Classifying Degree *mp* Extensions of the *p*-adic Numbers

Kaitlyn McGloin[1] Jacob Zoromski[2]

[1]Loyola Marymount University [2]University of Wisconsin - Madison

Introduction

A **polynomial** is an expression containing algebraic terms of the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

A **root** is a number r such that $f(r) = 0$. As an example, consider the polynomial $x^2 + ax + b$. Its roots are given by the quadratic formula:

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

Whether these roots "exist" depends on which number system we are using. In the real numbers, the roots exist only when $a^2 - 4b \geq 0$. In the rational numbers, the roots exist only when $a^2 - 4b$ is a perfect square. If the roots do not exist, we can **extend** our number system to include the roots. In general, we can extend any number system by adjoining a root of a polynomial. If the polynomial is irreducible, we call the **degree** of the extension the highest power of x in the polynomial. By adjoining a root of a polynomial, we obtain a number system in which the polynomial has at least one root. In the extension, the number of roots of the generating polynomial is the **order of the automorphism group**.

We are interested in the extensions of a number system called the ***p*-adic numbers**, or $\mathbb{Q}_p$, where p is prime. A p-adic number is a (potentially infinite) sum of powers of p, so that we can easily keep track of divisibility by p. $\mathbb{Q}_p$ contains the rational numbers, but it also contains some irrational numbers. Since primes are the building blocks of all numbers, studying $\mathbb{Q}_p$ and its extensions has important applications across all of mathematics, including number theory and cryptography. We can even do calculus over $\mathbb{Q}_p$, so understanding it will have consequences for both analysis and number theory.

Our Research

$\mathbb{Q}_p$ has only finitely many extensions of a given degree and the polynomials that generate these extensions have integer coefficients. Consequently, it is possible to classify all extensions of a given degree by making a complete list of generating polynomials. Degree p and $2p$ extensions of $\mathbb{Q}_p$ were classified by Amano [1] and Awtrey-Hadgis [2], respectively. For all other degrees n divisible by p, the only complete results are when $n \leq 15$. The goal of this project was to classify all extensions of degree mp, where p does not divide m.

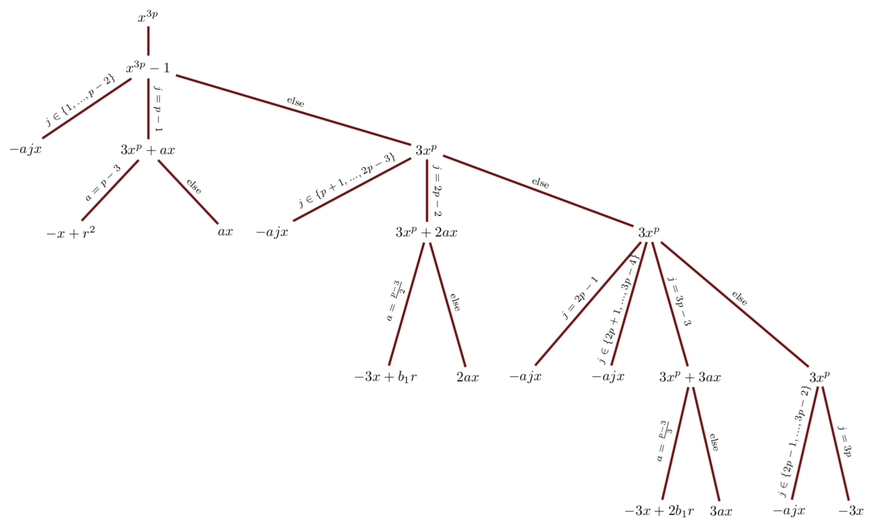
We produced a list of polynomials that generate all extensions of degree mp where $p > m$ and $\gcd(m, p-1) = 1$, along with their automorphism group sizes. With Panayi's Algorithm, we proved that the proposed polynomials define distinct extensions and verified that we indeed found all of the extensions and their automorphism sizes. Furthermore, we determined the number of distinct extensions for each possible j value.

Panayi's Algorithm

To prove our results, we used an algorithm developed by Panayi [3]. Let ϕ, ψ be two irreducible polynomials. Let π be a root of ϕ. The algorithm sequentially generates polynomials based on ψ to find the roots of ψ in $\mathbb{Q}_p(\pi)$. ψ generates the same extension as $\mathbb{Q}_p(\pi)$ if and only if ψ has a root in $\mathbb{Q}_p(\pi)$. So, with the algorithm we can determine if ψ and ϕ generate distinct extensions. Furthermore, if $\phi = \psi$, then the algorithm tells us how many roots of ϕ we get by adjoining π, or the order of the automorphism group.

Algorithm. (Panayi's Algorithm)
Input: $\mathbb{Q}_p(\pi)$, where π is the root of a polynomial, and a polynomial ϕ.
Output: A set G of approximations of the roots of $\phi(x)$ over $\mathbb{Q}_p(\pi)$.
Let $\phi^\sharp = \phi/\pi^\omega$, where ω is the highest power of π that divides all the terms of ϕ.

