. Thanks are also due to all people who have been involved in one way or another. Lastly, I want to make an apology to my parents and my wife for my absence in these past years.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 RESEARCH BACKGROUND

A p-adic-valued theory of probability – a non-Kolmogorov model in which probabilities take values in the field of p-adic numbers – was proposed in a series of papers by Khrennikov (1990a,b, 1991, 1992a,b, 1993, 1996a,b) and Khrennikov et al. (1999) in order to resolve the problem of the statistical interpretation of p-adic-valued wave functions in non-Archimedean quantum physics (Beltrametti & Cassinelli, 1972, Vladimirov et al., 1994, Volovich, 1987, Albeverio et al., 2010, Khrennikov, 1994, 2009). Moreover, in order to formalize the measure-theoretic approach for p-adic probability theory, Ilic-Stepic et al. (2016) developed several p-adic probability logics which are sound, complete and decidable extensions of the classical propositional logic.

In fact, a p-adic probability is defined as the limit of relative frequencies in the p-adic topology. Then the measure-theoretical aspects of the p-adic probability theory can be established. After that, the theory of stochastic processes with values in p-adic and more general non-Archimedean fields having (non-Kolmogorov) probability distributions with non-Archimedean values has been extensively developed and various kinds of limits theorems for p-adic-valued processes have been obtained. On the other hand, applications of p-adic functional and harmonic analysis have also shown up in theoretical physics and quantum mechanics (Albeverio et al., 1997a,b,c 2009, 2010, Dragovich et al., 2009). For summary, all recent developments on p-adic mathematical physics can be found in an article by Dragovich et al. (2017).

Gibbs measures which play a central role in statistical mechanics take its origin from Boltzmann and Gibbs who introduced a statistical approach to thermodynamics to deduce collective macroscopic behaviors from individual microscopic information. Gibbs measures associated to the Hamiltonian of a physical system generalize the notion of a canonical ensemble. In the classical case of the statistical mechanics where the mathematical model was prescribed over the field of real numbers, the physical phenomenon of phase transition is reflected by the non-uniqueness of the Gibbs measures. Thus one central problem in the study of Gibbs measures is to determine the size of the set of Gibbs measures.

Due to the convex structure of the set of Gibbs measures over the field of real numbers, in order to determine the size of the set of Gibbs measures, it suffices to study the number of its extremal elements. Hence, in the classical case, to predict a phase transition, the main attention was paid to finding all possible extremal Gibbs measures (Georgii, 2011). However, it turns out that finding all extremal Gibbs measures for spin models, even for the Ising spin model on trees is a hard and not fully solved problem (Gandolfo et al., 2012, Gandolfo et al, 2017).

The study of Gibbs measures for the Potts models on Cayley trees attracts much attention (Kulske et al., 2013, Rozikov & Khakimov, 2013, Gandalfo et al., 2017). The classical method to characterize Gibbs measures on Cayley trees, founded by Preston (1974) and Spitzer (1975), is the Markov random field theory and its recurrence equations. However, the modern theory of Gibbs measures on Cayley trees also uses group theory, information flows, node-weighted random walks, contour methods and nonlinear analysis. The recent development of the theory of Gibbs measures on Cayley trees can be found in the book by Rozikov (2013).

Mezard et al. (1987) found that the structure of correlation functions for spin glasses model are related to ultrametricity. This result thus leads us to study the statistical mechanics by using p-adic numbers. In these past decades, the p-adic counterpart of the theory of Gibbs measures on Cayley trees is actively studied. The p-adic Gibbs measures which are important subjects in the p-adic probability theory, present natural concrete examples of p-adic-valued processes (Mukhamedov, 2013, Ludkovsky & Khrennikov, 2003). The study of p-adic Gibbs measures on Cayley trees has been initiated by Ganikhodjaev et al. (1998) and Mukhamedov & Rozikov (2004, 2005). Mukhamedov (2013), Mukhamedov & Akin (2013), Mukhamedov et al. (2015) and Rozikov & Khakimov (2013) have established the existence of p-adic Gibbs measures as well as the phase transition for some lattice models. We stress that in the p-adic case, due to the lack of a convex structure of the set of p-adic Gibbs measures, it is quite difficult to predict a phase transition with some features of the set of p-adic Gibbs measures.

