Genus Bounds for Some Dynatomic Modular Curves

UWO Final Thesis Exam Public Lecture

Andrew W. Herring

30 August, 2021

Overview

1. Introduction
2. Function Fields and Curves
3. Flavors of Maximal Subgroups and Genus Bounds

Introduction

Polynomial Dynamical Systems

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;

Polynomial Dynamical Systems

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;
- For a non-constant polynomial $g(x) \in \mathbb{F}[x]$ and a positive integer k, let $g^k(x)$ denote the k-th iterate of g;

Polynomial Dynamical Systems

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;
- For a non-constant polynomial $g(x) \in \mathbb{F}[x]$ and a positive integer k, let $g^k(x)$ denote the k-th iterate of g;
- Define $\mathrm{Per}(g) := \{\alpha \in \bar{\mathbb{F}} : g^k(\alpha) = \alpha, \text{ some } k \geq 1\}$;

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;
- For a non-constant polynomial $g(x) \in \mathbb{F}[x]$ and a positive integer k, let $g^k(x)$ denote the k-th iterate of g;
- Define $\mathrm{Per}(g) := \{\alpha \in \bar{\mathbb{F}} : g^k(\alpha) = \alpha, \text{ some } k \geq 1\}$;
- Elements of $\mathrm{Per}(g)$ are periodic points of g;

Polynomial Dynamical Systems

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;
- For a non-constant polynomial $g(x) \in \mathbb{F}[x]$ and a positive integer k, let $g^k(x)$ denote the k-th iterate of g;
- Define $\mathrm{Per}(g) := \{\alpha \in \bar{\mathbb{F}} : g^k(\alpha) = \alpha, \text{ some } k \geq 1\}$;
- Elements of $\mathrm{Per}(g)$ are periodic points of g;
- The period of $\alpha \in \mathrm{Per}(g)$ is $n := \min\{k \geq 1 : g^k(\alpha) = \alpha\}$;

Polynomial Dynamical Systems

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;
- For a non-constant polynomial $g(x) \in \mathbb{F}[x]$ and a positive integer k, let $g^k(x)$ denote the k-th iterate of g;
- Define $\mathrm{Per}(g) := \{\alpha \in \bar{\mathbb{F}} : g^k(\alpha) = \alpha, \text{ some } k \geq 1\}$;
- Elements of $\mathrm{Per}(g)$ are periodic points of g;
- The period of $\alpha \in \mathrm{Per}(g)$ is $n := \min\{k \geq 1 : g^k(\alpha) = \alpha\}$;
- Define $\mathrm{Per}_n(g) := \{\alpha \in \bar{F} : \alpha \text{ has period } n\}$;

- Let $\mathbb{F}$ be any perfect field with a fixed algebraic closure $\bar{\mathbb{F}}$;
- For a non-constant polynomial $g(x) \in \mathbb{F}[x]$ and a positive integer k, let $g^k(x)$ denote the k-th iterate of g;
- Define $\mathrm{Per}(g) := \{\alpha \in \bar{\mathbb{F}} : g^k(\alpha) = \alpha,$ some $k \geq 1\}$;
- Elements of $\mathrm{Per}(g)$ are periodic points of g;
- The period of $\alpha \in \mathrm{Per}(g)$ is $n := \min\{k \geq 1 : g^k(\alpha) = \alpha\}$;
- Define $\mathrm{Per}_n(g) := \{\alpha \in \bar{F} : \alpha$ has period $n\}$;
- For any subset $S \subseteq \bar{F}$, define $\mathrm{Per}_n(g; S) := \mathrm{Per}_n(g) \cap S$

Motivating Problem

For $c \in \mathbb{Q}$, let $f_c(x) := x^2 + c \in \mathbb{Q}[x]$

Motivating Problem

For $c \in \mathbb{Q}$, let $f_c(x) := x^2 + c \in \mathbb{Q}[x]$

Conjecture: Flynn, Poonen, and Schaefer–1997; [3]

If $n \geq 4$, then $\mathrm{Per}_n(f_c; \mathbb{Q})$ is empty for every $c \in \mathbb{Q}$.