- Set $C \leftarrow \{(\phi^\sharp(x), 0, 0)\}$.
- Set $G \leftarrow \{\}$.
- While C is not empty:
  - For all $(\psi(x), \delta, s)$ in C:
    - $C \leftarrow C \backslash \{(\psi(x), \delta, s)\}$.
    - $R \leftarrow \{\beta | \beta \text{ is a root of } \psi(x) \text{ modulo } p\}$.
    - For all β in R:
      - Set $\psi(x) \leftarrow \psi(\pi x + \beta)$.
      - Replace $\psi(x) \leftarrow \psi^\sharp(x)$.
      - If $\deg \underline{\psi} = 1$, then $G \leftarrow G \cup \{\delta + \pi^s\beta\}$.
      - If $\deg \underline{\psi} > 1$, then $C \leftarrow C \cup \{(\psi(x), \delta + \pi^s\beta, s+1)\}$.
- Return G.



Panayi's Algorithm for automorphism group sizes of degree $3p$ extensions, where $gcd(3, p-1) = 1$. Starting at the top, each node of the tree shows the reduced polynomial $\phi^\sharp$ modulo p at that step. a is defined as in the table, and the branches with r represent p branches, one for each $r \in \{0, \ldots, p-1\}$.

Theorem

Let $p > m$, $\gcd(m, p-1) = 1$. The polynomials in the following table uniquely define all totally ramified degree mp extensions of $\mathbb{Q}_p$. There are $p^{m+1} + p^m - p$ total extensions.

j	Defining Polynomials	#Aut	#Extensions
$0 < j < p-1$	$x^{mp} + pax^j + p$	1	$p-1$
$p-1$	$x^{mp} + pax^j + p$	1	$2p-2$
	$x^{mp} + pb_1x^{j+1} + p\zeta_1x^j + p$	p	
$p < j < 2p-2$	$x^{mp} + pb_1x^{j+1} + pax^j + p$	1	$p^2 - p$
$2p-2$	$x^{mp} + pb_1x^{j+1} + pax^j + p$	1	$2p^2 - 2p$
	$x^{mp} + pb_2x^{j+2} + pb_1x^{j+1} + p\zeta_2x^j + p$	p	
$2p-1$	$x^{mp} + pb_1x^{j+2} + pax^j + p$	1	$p^2 - p$
$(k-1)p < j < k(p-1)$	$x^{mp} + \sum_{i=1}^{k-1} pb_ix^{j+i} + pax^j + p$	1	$p^k - p^{k-1}$
$k(p-1)$	$x^{mp} + \sum_{i=1}^{k-1} pb_ix^{j+i} + pax^j + p$	1	$2p^k - 2p^{k-1}$
	$x^{mp} + \sum_{i=1}^{k} pb_ix^{j+i} + p\zeta_kx^j + p$	p	
$k(p-1) < j < kp$	$x^{mp} + \sum_{i=1}^{k-1} pb_ix^{j+i+\delta_{i,j,k}} + pax^j + p$	1	$p^k - p^{k-1}$
$(m-1)p < j < m(p-1)$	$x^{mp} + \sum_{i=1}^{m-1} pb_ix^{j+i} + pax^j + p$	1	$p^m - p^{m-1}$
$m(p-1)$	$x^{mp} + \sum_{i=1}^{m-1} pb_ix^{j+i} + pax^j + p$	1	$2p^m - 2p^{m-1}$
	$x^{mp} + \sum_{i=1}^{m-1} pb_ix^{j+i} + p\zeta_mx^j + p + p^2b_m$	p	
$m(p-1) < j < mp$	$x^{mp} + \sum_{i=1}^{m-1} p\epsilon_{i,j}b_ix^{j+i+\delta_{i,j,k}} + pax^j + p$	1	$p^m - p^{m-1}$
mp	$x^{mp} + \sum_{i=1}^{m} p^2b_ix^i + p$	1	p^m

Table 1: Degree mp extensions of $\mathbb{Q}_p$, where $gcd(m, p-1) = 1$. Here $1 \leq a \leq p-1$, $0 \leq b \leq p-1$, $2 \leq k \leq m-1$, $\zeta_k = \frac{-m}{k} \mod p$, $\delta_{i,j,k} = 1$ if $i + j \geq kp, k < m$, $\delta_{i,j,k} = 1 - mp$ if $i + j \geq mp$, and 0 otherwise, $\epsilon_{i,j} = p$ if $i + j \geq mp$, and 1 otherwise.

Future Research

We have completely verified the generating polynomials and automorphism sizes of the extensions of degree mp when $p > m$ and $gcd(m, p-1) = 1$. Future research will focus on constructing and verifying the characteristics of the polynomials for the case when $m > p$ and when $\gcd(m, p-1) > 1$. A natural continuation of this work is to compute the Galois groups of degree mp polynomials over $\mathbb{Q}_p$.

References

[1] Shigeru Amano.
Eisenstein equations of degree p in a $\mathfrak{p}$-adic field.
J. Fac. Sci. Univ. Tokyo Sect. IA Math., 18:1–21, 1971.

[2] Chad Awtrey and Nick Hadgis.
Totally ramified p-adic fields of degree $2p$.
preprint.

[3] Peter Panayi.
Computation of Leopoldt's p-adic regulator.
PhD thesis, University of East Anglia, December 1995.

This work was supported in part by NSA grant # H98230-18-1-0012.