The set of p-adic Gibbs measures of the Potts models on Cayley trees is strongly tied up with a Diophantine problem, i.e. to find all solutions of a system of polynomial equations or to give a bound for the number of solutions over the field $\mathbb{Q}_p$ of p-adic numbers. Rozikov & Khakimov (2015) and Saburov & Ahmad (2015b) describe the existence of all translation-invariant p-adic Gibbs measures of the q-state Potts model on the Cayley trees of order two and three by studying the quadratic and cubic equation over the field of p-adic numbers respectively. In general, the same Diophantine problem may have different solutions from the field of p-adic numbers to the field of real numbers because of the different topological structures. The rise of the order of the Cayley tree makes it difficult to study the corresponding Diophantine problem over the field of p-adic numbers. Recently, this problem was answered for monomial equations (Mukhamedov & Saburov, 2013), quadratic equations (Saburov & Ahmad, 2015c), and depressed cubic equations for primes $p > 3$ (Mukhamedov et al., 2013, 2014).

1.2 RESEARCH OBJECTIVES

The objectives of this research are

i. to describe the existence of the translation-invariant p-adic Gibbs measures of the Potts model on the Cayley tree of order 3 and order 4.

ii. to study the dynamics of the Potts–Bethe mapping of degree 3 and degree 4 over $\mathbb{Q}_p$.

iii. to show the relation between the chaotic property of the Potts–Bethe mapping over $\mathbb{Q}_p$ and the phase transition of the Potts model over $\mathbb{Q}_p$ on the Cayley trees.

1.3 OVERVIEW OF THE THESIS

This thesis contains five chapters. In Chapter One, we give the research background and the overview of the thesis. In Chapter Two, we provide the preliminaries on p-adic numbers, polynomials, Cayley trees, p-adic probability measures (Potts model over the field $\mathbb{Q}_p$ of p-adic numbers) and the related dynamical systems.

In Chapter Three, we study the existence translation-invariant p-adic Gibbs measures of the q-state Potts model on the Cayley tree of order 4. To show the existence of translation-invariant p-adic Gibbs measures, we solve the following system of equations

$$z_i = \left(\frac{(\theta - 1)z_i + \sum_{\ell=1}^{q-1} z_\ell + 1}{\theta + \sum_{\ell=1}^{q-1} z_\ell}\right)^4 \quad \text{for} \quad 1 \le i \le q-1$$

where $\theta = \exp_p(J)$ and J is a coupling constant. We find the solution of this system of equations of the form $\mathbf{z} = (z_1, \cdots, z_{q-1})$ such that $z_i = 1$ or $z_i = z^* \in \mathcal{E}_p \subset \mathbb{Q}_p$ for $i = \overline{1, q-1}$ with z^* being the fixed points, i.e. $z^* = f(z^*)$ of the following map f

$$f(z) = \left(\frac{(\theta - 1 + m)z + q - m}{mz + \theta - 1 + q - m}\right)^4$$

called "Potts–Bethe mapping". We note that f satisfies $f(1) = 1$ and has the form $\left(\frac{ax+b}{cx+d}\right)^k$. To find the fixed points of f other than 1, we desribe some quartic equation having a solution $z \in \mathcal{E}_p$ (Propositions 3.2.1 and 3.2.2). This descriptions allows us to prove the non-uniqueness of the translation-invariant p-adic Gibbs measures (Theorem 3.2.3). In general, we also provide some conditions for the depressed quartic equation

$$x^4 + ax^2 + bx + c = 0$$

where $a, b, c \in \mathbb{Q}_p$ to have a solution in $\mathbb{Q}_p$ in terms of its coefficients (Theorem 3.3.8).

In Chapter Four, we study the dynamics of the Potts–Bethe mapping on $\mathbb{Q}_p$. First, we describe the Potts–Bethe mapping having good reduction (Proposition 4.2.1) and show that its dynamics is decomposed into minimal subsystems and their attracting basins (Theorem 4.2.2). Then we study separately the dynamics of the Potts–Bethe mapping of degree 3 and of degree 4 which has bad reduction. We consider the following Potts–Bethe mapping of degree 3

$$f_{\theta,q,3}(x) = \left(\frac{\theta x + q - 1}{x + \theta + q - 2}\right)^3.$$

We distinguish two cases: $0 < |\theta - 1|_p < |q|_p < 1$ and $0 < |q|_p < |\theta - 1|_p < 1$.