Motivating Problem

For $c \in \mathbb{Q}$, let $f_c(x) := x^2 + c \in \mathbb{Q}[x]$

Conjecture: Flynn, Poonen, and Schaefer–1997; [3]

If $n \geq 4$, then $\mathrm{Per}_n(f_c; \mathbb{Q})$ is empty for every $c \in \mathbb{Q}$.

The conjecture is known to hold for:

Motivating Problem

For $c \in \mathbb{Q}$, let $f_c(x) := x^2 + c \in \mathbb{Q}[x]$

Conjecture: Flynn, Poonen, and Schaefer–1997; [3]

If $n \geq 4$, then $\mathrm{Per}_n(f_c; \mathbb{Q})$ is empty for every $c \in \mathbb{Q}$.

The conjecture is known to hold for:

- $n = 4$; [6]

Motivating Problem

For $c \in \mathbb{Q}$, let $f_c(x) := x^2 + c \in \mathbb{Q}[x]$

Conjecture: Flynn, Poonen, and Schaefer–1997; [3]

If $n \geq 4$, then $\mathrm{Per}_n(f_c; \mathbb{Q})$ is empty for every $c \in \mathbb{Q}$.

The conjecture is known to hold for:

- $n = 4$; [6]
- $n = 5$; [3]

Motivating Problem

For $c \in \mathbb{Q}$, let $f_c(x) := x^2 + c \in \mathbb{Q}[x]$

Conjecture: Flynn, Poonen, and Schaefer–1997; [3]

If $n \geq 4$, then $\mathrm{Per}_n(f_c; \mathbb{Q})$ is empty for every $c \in \mathbb{Q}$.

The conjecture is known to hold for:

- $n = 4$; [6]
- $n = 5$; [3]
- $n = 6^*$; [9]

*Conditional on Birch and Swinnerton-Dyer Conjecture

Example

Let $c = -1 \in \mathbb{Q}$ and consider $f_c(x) = x^2 - 1 \in \mathbb{Q}[x]$.

Example

Let $c = -1 \in \mathbb{Q}$ and consider $f_c(x) = x^2 - 1 \in \mathbb{Q}[x]$.

- Suppose $f_c(\alpha) = \alpha$. Then α is a root of $f_c(x) - x = x^2 - x - 1$.

Example

Let $c = -1 \in \mathbb{Q}$ and consider $f_c(x) = x^2 - 1 \in \mathbb{Q}[x]$.

- Suppose $f_c(\alpha) = \alpha$. Then α is a root of $f_c(x) - x = x^2 - x - 1$.
- But the discriminant $\Delta(x^2 - x - 1) = 5$ is not a square in $\mathbb{Q}$.

Example

Let $c = -1 \in \mathbb{Q}$ and consider $f_c(x) = x^2 - 1 \in \mathbb{Q}[x]$.

- Suppose $f_c(\alpha) = \alpha$. Then α is a root of $f_c(x) - x = x^2 - x - 1$.
- But the discriminant $\Delta(x^2 - x - 1) = 5$ is not a square in $\mathbb{Q}$.
- Thus $\alpha \notin \mathbb{Q}$ and $\mathrm{Per}_1(f_c; \mathbb{Q})$ is empty.

Example

Let $c = -1 \in \mathbb{Q}$ and consider $f_c(x) = x^2 - 1 \in \mathbb{Q}[x]$.

- Suppose $f_c(\alpha) = \alpha$. Then α is a root of $f_c(x) - x = x^2 - x - 1$.
- But the discriminant $\Delta(x^2 - x - 1) = 5$ is not a square in $\mathbb{Q}$.
- Thus $\alpha \notin \mathbb{Q}$ and $\mathrm{Per}_1(f_c; \mathbb{Q})$ is empty.
- Meanwhile, we have

$$f_c(0) = (0)^2 - 1 = -1; \;\; f_c(-1) = (-1)^2 - 1 = 0; \text{ and}$$

$$f_c^2(x) - x = x^4 - 2x^2 - x = x(x+1)(x^2 - x - 1).$$

Example

Let $c = -1 \in \mathbb{Q}$ and consider $f_c(x) = x^2 - 1 \in \mathbb{Q}[x]$.

