New Points on Plane Curves over Cyclotomic Fields

Quincy Alston (University of Pennsylvania), Gesa Nestler (University of Tennessee, Knoxville), Jack Valerio-Straus (College of William and Mary)

Pomona Research in Mathematics Experience (PRiME)

Abstract

Let C be a curve defined by $f(x,y)=0$ such that $f(x,y)\in\mathbb{Q}[x,y]$. Faltings' theorem relates the amount of solutions to C in $\mathbb{Q}$ to the genus of the curve. This invites one to consider the set of solutions over a finite extension of $\mathbb{Q}$, and which field extensions give new points on the curve. Along these lines, Mazur and Rubin studied curves by understanding the field extensions of $\mathbb{Q}$ generated by a single point on that curve. We ask which field extensions arise this way, what their Galois groups can be, how many there are up to bounded complexity, and how this relates to the geometry of the curve. We explored these questions for different families of plane curves, using parametrization, Newton polygons, linear programming, SageMath, and Hilbert irreducibility.

Background

Definition: Let $K/\mathbb{Q}$ be a Galois field extension. The Galois group G of $K/\mathbb{Q}$, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the group of automorphisms under function composition of K that fix $\mathbb{Q}$.[3]

Inverse Galois Problem: Let G be a finite group. Is there a finite Galois extension $\mathbb{K}/\mathbb{Q}$ such that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})=G$?

In our project we focused on a more specified version of the inverse Galois problem. Let C be a plane curve over $\mathbb{Q}$ (that is, C is the set of points $(x,y)\in\mathbb{C}^2$ such that $F(x,y)=0$ for a fixed polynomial $F(x,y)$). If we consider $\mathbb{Q}(P)$ such that P is a point on C, which groups can arise as $G=\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$?

Lemke Oliver–Thorne produced several field extensions with Galois group S_n by adjoining points on elliptic curves to $\mathbb{Q}$. They also linked the finite quantity of S_n field extensions up to bounded discriminant to the geometry of the curve; Keyes extended this result to hyperelliptic curves.[4] Only n satisfying certain divisibility conditions were considered in this work; indeed, a result of Bhargava, Gross, and Wang outlines that for even-degree hyperelliptic curves, there are "divisibility restrictions' on the parameterizations 100% of the time.[2]

"Parameterization" Method

Definition: Consider a plane curve $F(x,y)=0$. Let $x(t),\ y(t)\in\mathbb{Q}[t]$. Then $F(x(t),y(t))=0$ is a parameterization of $F(x,y)$. Let $\alpha\in\overline{\mathbb{Q}}$. If $F(x(\alpha),y(\alpha))=0$, then $(x(\alpha),y(\alpha))$ is a point on $C: F(x,y)=0$.

The parameterization $x(t)=t$, $y(t)=\frac{g(t)}{h(t)}$ on the hyperelliptic curve $F: y^2=f(x)$ gives the following:

$$\frac{g(t)^2}{h(t)^2}-f(t)=0$$
$$\Theta(t)=g(t)^2-h(t)^2f(t)=0$$

For each root α such that $\Theta(\alpha)=0$, $P=\left(\alpha,\frac{g(\alpha)}{h(\alpha)}\right)$ is a point on F. We adjoin P to $\mathbb{Q}$ so that $\mathbb{Q}\left(\alpha,\frac{g(\alpha)}{h(\alpha)}\right)$ is a Galois extension. The field $\mathbb{Q}\left(\alpha,\frac{g(\alpha)}{h(\alpha)}\right)$ is equal to $\mathbb{Q}(\alpha)$.[4]