Case $0 < |\theta - 1|_p < |q|_p < 1$: When $p \equiv 5 \pmod 6$, we find the attracting basin $\mathfrak{B}(\mathbf{x}^{(0)})$ of the fixed point $\mathbf{x}^{(0)} = 1$ (Theorem 4.3.8) as follows

$$\mathfrak{B}(\mathbf{x}^{(0)}) = \mathbb{Q}_p \backslash \left(\{\mathbf{x}^{(1)}\} \cup \bigcup_{n=0}^{\infty} f_{\theta,q,3}^{-n}\{\mathbf{x}^{(\infty)}\} \right)$$

where $\mathbf{x}^{(\infty)} = 2 - \theta - q$ and $\mathbf{x}^{(1)}$ is the repelling fixed point. When $p \equiv 1 \pmod 6$, the Julia set $\mathcal{J}$ of the Potts–Bethe mapping is non-empty. We divide into two subcases: $0 < |\theta - 1|_p < |q|_p^2 < 1$ and $0 < |q|_p^2 \leq |\theta - 1|_p < |q|_p < 1$. For $0 < |\theta - 1|_p < |q|_p^2 < 1$, there exists a subsystem $(\mathcal{J}, f_{\theta,q,3})$ that is isometrically conjugate to the full shift dynamics on 3 symbols (Theorem 4.3.13). For $0 < |q|_p^2 \leq |\theta - 1|_p < |q|_p < 1$, there exists a subsystem $(\mathcal{J}, f_{\theta,q,3})$ that is isometrically conjugate to a subshift of finite type on r symbols where $r \geq 4$. However, these subshifts on r symbols are all topologically conjugate to the full shift on 3 symbols (Theorem 4.3.19). In both case, we have the following decomposition

$$\mathbb{Q}_p = \mathfrak{B}(\mathbf{x}^{(0)}) \cup \mathcal{J} \cup \bigcup_{n=0}^{+\infty} f_{\theta,q,3}^{-n}\{\mathbf{x}^{(\infty)}\}$$

where $\mathbf{x}^{(\infty)} = 2 - \theta - q$ and $\mathfrak{B}(\mathbf{x}^{(0)})$ is the attracting basin of the attracting fixed point $\mathbf{x}^{(0)}$.

Case $0 < |q|_p < |\theta - 1|_p < 1$: In this case we find the Siegel disks of the neutral fixed points $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(1)}$ (Theorem 4.3.27). When $p \equiv 5 \pmod 6$, in certain case, we calculate the attracting periodic orbits or Siegel disk of periodic orbits and their basins. When $p \equiv 1 \pmod 6$, the Julia set $\mathcal{J}$ of the Potts–Bethe mapping is non-empty. There exists a subsystem $(\mathcal{J}, f_{\theta,q,3})$ that is isometrically conjugate to the full shift dynamics on 2 symbols (Theorem 4.3.29).

Next we consider the following the Potts–Bethe mapping of degree 4

$$f_{\theta,q,4}(x) = \left(\frac{\theta x + q - 1}{x + \theta + q - 2}\right)^4.$$

Similar to the Potts–Bethe mapping of degree 3, we consider two case: $0 < |\theta - 1|_p < |q|_p < 1$ and $0 < |q|_p < |\theta - 1|_p < 1$.