- Suppose $f_c(\alpha) = \alpha$. Then α is a root of $f_c(x) - x = x^2 - x - 1$.
- But the discriminant $\Delta(x^2 - x - 1) = 5$ is not a square in $\mathbb{Q}$.
- Thus $\alpha \notin \mathbb{Q}$ and $\mathrm{Per}_1(f_c; \mathbb{Q})$ is empty.
- Meanwhile, we have

$$f_c(0) = (0)^2 - 1 = -1; \;\; f_c(-1) = (-1)^2 - 1 = 0; \text{ and}$$

$$f_c^2(x) - x = x^4 - 2x^2 - x = x(x+1)(x^2 - x - 1).$$

- Hence, $\mathrm{Per}_2(f_c; \mathbb{Q}) = \{0, -1\}$.

Motivating Problem–Finitely Many Exceptions

For $n \geq 1$ consider the statement

F.E.(n) ="there are at most finitely many $c \in \mathbb{Q}$ such that $\mathrm{Per}_n(f_c; \mathbb{Q})$ is non-empty"

Motivating Problem–Finitely Many Exceptions

For $n \geq 1$ consider the statement

F.E.(n) ="there are at most finitely many $c \in \mathbb{Q}$ such that $\mathrm{Per}_n(f_c;\mathbb{Q})$ is non-empty"

Theorem: Krumm–2019; [5]

F.E.(n) holds for $n \in \{5,6,7,9\}$.

Motivating Problem–Finitely Many Exceptions

For $n \geq 1$ consider the statement

F.E.(n) =“there are at most finitely many $c \in \mathbb{Q}$ such that $\mathrm{Per}_n(f_c; \mathbb{Q})$ is non-empty”

Theorem: Krumm–2019; [5]

F.E.(n) holds for $n \in \{5, 6, 7, 9\}$.

Theorem: H.–2021

F.E.(n) holds for every $n \geq 10$.

Motivating Problem–Finitely Many Exceptions

For $n \geq 1$ consider the statement

F.E.(n) =“there are at most finitely many $c \in \mathbb{Q}$ such that $\mathrm{Per}_n(f_c;\mathbb{Q})$ is non-empty”

Theorem: Krumm–2019; [5]

F.E.(n) holds for $n \in \{5, 6, 7, 9\}$.

Theorem: H.–2021

F.E.(n) holds for every $n \geq 10$.

Thus F.E.(n) holds for every $n \geq 5$ except possibly for $n = 8$

Dynatomic Polynomials

- Let t be transcendental over $\mathbb{C}$ and consider $K_0 := \mathbb{Q}(t)$, $A_0 := \mathbb{Q}[t]$, and $f(x) := x^2 + t \in A_0[x]$.

Dynatomic Polynomials

- Let t be transcendental over $\mathbb{C}$ and consider $K_0 := \mathbb{Q}(t)$, $A_0 := \mathbb{Q}[t]$, and $f(x) := x^2 + t \in A_0[x]$.
- For $n \geq 1$, the n-th dynatomic polynomial is

$$\Phi_n(x) := \prod_{d|n} \left(f^d(x) - x\right)^{\mu(n/d)}$$

where μ is the Mobius function.

Dynatomic Polynomials

- Let t be transcendental over $\mathbb{C}$ and consider $K_0 := \mathbb{Q}(t)$, $A_0 := \mathbb{Q}[t]$, and $f(x) := x^2 + t \in A_0[x]$.
- For $n \geq 1$, the *n-th dynatomic polynomial* is

$$\Phi_n(x) := \prod_{d|n} \left(f^d(x) - x \right)^{\mu(n/d)}$$

where μ is the Mobius function.