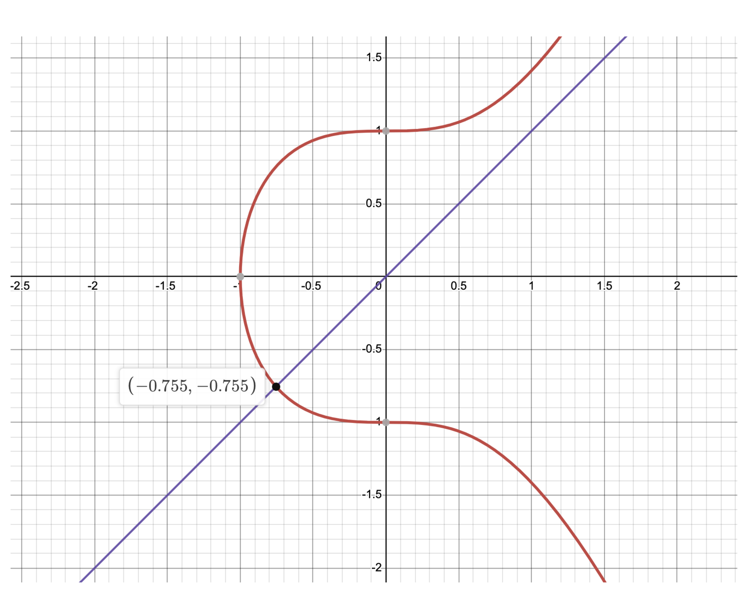

Figure 1: $y^2=x^3+1$

Newton Polygons and Linear Programming

Let $f(x,y)\in\mathbb{Q}[x,y]$ where $f(x,y)=\sum_{i,j}a_{i,j}x^iy^j$ for $0\le i+j\le \deg(f(x,y))$. The Newton polygon of $f(x,y)$ is the convex hull of the set of points (i,j) such that $a_{i,j}$ is non-zero.

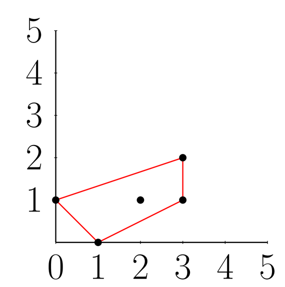

Figure 2: Newton polygon of $h(x,y)=4x^3y^2+3x^2y+x-5x^3y+2y$

Let $x(t),y(t)\in\mathbb{Q}[t]$, and let $n:=\deg x(t)$, $m:=\deg y(t)$. Using the method of linear programming we can compute the degree of $f(x(t),y(t))$ geometrically. If $a_{i,j}x^iy^j$ is a monomial of $f(x,y)$ then the degree of that monomial under $f(x(t),y(t))$ is $in+jm$; this value is maximized at a vertex of the Newton Polygon of f.

Example: let $x(t)=t$ and $y(t)=t$.

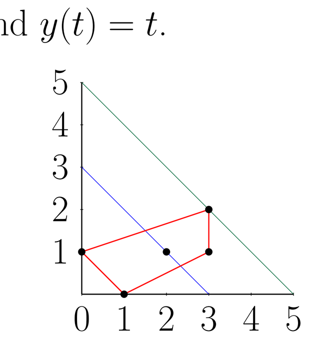

Figure 3: $i+j=3$, monomials with t-degree 3; $i+j=5$, monomials with t-degree 5

Degrees of Parameterizations

Problem: Suppose $\deg f(x)$ is even. can we find parameterizations that give us odd degree extensions that have Galois group that are not S_n?

Example: By the method of linear programming, the possible $\deg F(x(t),y(t))$ for any parameterization $x(t),y(t)\in\mathbb{Q}[t]$ will be a multiple of 2.

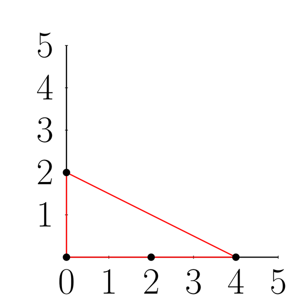

Figure 4: Newton Polygon of $F(x,y)=y^2-x^4-x^2-1=0$

We looked at polynomials $f(x,y)\in\mathbb{Q}[x,y]$ such that $\deg f(x,y)\le 4$. We wanted to see if we could find parameterizations of $f(x,y)$ that give us odd degree $f(x(t),y(t))$.

Let $f(x,y)=\Sigma_k a_{ij}x^iy^j$ and $\deg f(x)=\max\{i+j\,|\,a_{ij}\neq 0\}\le 4$. We partitioned the possible degrees of $f(x,y)$ into sets A and B:

Let

$$A:=\{(1,0),(0,1),(1,1),(2,1),(1,2),(1,3),(3,1)\}$$
$$B:=\{(0,0),(2,2),(2,0),(0,2),(3,0),(0,3),(0,4),(4,0)\}$$

Proposition: Let P be the polygon for $f(x,y)$, and suppose that all of the vertices of P are in set A. Then $\deg f(x,y)$ has no restrictions.

Consider again $f(x,y)$; if all $(i,j)\in B$, then the Newton polygon seemed to impose restrictions on $\deg f(x(t),y(t))$. We wanted to see if a parameterization of $f(x,y)$ caused cancellation of the highest degree terms, if new $\deg f(x(t),y(t))$ occur. To our knowledge, the following result is new:

Theorem 1. [A.–N.–V.]: Let P be the Newton Polygon of $f(x(t),y(t))$, and suppose that degree ordered pairs of $f(x,y)$, including the vertices of P, are elements of the set B. Suppose there exists parameterizations $x(t)$ and $y(t)$, such that the highest degree terms of $f(x(t),y(t))$ cancel. Then the resulting $\deg f(x(t),y(t))$ is restricted to multiples of 2, 3 or 4.