Case $0 < |\theta - 1|_p < |q|_p < 1$: In this case the Julia set $\mathcal{J}$ is non-empty. When $p \equiv 3 \pmod 4$, there exists a subsystem $(\mathcal{J}, f_{\theta,q,4})$ that is topologically conjugate to the full shift dynamics on 2 symbols (Theorem 4.4.9). Whereas when $p \equiv 1 \pmod 4$, there exists a subsystem $(\mathcal{J}, f_{\theta,q,4})$ that is topologically conjugate to the full shift dynamics on 4 symbols (Theorem 4.4.9). In both case, we have the following decomposition

$$\mathbb{Q}_p = \mathfrak{B}\big(\mathbf{x}^{(0)}\big) \cup \mathcal{J} \cup \bigcup_{n=0}^{+\infty} f_{\theta,q,3}^{-n}\{\mathbf{x}^{(\infty)}\}$$

where $\mathbf{x}^{(\infty)} = 2 - \theta - q$ and $\mathfrak{B}\big(\mathbf{x}^{(0)}\big)$ is the attracting basin of the attracting fixed point $\mathbf{x}^{(0)}$.

Case $0 < |q|_p < |\theta - 1|_p < 1$: We calculate the Siegel disks of neutral fixed points $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(1)}$ (Theorem 4.4.17). When $p \equiv 3 \pmod 4$, in certain case, we find the attracting periodic orbits and/ or Siegel disk of periodic orbits and their basins. When $p \equiv 1 \pmod 4$, the corresponding Julia set $\mathcal{J}$ is non-empty. We obtain a subsystem $(\mathcal{J}, f_{\theta,q,4})$ that is isometrically conjugate to the full shift dynamics on 3 symbols (Theorem 4.4.17).

Then we show for many prime numbers p, the Potts–Bethe mapping has chaotic properties. These chaotic properties of the Potts-Bethe mapping implies the vastness of the set of the p-adic Gibbs measures (Theorems 4.5.1 and 4.5.2). As application, for many prime numbers p, the phase transition occurs for the Potts models over $\mathbb{Q}_p$ on the Cayley trees of orders 3 and 4. We also remark that the statement phase transition implies chaos is not true, in the last part of Section 4.5.

In Chapter Five, we give the summary of this thesis and suggestion for the future research.

CHAPTER TWO

PRELIMINARIES

2.1 *P*-ADIC NUMBERS

For an introduction to p-adic numbers and p-adic analysis, we recommend the books of Schikhof (1984), Koblitz (1984) and Katok (2007).

2.1.1 p-adic Numbers and p-adic Integers

Most of the materials here are taken from Caruso (2017). Recall that each positive integer n can be written in base p

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_\ell p^\ell.$$

Definition 2.1.1. *A p-adic integer a is a formal series*

$$a = a_0 + a_1 p + a_2 p^2 + \cdots$$

where $0 \leq a_i \leq p - 1$. The set of all p-adic integers is denoted by $\mathbb{Z}_p$.

For any $a \in \mathbb{Z}_p$, we define

$$\alpha_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \in \mathbb{Z}/p^n\mathbb{Z}.$$

Then we set the following functions

$$\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}, \quad \pi_n(a) = \alpha_n.$$

We have for any $a \in \mathbb{Z}_p, \pi_{n+1}(a) \equiv \pi_n(a) \pmod{p^n}$. More generally, $\pi_m(a) \equiv \pi_n(a) \pmod{p^n}$ for $m \geq n$. Then putting π_n's together we get

$$\pi : \mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}, \quad a \mapsto (\pi_1(a), \pi_2(a), \cdots)$$

where

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \left\{ a = (a_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : \pi_{n+1}(a) \equiv \pi_n(a) \pmod{p^n} \ \forall n \right\}$$

is the projective limit of $\mathbb{Z}/p^n\mathbb{Z}$.

Consider a sequence $\alpha = (\alpha_1, \alpha_2, \cdots) \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Write

$$\alpha_n = a_{n,0} + a_{n,1}p + \cdots a_{n,n-1}p^{n-1}.$$

The condition $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ implies $a_{n+1,i} = a_{n,i}$ for $0 \le i \le n-1$. This means $(a_{n,i})_{n>i}$ is constant and converges to some a_i. Set

$$\psi(\alpha) = a = (a_0, a_1, \cdots) \in \mathbb{Z}_p.$$

We can check that ψ is the inverse function of π. Thus we have the following

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

The descriptions of $\mathbb{Z}_p$ as a limit of $\mathbb{Z}/p^n\mathbb{Z}$ allows us to endow $\mathbb{Z}_p$ with a commutative ring structure, that is for $a, b \in \mathbb{Z}_p$ we look at their sequences $\alpha_n, \beta_n \in \mathbb{Z}/p^n\mathbb{Z}$. Then $\alpha_n + \beta_n \in \mathbb{Z}/p^n\mathbb{Z}$ yields a well defined element $a + b \in \mathbb{Z}_p$. Note that $\mathbb{Z} \subset \mathbb{Z}_p$. One can see $\frac{1}{p} \notin \mathbb{Z}_p$. We have $\mathbb{Q}_p$ a fraction field of $\mathbb{Z}_p$.