Example:

$$\Phi_1(x) = x^2 - x + t; \;\; \Phi_2(x) = x^2 + x + t + 1$$

$$\Phi_3(x) = x^6 + x^5 + (3t+1)x^4 + (2t+1)x^3 + \left(3t^2 + 3t + 1\right)x^2 + \left(t^2 + 2t + 1\right)x + t^3 + 2t^2 + t + 1$$

Dynatomic Polynomials

Fix $n \geq 1$. Let L_0 denote the splitting field of $\Phi_n(x)$ over K_0 and let $Z := \{\alpha \in L_0 : \Phi_n(\alpha) = 0\}$ denote the zero set of Φ_n.

Dynatomic Polynomials

Fix $n \geq 1$. Let L_0 denote the splitting field of $\Phi_n(x)$ over K_0 and let $Z := \{\alpha \in L_0 : \Phi_n(\alpha) = 0\}$ denote the zero set of Φ_n.

Proposition

The following hold:

Dynatomic Polynomials

Fix $n \geq 1$. Let L_0 denote the splitting field of $\Phi_n(x)$ over K_0 and let $Z := \{\alpha \in L_0 : \Phi_n(\alpha) = 0\}$ denote the zero set of Φ_n.

Proposition

The following hold:

1. $\Phi_n(x) \in A_0[x]$ and $\Phi_n(x)$ is monic in x; [7]

Fix $n \geq 1$. Let L_0 denote the splitting field of $\Phi_n(x)$ over K_0 and let $Z := \{\alpha \in L_0 : \Phi_n(\alpha) = 0\}$ denote the zero set of Φ_n.

Proposition

The following hold:

1. $\Phi_n(x) \in A_0[x]$ and $\Phi_n(x)$ is monic in x; [7]
2. $\Phi_n(x)$ is irreducible over $\mathbb{C}(t)$; [1]

Fix $n \geq 1$. Let L_0 denote the splitting field of $\Phi_n(x)$ over K_0 and let $Z := \{\alpha \in L_0 : \Phi_n(\alpha) = 0\}$ denote the zero set of Φ_n.

Proposition

The following hold:

1. $\Phi_n(x) \in A_0[x]$ and $\Phi_n(x)$ is monic in x; [7]
2. $\Phi_n(x)$ is irreducible over $\mathbb{C}(t)$; [1]
3. $Z = \mathrm{Per}_n(f; \bar{\mathbb{Q}})$;

Dynatomic Polynomials

Fix $n \geq 1$. Let L_0 denote the splitting field of $\Phi_n(x)$ over K_0 and let $Z := \{\alpha \in L_0 : \Phi_n(\alpha) = 0\}$ denote the zero set of Φ_n.

Proposition

The following hold:

1. $\Phi_n(x) \in A_0[x]$ and $\Phi_n(x)$ is monic in x; [7]
2. $\Phi_n(x)$ is irreducible over $\mathbb{C}(t)$; [1]
3. $Z = \mathrm{Per}_n(f; \bar{\mathbb{Q}})$;
4. $\Phi_n(x)$ divides $\Phi_n(f(x))$. [7]

Corollary

Let $r := \frac{\deg \Phi_n(x)}{n}$. Then

$$Z = \sqcup_{i=1}^{r} A_i$$

where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ for some $\alpha_i \in L_0$ for every $i = 1, \ldots r$.

Corollary

Let $r := \frac{\deg \Phi_n(x)}{n}$. Then

$$Z = \sqcup_{i=1}^{r} A_i$$

where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ for some $\alpha_i \in L_0$ for every $i = 1, \ldots r$.

Each set A_i is an f-orbit.

Specializations

Let $c \in \mathbb{Q}$

Specializations

Let $c \in \mathbb{Q}$

- $f_c(x) = x^2 + c = (x^2 + t)\mid_{t=c} = f(x)\mid_{t=c}$, i.e., $f_c(x)$ is a specialization of $f(x)$.