Motivating Question

The Inverse Galois Problem: Let G be a finite group. Is there a finite Galois extension $\mathbb{K}/\mathbb{Q}$ such that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})=G$?

Our Extension: Let C be a plane curve over $\mathbb{Q}$. If we consider $\mathbb{Q}(P)$ such that P is a point on C, which groups can arise as $G=\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$?

S_n Computations

It is a theorem by Bhargava that 100% of polynomials are irreducible and have Galois group S_n.[1] Therefore, if we iterate through random curves and parameterizations $F(x(t),y(t))=g(t)^2-f(t)h(t)^2$ we will likely find 100% S_n Galois groups. Our Sage experiments agree with this result.

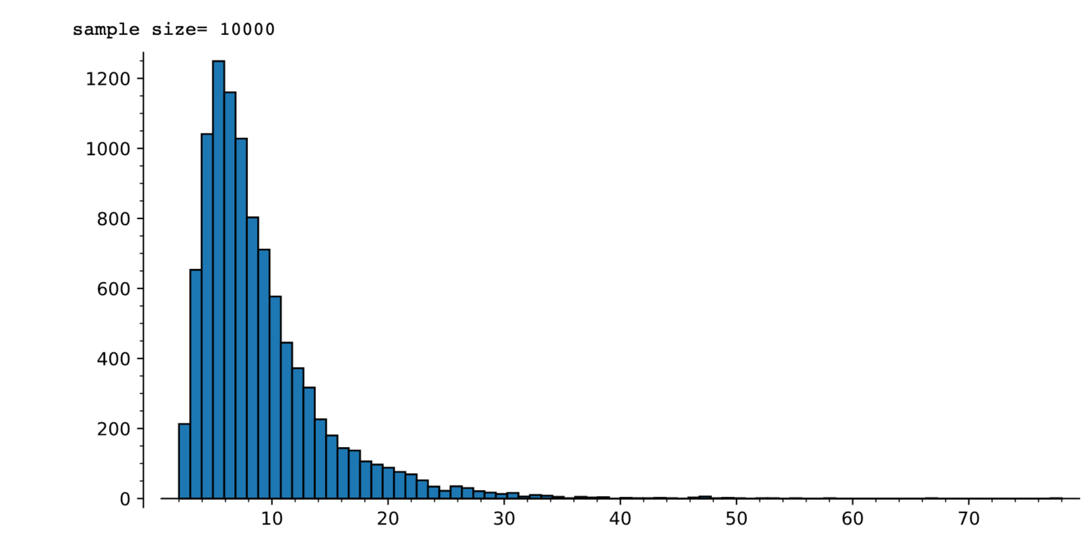

Figure 5: Frequency of a random degree 7 polynomial taking m primes to confirm Galois group S_n.

Reverse Parametrization Strategy

Definition: Let $V=(\mathbb{Z}/n\mathbb{Z})^\times$, and let ζ_n be a primitive nth root of unity. The nth cyclotomic polynomial $\Phi_n(x)=\Pi_{a\in V}(x-\zeta_n^a)$ is the minimal polynomial of the nth primitive roots of unity.[3]

We coded the following algorithm in Sage. Fix $\Theta(t)$ and make a Cartesian product from its coefficients and loop through every element. We set each element of the Cartesian product equal to the coeffecients of a prospective $g(t)^2$. Next, we verify that our choice of $g(t)^2$ is a perfect square by factoring and checking each factor for even multiplicity. If so, for $\Theta(t)=g(t)^2-h(t)^2f(t)=0$ we take $g(t)^2-\Theta(t)=h(t)^2f(t)$. We then factor $h(t)^2f(t)$ and set factors with even multiplicity equal to $h(t)^2$ and odd equal to $f(t)$. We apply this method to the cyclotomic polynomials by setting $\Theta(t)=\Phi_n(t)$.

Selected Cyclotomic Parametrizations

Φ_n	f cyclotomic factors	f non cyclotomic factors	g^2 parameter	h parameter factors
Φ_5	Φ_6		x^2	Φ_2
Φ_{10}	Φ_3		x^2	Φ_1
Φ_{13}	Φ_3,Φ_6,Φ_{14}		x^6	Φ_2
Φ_{17}	$\Phi_4,\Phi_6,\Phi_8,\Phi_{18}$		x^8	Φ_2
Φ_{25}	Φ_6,Φ_{30}		x^{10}	Φ_2,Φ_{10}
Φ_{26}	Φ_3,Φ_6,Φ_7		x^6	Φ_1
Φ_{29}	$\Phi_6,\Phi_7,\Phi_{10},\Phi_{14},\Phi_{30}$		x^{14}	Φ_2
Φ_{34}	$\Phi_3,\Phi_4,\Phi_8,\Phi_9$		x^8	Φ_1
Φ_{35}	$\Phi_3,\Phi_4,\Phi_6,\Phi_8$	$x^{10}-x^9+x^5-x+1$	x^{12}	Φ_1,Φ_2
Φ_{39}	$\Phi_4,\Phi_6,\Phi_7,\Phi_{12},\Phi_{14}$		x^{12}	Φ_1,Φ_2

Table 1: Computed examples of the reverse parameterizations of cyclotomic polynomials by the Keyes method.