Definition 2.1.2. *A p-adic number a is a series*

$$a = \sum_{i \ge m} a_i p^i$$

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

2.1.2 p-adic Norm and Completeness

According to Ostrowski's theorem, see Koblitz (1984), there are only two kinds of completions of the field $\mathbb{Q}$ of rational numbers. These two kinds of completions give the field $\mathbb{R}$ of real numbers or the field $\mathbb{Q}_p$ of p-adic numbers. For a fixed prime p, we introduce the notion of p-adic valuation and p-adic norm (absolute value). Let $x =$

$p^k \frac{m}{n} \in \mathbb{Q}$ with $k, m \in \mathbb{Z}, n \in \mathbb{N}, p|m$ and $p|n$. The number k is called the p-adic valuation of x and is denoted by $ord_p(x)$. By convention, we define $ord_p(0) = \infty$. Thus

$$ord_p(x) = \begin{cases} k & if \;\; x \neq 0, \\ \infty & if \;\; x = 0. \end{cases}$$

Then we can define the p-adic norm (absolute value) as follows

$$|x|_p = \begin{cases} p^{-k} & if \;\; x \neq 0, \\ 0 & if \;\; x = 0. \end{cases}$$

This norm is non-Archimedean because it satisfies the strong triangle inequality: $|x + y|_p \leq \max(|x|_p, |y|_p)$. The metric induced by this norm, $d(x, y) = |x - y|_p$, satisfies the ultrametric property: for all $x, y, z \in \mathbb{Q}$, $d(x, y) \leq \max(d(x, z), d(z, y))$. We notice that d is taken values from the proper subset $\{0\} \cup \{p^n : n \in \mathbb{Z}\}$ of $\mathbb{R}$. Recall the following definitions.

Definition 2.1.3. *A sequence (x_n) in a field K is called Cauchy if for every $\epsilon > 0$ there exists N such that $|x_n - x_m| < \epsilon$ whenever $n, m > N$.*

Definition 2.1.4. *A field K is complete with respect to the norm (absolute value) $|\cdot|$ if every Cauchy sequence of K converges in K.*

By these definitions, we have the following proposition.

Proposition 2.1.5 (see Katok (2007))**.** *The field $\mathbb{Q}_p$ of p-adic numbers is the completion of the field $\mathbb{Q}$ of rational numbers with respect to the p-adic norm (absolute value) $|\cdot|_p$.*

Denote $\mathbb{B}_r(a) := \{x \in \mathbb{Q}_p : |x - a|_p < r\}$ and $\mathbb{S}_r(a) := \{x \in \mathbb{Q}_p : |x - a|_p = r\}$ the open ball and the sphere in $\mathbb{Q}_p$ with center a and radius r. Remark that the open ball is also closed. Then the set of all p-adic integers and p-adic units of $\mathbb{Q}_p$ are denoted by $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ and $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$ respectively. Any p-adic unit $x \in \mathbb{Z}_p^*$ has the unique canonical form

$$x = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots$$

where $x_0 \in \{1,2,\cdots p-1\}$ and $x_i \in \{0,1,2,\cdots p-1\}$ for $i \in \mathbb{N}$. Furthermore, any p-adic number $x \in \mathbb{Q}_p$ has the following unique canonical form

$$x = p^{ord_p(x)}(x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots)$$

where $x_0 \in \{1,2,\ldots,p-1\}$ and $x_i \in \{0,1,2,\ldots,p-1\}$ for $i \in \mathbb{N}$. Therefore,

$$x = \frac{x^*}{|x|_p}$$

such that $x^* \in \mathbb{Z}_p^*$.

