Classifying p-adic Fields of Degree p^2

Cameron Cinel[1] Judah Devadoss[2] Elisabeth Howard[3] Alex Jenny[4]

[1]University of Southern California [2]Williams College [3]Hamilton College [4]Midwestern State Unversity

Introduction

A polynomial over the rational numbers can be written as

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

where each a_i is a rational number (a fraction). The **roots** of f are the numbers r such that $f(r) = 0$. The quadratic formula gives the roots of the polynomial $ax^2 + bx + c$ in terms of a, b and c:

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

For example, the roots of $x^2 - 2$ are $\pm\sqrt{2}$. Note that $\sqrt{2}$ is not a rational number because it cannot be expressed as a fraction. However, you can add $\sqrt{2}$ and its multiples into the rationals. When we add the roots of a polynomial to the rational numbers we obtain a **field extension**. The way the roots of a polynomial interact with each other, called the polynomial's **Galois group**, determines properties of the polynomial.

Let p be a prime. The **field of p-adic numbers**, denoted $\mathbb{Q}_p$, is the collection of all numbers of the form

$$\sum_{k=N}^{\infty} a_k p^k$$

where the p-adic digits a_k are elements of $\{0, 1, \ldots, p-1\}$. Note that $\mathbb{Q}_p$ contains the rational numbers, and is a number theoretic analog to the field of real numbers.

The p-adic numbers have implications in cryptography, and polynomials are used for modeling across multiple disciplines. Our project focuses on determining when polynomials with p-adic coefficients have certain arithmetic properties.

Our Research

There are only a finite number of extensions of $\mathbb{Q}_p$ for a given degree, making a complete classification of these extensions possible. The case where p does not divide the degree of the extension is understood. Degree p and $2p$ extensions were classified by Amano [1] and Awtrey-Hadgis [2], respectively. For all other degrees divisible by p, the only known cases are when $n \leq 15$. In the case of totally ramified degree p^2 extensions of $\mathbb{Q}_p$, it is known that there are $p^{p+3} + p^p - p$ distinct generating polynomials. The motivating idea behind this project was to classify these distinct generating polynomials.

Adjoining a root of a polynomial to a field creates an extension that may contain other roots of the polynomial. The number of roots of the generating polynomial that the extension contains is **order of the automorphism group**. We classified our polynomials by the three possible automorphism group orders: 1, p, and p^2. We only considered the order 1 and order p cases because polynomials with automorphism group order p^2 define Galois extensions and have already been classified [3].

Classifying Size p Automorphism Groups

j	Generating Polynomial	Conditions
$j = (m+n)p - m$	$x^{p^2} + q_j(x) + (-1)^s m^{-1} nap^{s+1}x^t + apx^{np} + (bp^{s+1} + 1)p$	$n \neq p$
$j = p^2 - 1$	$x^{p^2} + (p - a - 1)px^j + apx^{p(p-1)} + (bp + 1)p$	
$j = (1+p)p - 1$	$x^{p^2} + pq_j(x) + (p-1)px^{p(p-1)} - m^{-1}p^2x^{p-1} + (bp + 1)p$	$n = p$ $m = 1$
$j = (m+p)p - m$	$x^{p^2} + pq_j(x) - m^{-1}p^2x^t + (\delta_{t,p^2-1}ap + b)p^2x^p + p$	$n = p$ $m \neq 1$

