STABILITY AND MONOGENITY OF ITERATES OF POLYNOMIALS

HIMANSHU SHARMA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI

May 2024

STABILITY AND MONOGENITY OF ITERATES OF POLYNOMIALS

by

HIMANSHU SHARMA

Department of Mathematics

Submitted

in fulfilment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi

May 2024

Dedicated to Sardarji and Shri Krishna

Certificate

This is to certify that the thesis entitled **STABILITY AND MONOGENITY OF ITERATES OF POLYNOMIALS** submitted by **Mr. Himanshu Sharma** to the Indian Institute of Technology, Delhi, for the award of the degree of **Doctor of Philosophy** is a record of the original bonafide research work carried out by him under my supervision and guidance. The thesis has met the standards, fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other University or Institute for the award of any degree or diploma.

Dr. Ritumoni Sarma
Assosiate Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016

Dr. Shanta Laishram
Professor
Stat-Math Unit
Indian Statistical Institute
New Delhi 110016

Acknowledgements

I would like to express my heartfelt gratitude to my supervisors, Prof. Ritumoni Sarma and Prof. Shanta Laishram for their constant help and encouragement throughout my Ph.D. Their outstanding direction from the beginning helped me to gain a grasp of the area. Their ability to make everyone comfortable is really admirable. I appreciate the flexibility they gave me with my work. I am thankful for their academic and non-academic counsel and their valuable response to all my queries, which helped me grow mathematically and in other dimensions of life. I am thankful to them for going through the different versions of the research papers, which improved their quality. I also want to thank them for introducing this interesting area to me. The completion of the thesis would not have been possible without their excellent support and discussions. They always appreciated the ideas and showed their active involvement. I consider myself fortunate that they are my advisors.

I would also like to thank my SRC (Student Research Committee) members, Prof. N. Shravan Kumar, Prof. Surjeet Kaur, Prof. Amit Priyadarshi, and Prof. S.D. Joshi, for their valuable comments and their support. I would like to thank all the instructors of the courses that I have taken during my Ph.D. coursework. I acknowledge IIT Delhi for all the facilities and the financial support.

I am grateful to my school teachers and professors during my graduation and postgraduation for their wonderful teaching and for enhancing my interest in mathematics. I appreciate my seniors, Dr. Vidya Sagar and Dr. Ankita Jindal, for motivating me to work in this field. I also want to thank my juniors, Anuj, Aakanksha, Ankit, Chetan, and Ridip, for creating a pleasant working environment. I want to thank my friends Manuj, Gyanendra, Santosh, Divay, Gurdev, Aakash, Prabhakar, Dr. Sushil, Jyotsna, Manisha, Tanvi, and Anisha for creating everlasting memories.

I am thankful to my parents and siblings for their constant love and support, which keeps me motivated and confident. I am thankful to my beloved wife for her constant support and belief in me. My achievements are the consequence of their faith in me. My deepest gratitude goes to my mother and father for their unconditional love and support.

New Delhi | Himanshu Sharma

May 2024

Abstract

In this thesis, our main focus is to study certain properties of iterates of polynomials over a field. In fact, we discuss the irreducibility and monogenity of iterates of a polynomial. To study the irreducibility of polynomials over a field is important due to its applications in number theory and in other areas of mathematics as well. In this thesis, we investigate the irreducibility of iterates of the binomial $x^d + \frac{1}{c}$ for $c \in \mathbb{Z} \setminus \{0\}$, and $d \geq 3$, and prove that for an infinite family of these irreducible binomials, all their iterates are also irreducible over $\mathbb{Q}$. Next, we give a conditional result and show that if the binomial $f(x) = x^d + \frac{1}{c}$, for $c \in \mathbb{Z} \setminus \{0\}$ and $d \geq 3$, is irreducible, then all its iterates are also irreducible under the *abc*-conjecture. Moreover, when $d = 3$, we show that the number of irreducible factors of iterates of $x^3 + \frac{1}{c}$ is atmost 2 if $|c| \leq 10^{12}$.

In particular, the irreducibility of polynomials over finite fields is important due to their applications in cryptography and coding theory. In this thesis, we study the irreducibility of iterates of certain trinomials over finite fields of odd characteristics. Furthermore, we prove that for a family of trinomials of prime degree p, its second iterate is a product of p irreducible polynomials, each of degree p. Besides, we give a criterion for a family of polynomials of certain type to be "dynamically irreducible" over a finite field and produce dynamically irreducible sets of polynomials.

One of the oldest problems in algebraic number theory is finding the ring of integers in a number field. If the ring of integers of a number field K is $\mathbb{Z}[\theta]$ for some $\theta \in K$, then the number field K is referred to as a monogenic field. The ring of integers of a monogenic number field is easy to understand. In this thesis, we also study the monogenity of the iterates of certain families of polynomials. If a polynomial is monogenic, then every number field defined by the polynomial is also monogenic. To discuss the monogenity of the iterates of a polynomial, we need the iterates of the polynomial to be irreducible. First, we give a necessary condition for the

iterates of a polynomial to be monogenic. If a polynomial satisfies certain Eisenstein criteria, we give a sufficient condition for the iterates to be monogenic. In fact, using our result, we give a couple of examples that give an infinite tower of monogenic number fields.

Finally, we give a condition that is both necessary and sufficient for the monogenity of the iterates of an irreducible binomial. We also give infinite families of polynomials such that all their iterates are non-monogenic.