Elliptic Curve Group Law

Liu–Lorenzini found an elliptic curve $y^2=-\ell(x)$ with irreducible $\ell(x)$ which parameterized such that $f(x)=h(x)^2+\ell(x)$ where $f(x)=\Phi_3(x)\Phi_4(x)\Phi_5(x)$. Using the group law over elliptic curves and the irreducibility of $\ell(x)$ they found that the curve had a new point over $\mathbb{Q}(\zeta_3,\zeta_4,\zeta_5)=\mathbb{Q}(\zeta_{60})$.[5]

We propose a series of plane curves which give new points over the p^n cyclotomic field with p prime. We are interested in deploying the group law method to find curves with new points over non p^n cyclotomic fields.

Conjectures and Results

Conjecture A: Let $2<n$ and let $\Phi_n(x)$ be a cyclotomic polynomial and let $d=\deg(\Phi_n)$. Then

$$x^{\frac{d}{2}}-\Phi_n(x)=\prod_{j\in S}\Phi_j(x)^2\cdot\prod_{k\in T}\Phi_k(x)\cdot R(x)$$

for some finite $S\subset\mathbb{Z}^+, T\subset\mathbb{Z}^+$ such that $S\cap T=\emptyset$ and for some irreducible polynomial $R(x)\in\mathbb{Q}[x]$. The following conditions also hold:

- $S\cup T\neq\emptyset$
- Either $S=\emptyset$, $1\in S$ or $2\in S$
- If $T=\emptyset$ and $f(x)=1$ then $6\mid n$
- $R(x)$ is monic and $\deg(R(x))$ is even

Conjecture B: If $x(t)=y(t)=t$ then $\exists f(x,y)=g(x)+h(y)$ for $g(x)\in\mathbb{Q}[x]$ and $h(y)\in\mathbb{Q}[y]$ such that the Galois group of $f(x(t),y(t))$ is $\mathrm{D}_{\deg f(x(t),y(t))}$.

Conjecture C: Let p be an odd prime and $m\in\mathbb{Z}^+$. Let

$$F(x,y)=(x^{p^{m-1}})^{p-1}+(y^{p^{m-1}})^{p-2}+\ldots+(y^{p^{m-1}})+1+x+y=0$$

be the associated plane curve of Φ_{p^m}. Then $F(x,y)$ is non-singular at every point $(-\zeta,\zeta)$, such that ζ is a primitive root of $\Phi_{p^m}(t)$.

Theorem 2. [A.–N.–V.]: Consider the plane curve $F(x,y)$ as described in Conjecture C. Then for the parameterization $x(t)=-t, y(t)=t$, if α is a root of $F(x(t),y(t))$, it follows that the Galois group of $\mathbb{Q}(x(\alpha),y(\alpha))$ is abelian.

Conjecture D: Let P be the polygon for $f(x,y)$, and suppose that at least one of the vertices of P is in the set A. Then $\deg f(x,y)$ has no restrictions.

Future Work

- Making a constructive proof of the sets S,T and $R(x)$ in Conjecture A will allow us to generalize a series of Cyclotomics which arise as hyperelliptic curve parameterizations.
- If we can prove Conjecture C, then for every odd prime p and $m\in\mathbb{Z}^+$ we have a formula for a plane curve and a parameterization that yields $\Phi_{p^m}(t)$.

References

[1] M. Bhargava, *Galois groups of random integer polynomials and van der waerden's conjecture*, (2021).

[2] M. Bhargava, B. H. Gross, and X. Wang, *A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension.*, J. Amer. Math. Soc., (2017).

[3] D. S. Dummitt and R. M. Foote, *Abstract Algebra*, Wiley, 3 ed., 2003.

[4] C. D. Keyes, *Growth of points on hyperelliptic curves over number fields*, (2019).

[5] Q. Liu and D. Lorenzini, *New points on curves*, (2017).

Acknowledgements

- Dr. Renee Bell (Lehman College, City University New York)
- Kayla Gibson (Rutgers University)
- Department of Mathematics, Pomona College
- National Science Foundation (DMS-2113782)
- Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author, and do not necessarily reflect the views od the National Science Foundation.