Discriminants as Invariants of Local Fields

Alexander Gaura (Princeton University) and Ariel Uy (Carnegie Mellon University)

Introduction

One of the goals of mathematics is the classification of mathematical objects. Numerical invariants, or numbers attached to classes of objects which share certain traits, are important tools for differentiating these objects.

After examining millions of examples, we conjectured that the first non-zero digit of the discriminant of an Eisenstein polynomial is an invariant of the extension generated by the polynomial in many cases.

We proved this conjecture and applied the invariant to distinguish extensions generated by polynomials of degree p.

Technical Abstract

If two Eisenstein polynomials φ and ψ over the p-adic numbers generate isomorphic extensions, then $v_p(\mathrm{disc}(\varphi)) = v_p(\mathrm{disc}(\psi))$.

We have proven that, if $(p-1)$ divides $n(n-1)$ where n is the degree of φ, then

$$v_p(\mathrm{disc}(\varphi) - \mathrm{disc}(\psi)) \geq v_p(\mathrm{disc}(\varphi)) + 1.$$

This makes the first (non-zero) digit of $\mathrm{disc}(\varphi)$ an invariant of the extension generated by φ.

For polynomials φ of degree p in most cases, this new invariant together with the valuation of the discriminant completely determines the extension generated by φ.

p-Adic Numbers

A prime number is a number whose only divisors are 1 and itself. Primes are the building blocks of numbers: we can write any number using only primes. For example, $12 = 2 \cdot 2 \cdot 3$. For any prime number p, we can define the *p-adic numbers*. We use p-adic numbers to investigate what happens with respect to one prime.

Any p-adic number can be written as a sum of powers of p. If we choose $p = 3$, then 12 would be written as $1 \cdot 3^1 + 1 \cdot 3^2$, and 29 would be written as $2 \cdot 3^0 + 1 \cdot 3^3$.

The *p-adic valuation*, $v_p(n)$ of a number n, is the lowest exponent of p in the expansion of n. So $v_3(12) = 1$ as 3^1 is the lowest power of 3 in the expansion of 12.

Polynomials

Polynomials are basic building blocks of mathematical functions. We consider monic polynomials of degree n: $x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ where each c_i is a p-adic number.

A polynomial with p-adic coefficients is called *Eisenstein* if its coefficients are all divisible by p and its constant term is not divisible by p^2. For example, the 3-adic polynomial $x^3 + 6x + 3$ is Eisenstein.

Polynomials φ and ψ of the degree generate isomorphic extensions if a root of φ can be written in terms of root of ψ. Extensions generated by p-adic polynomials are called *local fields*.

Discriminants

The roots of a polynomial $\varphi(x)$ are the solutions to the equation $\varphi(x) = 0$. The *discriminant* of the polynomial φ, written $\mathrm{disc}(\varphi)$, is the product of all the differences of its roots, times $(-1)^{n(n-1)/2}$ where n is the degree of φ.

Example: If $\varphi(x) = (x-1)(x-2)(x-3)$, the roots of φ are 1, 2, and 3. We get $\mathrm{disc}(\varphi) = -(1-3)(3-1)(1-2)(2-1)(2-3)(3-2) = -(-2)\cdot 2\cdot(-1)\cdot 1\cdot(-1)\cdot 1 = 4$.

In our research, we found a relationship between the discriminant of polynomials and characteristics of the field they generate.

Experimental Results

We wrote computer programs to examine millions of examples and found the behavior illustrated below.

For Eisenstein polynomials of degree 3 over the 3-adic numbers we give eleven polynomials that generate isomorphic extensions and their discriminants and

$$\delta = v_p(\mathrm{disc}(\varphi) - \mathrm{disc}(\psi_i)) - v_p(\mathrm{disc}(\varphi)).$$

In the table δ is the number of digits in the p-adic expansion of the discriminant of φ and the polynomial in the row have in common (excluding leading zeros). Notice that δ is greater than or equal to 1 for each ψ_i.