As parallel to the construction of the field $\mathbb{C}$ of complex numbers, we can also construct an analogue for p-adic numbers, see for example Koblitz (1984) and Schikhof (1984). We consider the algebraic extension of $\mathbb{Q}_p$. It will extend the p-adic absolute value uniquely. However, any extension of finite order of $\mathbb{Q}_p$ is not algebraically closed. Hence, the algebraic closure $\mathbb{Q}_p^a$ of $\mathbb{Q}_p$ is an infinite extension. This algebraic closure is not complete. Fortunately, the topological completion of $\mathbb{Q}_p^a$ is algebraically closed. Thus this field denoted by $\mathbb{C}_p$ is called the field of complex p-adic numbers.

2.2 POLYNOMIAL

2.2.1 Resultant and Discriminant

We refer the book of Gelfand et al. (1994) and the article of Dilcher & Stolarsky (2005) for the resultant and dicriminant of the polynomials.

We write a polynomial over a field K as $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ where $a_n \neq 0$ and $a_i \in K$ for $i = 0, \dots, n$. We denote $n = \deg(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0)$ the degree of the polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. The examples of the field K that can be considered are $\mathbb{F}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and etc. Later, we will concentrate on the polynomial equations over $\mathbb{Q}_p$. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ and $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ be polynomials of degrees $n \geq 1$ and $m \geq 1$ (a_n and a_m do not vanish) with coefficient in an arbitrary field K respectively. Denote by $R_{m,n}(f,g)$ of their resultant. Sometimes we denote it as $R(f,g)$.

Definition 2.2.1. *Let* $a_n \neq 0$ *and* $b_m \neq 0$. *Then*

1) $R(f,g) = a_n^m b_m^n \prod_{i,j} (x_i - y_j)$

   where $x_1, \dots, x_n$ and $y_1, \dots, y_m$ are roots of f and g respectively.

2) $R(f,g)$ is equal to the determinant of the following $(n+m)$ by $(n+m)$ Sylvester matrix, i.e.

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} & a_n & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & a_2 & a_3 & \cdots & a_n \\ b_0 & b_1 & b_2 & \cdots & b_m & 0 & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_m \end{vmatrix}.$$

The following is one of the result on resultant of two polynomials f and g.

Theorem 2.2.2 (see Gelfand et al. (1994))**.** *For two concrete polynomials* f *and* g, $R(f,g) = 0$ *is equivalent to the fact that* f *and* g *have a common root. This also means that* $R(f,g) \neq 0$ *is equivalent to the fact that* f *and* g *have no common root.*

We denote by $\Delta_n(f)$ the discriminant of polynomial f. Frequently, we write it as $\Delta(f)$.

Definition 2.2.3. *Let* $a_n \neq 0$. *Then*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2$$

where $x_1, \ldots, x_n$ are roots of f.

There is a relation between resultant and discriminant of polynomial as stated in the following theorem.

Theorem 2.2.4 (Dilcher & Stolarsky, 2005)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degrees $n \geq 1$ with coefficient in an arbitrary field K. Then the discriminant of f is given by*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1} R(f, f').$$

This relation allows us to find the discriminant of a polynomial. For example, the quadratic polynomial has

$$\Delta(ax^2 + bx + c) = b^2 - 4ac,$$

the cubic polynomial has

$$\Delta(ax^3 + bx^2 + c + d) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

and the quartic polynomial has

$$\begin{aligned}\Delta(ax^4 + bx^3 + cx^2 + dx + e)& \\ &= 256a^3e^3 - 192a^2bde^2 - 128a^2c^2e^2 + 144a^2cd^2e - 27a^2d^4 \\ &+ 144ab^2ce^2 - 6ab^2d^2e - 80abc^2de + 18abcd^3 + 16ac^4e \\ &- 4ac^3d^2 - 27b^4e^2 + 18b^3cde - 4b^3d^3 - 4b^2c^3e + b^2c^2d^2.\end{aligned}$$

2.2.2 Polynomial Congruences

For linear and quadratic congruences, we refer to the book of Rosen (2011). The simplest congruence is linear

$$ax \equiv b \pmod{m} \tag{1}$$