Specializations

Let $c \in \mathbb{Q}$

- $f_c(x) = x^2 + c = (x^2 + t) \mid_{t=c} = f(x) \mid_{t=c}$, i.e., $f_c(x)$ is a specialization of $f(x)$.
- Define

$$\Phi_{n,c}(x) := \Phi_n(x) \mid_{t=c} = \prod_{d|n} \left(f_c^d(x) - x\right)^{\mu(n/d)} \in \mathbb{Q}[x]$$

the n-th dynatomic polynomial at c.

Specializations

Let $c \in \mathbb{Q}$

- $f_c(x) = x^2 + c = (x^2 + t) \mid_{t=c} = f(x) \mid_{t=c}$, i.e., $f_c(x)$ is a specialization of $f(x)$.
- Define

$$\Phi_{n,c}(x) := \Phi_n(x) \mid_{t=c} = \prod_{d \mid n} \left(f_c^d(x) - x \right)^{\mu(n/d)} \in \mathbb{Q}[x]$$

  the n-th dynatomic polynomial at c.
- Let $L_{0,c}$ denote the splitting field of $\Phi_{n,c}(x)$ over $\mathbb{Q}$, and let $Z_c := \{\alpha \in L_{0,c} : \Phi_{n,c}(\alpha) = 0\}$ denote the zero set of $\Phi_{n,c}$.

Specializations

Let $c \in \mathbb{Q}$

- $f_c(x) = x^2 + c = (x^2 + t)\mid_{t=c} = f(x)\mid_{t=c}$, i.e., $f_c(x)$ is a specialization of $f(x)$.
- Define

$$\Phi_{n,c}(x) := \Phi_n(x)\mid_{t=c} = \prod_{d\mid n}\left(f_c^d(x) - x\right)^{\mu(n/d)} \in \mathbb{Q}[x]$$

  the n-th dynatomic polynomial at c.
- Let $L_{0,c}$ denote the splitting field of $\Phi_{n,c}(x)$ over $\mathbb{Q}$, and let $Z_c := \{\alpha \in L_{0,c} : \Phi_{n,c}(\alpha) = 0\}$ denote the zero set of $\Phi_{n,c}$.
- We have $\mathrm{Per}_n(f_c) \subseteq Z_c$, but equality need not hold.

Galois Groups

- L_0/K_0 is a finite Galois extension; let $G := \mathrm{Gal}(L_0/K_0)$ and call it the n-th dynatomic Galois group.

Galois Groups

- L_0/K_0 is a finite Galois extension; let $G := \mathrm{Gal}(L_0/K_0)$ and call it the *n*-th dynatomic Galois group.
- For every $c \in \mathbb{Q}$, also have that $L_{0,c}/\mathbb{Q}$ is a finite Galois extension; let $G_c := \mathrm{Gal}(L_{0,c}/\mathbb{Q})$ and call it the n-th dynatomic Galois group at c.

Galois Groups

- L_0/K_0 is a finite Galois extension; let $G := \mathrm{Gal}(L_0/K_0)$ and call it the n-th dynatomic Galois group.
- For every $c \in \mathbb{Q}$, also have that $L_{0,c}/\mathbb{Q}$ is a finite Galois extension; let $G_c := \mathrm{Gal}(L_{0,c}/\mathbb{Q})$ and call it the n-th dynatomic Galois group at c.
- Define

$$D_n := \{c \in \mathbb{Q} : \Phi_{n,c} \text{ is inseparable}\}.$$

Galois Groups

- L_0/K_0 is a finite Galois extension; let $G := \mathrm{Gal}(L_0/K_0)$ and call it the *n-th dynatomic Galois group*.
- For every $c \in \mathbb{Q}$, also have that $L_{0,c}/\mathbb{Q}$ is a finite Galois extension; let $G_c := \mathrm{Gal}(L_{0,c}/\mathbb{Q})$ and call it the *n-th dynatomic Galois group at c*.
- Define

$$D_n := \{c \in \mathbb{Q} : \Phi_{n,c} \text{ is inseparable}\}.$$

Proposition

If $c \in \mathbb{Q} - D_n$, then $G_c \leq G$.