	Polynomial	**Disc**	***p*-adic Expansion of Disc**	δ
φ	$x^3 + 6x + 3$	-1107	$1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + 1 \cdot 3^6 + 2 \cdot 3^7 + 1 \cdot 3^8 + \ldots$	∞
ψ_1	$x^3 + 3x^2 + 6x - 3$	-1431	$1 \cdot 3^3 + 0 \cdot 3^4 + 0 \cdot 3^5 + 1 \cdot 3^6 + \ldots$	1
ψ_2	$x^3 - 6x^2 - 3x - 15$	-23463	$1 \cdot 3^3 + 1 \cdot 3^4 + 2 \cdot 3^5 + \ldots$	2
ψ_3	$x^3 + 9x^2 + 15x - 15$	5940	$1 \cdot 3^3 + 1 \cdot 3^4 + 0 \cdot 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7$	2
ψ_4	$x^3 + 9x^2 + 6x - 12$	21492	$1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + 2 \cdot 3^6 + 1 \cdot 3^9$	3
ψ_5	$x^3 + 3x^2 - 3x - 6$	857	$1 \cdot 3^3 + 1 \cdot 3^4 + 0 \cdot 3^5 + 1 \cdot 3^6$	2
ψ_6	$x^3 - 15x^2 - 12x - 12$	-165456	$1 \cdot 3^3 + 0 \cdot 3^4 + 0 \cdot 3^5 + 1 \cdot 3^6 + \ldots$	1
ψ_7	$x^3 - 15x^2 - 3x + 3$	44820	$1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + 1 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^9$	5
ψ_8	$x^3 - 12x^2 + 15x - 6$	-4104	$1 \cdot 3^3 + 0 \cdot 3^4 + 1 \cdot 3^5 + \ldots$	1
ψ_9	$x^3 + 6x^2 - 3x + 6$	-7668	$1 \cdot 3^3 + 1 \cdot 3^4 + 1 \cdot 3^5 + 1 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + \ldots$	5
ψ_{10}	$x^3 - 3x^2 - 3x + 3$	756	$1 \cdot 3^3 + 0 \cdot 3^4 + 0 \cdot 3^5 + 1 \cdot 3^6$	1

The ψ below and φ from above do not generate isomorphic extensions. Notice that δ is 0, meaning the discriminants are different.

	Polynomial	**Disc**	***p*-adic Expansion of Disc**	δ
ψ	$x^3 + 6x^2 + 12$	-14256	$0 \cdot 3^3 + 1 \cdot 3^4 + \ldots$	0

In the following example over the 5-adic numbers, φ and ψ have degree 3 and generate isomorphic extensions, but δ is 0.

	Polynomial	**Disc**	***p*-adic Expansion of Disc**	δ
φ	$x^3 + 5$	-675	$3 \cdot 5^2 + \ldots$	∞
ψ	$x^3 + 10x^2 - 20x - 10$	145300	$2 \cdot 5^2 + \ldots$	0

Notice that here $p - 1 = 4$ does not divide $n(n-1) = 6$. This and many more examples lead us to conjecture that $\delta \geq 1$ only when $n(n-1)$ is a multiple of $p - 1$.

Background

The valuation $v_p(\mathrm{disc}(\varphi))$ of the discriminant of an Eisenstein polynomial is the same for all polynomials φ generating isomorphic extensions.

This makes the valuation of the discriminant of an Eisenstein polynomial φ an invariant of the extension generated by φ.

A bit more than just the valuation of the discriminant is is known to be an invariant:

Theorem (from Cassels 'Local Fields'): Let p be a prime number. Let φ and ψ be Eisenstein polynomials of degree n over the p-adic numbers that generate isomorphic extensions. Then $\mathrm{disc}(\varphi)$ and $\mathrm{disc}(\psi)$ differ by a square.

Our Main Result

Theorem: Let p be an odd prime number and $n \geq 3$. Let φ and ψ be Eisenstein polynomials of degree n over the p-adic numbers that generate isomorphic extensions. If $(p-1)$ divides $n(n-1)$, then

$$v_p(\mathrm{disc}(\varphi) - \mathrm{disc}(\psi)) \geq v_p(\mathrm{disc}(\varphi)) + 1.$$

This shows that the first non-zero digit of the discriminant is an invariant of the extension generated by φ.

Applications

A new invariant of an object is valuable only if it contains useful information about the object. Our new invariant can be used to distinguish extensions of the p-adic numbers.

Theorem: Let φ be an Eisenstein polynomial of degree p over the p-adic numbers. If φ has a noncyclic Galois group and $v_p(\mathrm{disc}(\varphi)) \neq 2p - 1$, then the extension generated by φ can be uniquely determined by $v_p(\mathrm{disc}(\varphi))$ and the p-adic expansion of $\mathrm{disc}(\varphi)$.

This fact can be used to find Galois groups of polynomials.

Future Research

Next we will work on proving the following conjectures.

Conjecture: Suppose φ and ψ are Eisenstein polynomials over the p-adic numbers and have degree p^m. If φ and ψ generate isomorphic extensions and have cyclic Galois groups, then $v_p(\mathrm{disc}(\varphi) - \mathrm{disc}(\psi)) \geq v_p(\mathrm{disc}(\varphi)) + m + 1$.

Conjecture: If an Eisenstein polynomial over the p-adic numbers generates a cyclic extension, then the first non-zero digit of its discriminant is 1 or $p - 1$.

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