Classifying Size 1 Automorphism Groups

j	Generating Polynomial	f Exponents
$j < p$	$x^{p^2} + apx^j + p$	
$p < j < p^2 - p$	$x^{p^2} + apx^j + b_0px^{qp} + p$	
	$x^{p^2} + f(x) + apx^j + bpx^{\mu p} + p$	$[j+1, j+y]$
$p^2 - p < j < p^2 - 1$	$x^{p^2} + apx^j + bpx^{2p} + p$	
	$x^{p^2} + f(x) + apx^j + bpx^p + p$	$[j+1, p^2-1], p[1, r-\mu]$
$j = p^2 - 1$	$x^{p^2} + apx^j + p$	
	$x^{p^2} + apx^j + bpx^{\mu p} + p \cdot f(x) + p$	$[1, t-\mu]$
$p^2 < j < p^2 + p$	$x^{p^2} + ap^2x^t + bp^2x^{t+1} + p$	
	$x^{p^2} + apx^{\mu p} + p \cdot f(x) + bp^2x^t + p$	$[t+1, t+p-\mu+1], i \neq p$
$p^2 < j < 2p^2 - p$, $p \mid j$	$x^{p^2} + p \cdot f(x) + apx^t + p$	$[t+1, t+p+1], i \neq t+p$
$p^2+p < j < 2p^2-p, p \nmid j$	$x^{p^2} + p \cdot f(x) + ap^2x^t + bpx^{\mu p} + p(1 + cp^2)$	$[t+1, t+p+\mu+w], p \nmid i$
$j = 2p^2 - p$	$x^{p^2} + p \cdot f(x) + apx^t + p(1 + bp)$	$p[1], [t+1, t+p-1]$
$2p^2 - p < j < 2p^2 - 1$	$x^{p^2} + p \cdot f(x) + apx^t + p$	$p[1, r], [t+1, p^2-1]$
$j = 2p^2 - 1$	$x^{p^2} + p \cdot f(x) + ap^2x^t + bp^2x^p + p$	$p[1, p-1]$
$j = 2p^2$	$x^{p^2} + p \cdot f(x) + apx^p + p$	$p[1, p+1], i \neq p$

Variable Definitions

- $j = (m+n)p - m,\ j = qp + r,\ j = sp^2 + t$
- $q_j(x) = \sum_{i=1, p \nmid (i+t}^{\min\{m,p\}} apx^{(i+t+\lfloor \frac{m}{p} \rfloor)} \pmod{p^2}$
- f exponents = $[u, v], p[z]$, $a_i \in [0, p-1]$ denotes

$$f(x) = p(a_zpx^z) + \sum_{i=u}^{v} a_ipx^i.$$

- $a, b, c \in [0, p-1]$, and μ, w, y are dependent on j

*Because of the charts' compression, they may contain previously enumerated polynomials of greater automorphism size.

Methods

We generated all totally ramified extensions using a Magma package written by Brian Sinclair [6] and wrote our own Magma programs to remove the isomorphic extensions and calculate automorphism group sizes. By inspection, we determined all general forms for the generating polynomials based on j invariants and the automorphism group size.

To prove our conjectures, we used Panayi's Algorithm [5]. For each general form, we applied the algorithm first to prove the order of the automorphism group, and then to demonstrate that two polynomials sharing the same general form generate isomorphic extensions if and only if their coefficients are equal. To verify that we had obtained not only the proper extensions, but also the correct number of extensions, we summed the calculated mass for the non-isomorphic polynomials to get the total mass for each j value, which we checked against Krasner's formula [4].

Number of Polynomials and Masses

Aut Size	Num. of Gen. Poly
1	$\frac{p^{p+4}-2p^{p+3}+p^{p+2}-p^p+p}{p-1}$
p	$\frac{p(p^{p+2}-p^{p+1}+p^p-p^2)}{p-1}$
p^2	p^2

j	Mass
$(k-1)p < j < kp$	$p^{k+1}(p-1)$
$p^2 < j < 2p^2$	$p^{p+2}(p-1)$
$2p^2$	p^{p+3}

Future Research

We have classified the generating polynomials of degree p^2 extensions of $\mathbb{Q}_p$ in complete generality. The next step would be to compute the Galois group for each generating polynomial.

References

[1] Shigeru Amano.
Eisenstein equations of degree p in a 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] Chad Awtrey, Peter Komlofske, Christian Reese, and Janaé Williams.
Totally ramified Galois p-adic fields of p-power degree.
preprint.

[4] Marc Krasner.
Nombre des extensions d'un degré donné d'un corps p-adique.
In *Les Tendances Géom. en Algèbre et Théorie des Nombres*, pages 143–169. Editions du Centre National de la Recherche Scientifique, Paris, 1966.

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

[6] Sebastian Pauli and Brian Sinclair.
Enumerating extensions of (π)-adic fields with given invariants.
Int. J. Number Theory, 13(8):2007–2038, 2017.

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