सार

इस थीसिस में हमारा मुख्य ध्यान एक क्षेत्र या फील्ड में बहुपदों के पुनरावृत्तों के कुछ गुणों का अध्ययन करना है| वास्तव में, हम एक बहुपद के पुनरावृत्तों की इर्रिड्युसिबिलिटी और मोनोजेनिटी पर चर्चा करते हैं| नंबर थ्योरी और गणित के अन्य क्षेत्रों में इसके अनुप्रयोगों के कारण किसी क्षेत्र में बहुपदों की इर्रिड्युसिबिलिटी का अध्ययन करना महत्वपूर्ण है। इस थीसिस में हम $c \in \mathbb{Z} \setminus \{0\}$, और $d \geq 3$ के लिए द्विपद $x^d + \frac{1}{c}$ के पुनरावृत्तों की इर्रिड्युसिबिलिटी की जांच करते हैं और सिद्ध करते हैं कि इन इर्रिड्युसिबल द्विपदों के अनंत परिवार के लिए उनके सभी पुनरावृत्त भी क्षेत्र $\mathbb{Q}$ पर इर्रिड्युसिबल हैं| इसके बाद हम एक सशर्त परिणाम देते हैं और दिखाते हैं कि यदि द्विपद $f(x) = x^d + \frac{1}{c}, c \in \mathbb{Z} \setminus \{0\}$ और $d \geq 3$ के लिए इर्रिड्युसिबल है तो एबीसी-कन्जेक्चर के तहत इसके सभी पुनरावृत्त भी इर्रिड्युसिबल हैं। इसके अलावा, जब $d = 3$ और $|c| \leq 10^{12}$ हो तब हम दिखाते हैं कि $x^3 + \frac{1}{c}$ के पुनरावृत्तों के इर्रिड्युसिबल कारकों की संख्या अधिकतम 2 है| विशेष रूप से, क्रिप्टोग्राफी और कोडिंग थ्योरी में अनुप्रयोगों के कारण फाइनाइट क्षेत्र पर बहुपदों की इर्रिड्युसिबिलिटी महत्वपूर्ण है। इस थीसिस में हम विषम कैरिक्टरिस्टिक के फाइनाइट क्षेत्र पर कुछ त्रिपदों के पुनरावृत्तों की इर्रिड्युसिबिलिटी का अध्ययन करते हैं। इसके अलावा हम यह सिद्ध करते हैं कि अभाज्य डिग्री p के त्रिपदों के एक परिवार के लिए इसका दूसरा पुनरावृत्त p इर्रिड्युसिबल बहुपदों का गुणनफल है, जिनमें से प्रत्येक की डिग्री p है। इसके अलावा, हम निश्चित तरह के बहुपदों के एक परिवार के लिए फाइनाइट क्षेत्र पर डाइनामिकली इर्रिड्युसिबल होने के लिए एक मानदंड देते हैं और बहुपदों के डाइनामिकली इर्रिड्युसिबल सेट का उदाहरण भी देते है| ऐल्जब्रैइक नंबर थ्योरी में नंबर फील्ड की रिंग ऑफ इंटीजर्स ढूंढना सबसे पुरानी समस्याओं में से एक है। यदि किसी नंबर फ़ील्ड K की रिंग ऑफ इंटीजर्स किसी $\theta \in K$ के लिए $\mathbb{Z}[\theta]$ है तो नंबर फ़ील्ड K को मोनोजेनिक फ़ील्ड कहा जाता है। एक मोनोजेनिक नंबर फील्ड की रिंग ऑफ इंटीजर्स को समझना आसान है| इस थीसिस में हम बहुपदों के कुछ परिवारों के पुनरावृत्तों की मोनोजेनिटी का भी अध्ययन करते हैं। यदि एक बहुपद मोनोजेनिक है तो बहुपद द्वारा परिभाषित किया गया प्रत्येक नंबर फील्ड भी मोनोजेनिक है। एक बहुपद के पुनरावृत्तों की मोनोजेनिटी पर चर्चा करने के लिए बहुपद की पुनरावृत्तियों का इर्रिड्युसिबल होना आवश्यक है। सबसे पहले हम एक बहुपद की पुनरावृत्तियों के मोनोजेनिक होने के लिए एक आवश्यक शर्त देते हैं| यदि एक बहुपद कुछ आइज़ेंस्टीन मानदंडों को पूरा करता है तो हम पुनरावृत्तियों को मोनोजेनिक होने के लिए पर्याप्त शर्त देते हैं। वास्तव में, अपने परिणाम का उपयोग करते हुए हम दो उदाहरण देते हैं जो मोनोजेनिक नंबर फील्ड का एक अनंत टॉवर देते हैं। अंत में हम एक शर्त देते हैं जो एक इर्रिड्युसिबल द्विपद के पुनरावृत्तों की मोनोजेनिटी के लिए आवश्यक और पर्याप्त दोनों है। हम ऐसे बहुपदों के अनंत परिवार भी देते हैं जिनके सभी पुनरावृत्त गैर-मोनोजेनिक हैं।

Contents

List of Symbols

Symbol

$\mathbb{N}$	Set of natural numbers,
$\mathbb{Z}$	Ring of rational integers,
$\mathbb{Q}$	Field of rational numbers,
$\mathbb{C}$	Field of complex numbers,
$\mathbb{P}^1(K)$	Projective line over the field K,
$\mathbb{F}_q$	The finite field of order $q = p^n$, where p is prime number and $n \geq 1$,
$Tr_{q\|p}(\alpha)$	Trace of $\alpha \in \mathbb{F}_q$ over $\mathbb{F}_p$, where p is a prime and q is a prime power,
$N_{L/K}(\alpha)$	Norm of $\alpha \in L$ over K, where L/K is field extension,
$\mathcal{O}_K$	Ring of integers of the number field K.
$\overline{K}$	Algebraic closure of the field K.