Galois Groups

- L_0/K_0 is a finite Galois extension; let $G := \mathrm{Gal}(L_0/K_0)$ and call it the n-th dynatomic Galois group.
- For every $c \in \mathbb{Q}$, also have that $L_{0,c}/\mathbb{Q}$ is a finite Galois extension; let $G_c := \mathrm{Gal}(L_{0,c}/\mathbb{Q})$ and call it the n-th dynatomic Galois group at c.
- Define

$$D_n := \{c \in \mathbb{Q} : \Phi_{n,c} \text{ is inseparable}\}.$$

Proposition

If $c \in \mathbb{Q} - D_n$, then $G_c \leq G$.

D_n is the zero set of the discriminant of Φ_n, and is therefore finite.

Exceptional Values

Define

$$E_n := \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

and call it the *n-th exceptional set*. Elements of E_n are *exceptional values*

Exceptional Values

Define

$$E_n := \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

and call it the n-th exceptional set. Elements of E_n are exceptional values

Proposition

If $c \in \mathbb{Q} - D_n$ and $\mathrm{Per}_n(f_c;\mathbb{Q})$ is non-empty, then $c \in E_n$.

Exceptional Values

Define

$$E_n := \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

and call it the n-th exceptional set. Elements of E_n are exceptional values

Proposition

If $c \in \mathbb{Q} - D_n$ and $\mathrm{Per}_n(f_c;\mathbb{Q})$ is non-empty, then $c \in E_n$.

Thus to prove F.E.(n), it suffices to show that E_n is finite.

Exceptional Values

Define

$$E_n := \{c \in \mathbb{Q} - D_n : G_c \lneq G\}$$

and call it the n-th exceptional set. Elements of E_n are exceptional values

Proposition

If $c \in \mathbb{Q} - D_n$ and $\mathrm{Per}_n(f_c; \mathbb{Q})$ is non-empty, then $c \in E_n$.

Thus to prove F.E.(n), it suffices to show that E_n is finite.

Remark

By Hilbert's Irreducibility Theorem, E_n is known to be "thin." Thin sets are small (in a suitable sense), but can still be infinite.

Function Fields and Curves

Equivalent Diagrams

- For a subgroup $H \leq G$, let L_0^H denote the fixed field of H in L_0.

Equivalent Diagrams

- For a subgroup $H \leq G$, let L_0^H denote the fixed field of H in L_0.
- Each of the fields K_0, L_0, and L_0^H is a function field over $\mathbb{Q}$. That is, for every $\mathbb{F} \in \{K_0, L_0, L_0^H\}$, $\mathbb{F}$ is a finitely generated extension of $\mathbb{Q}$ with transcendence degree 1 over $\mathbb{Q}$ and $\mathbb{Q}$ is algebraically closed in $\mathbb{F}$.

Equivalent Diagrams

- For a subgroup $H \leq G$, let L_0^H denote the fixed field of H in L_0.
- Each of the fields K_0, L_0, and L_0^H is a function field over $\mathbb{Q}$. That is, for every $\mathbb{F} \in \{K_0, L_0, L_0^H\}$, $\mathbb{F}$ is a finitely generated extension of $\mathbb{Q}$ with transcendence degree 1 over $\mathbb{Q}$ and $\mathbb{Q}$ is algebraically closed in $\mathbb{F}$.
- By a well-known equivalence of categories, there are curves X, Y, W defined over $\mathbb{Q}$ corresponding to L_0, L_0^H, and K_0, respectively.

Equivalent Diagrams

- For a subgroup $H \leq G$, let L_0^H denote the fixed field of H in L_0.
- Each of the fields K_0, L_0, and L_0^H is a function field over $\mathbb{Q}$. That is, for every $\mathbb{F} \in \{K_0, L_0, L_0^H\}$, $\mathbb{F}$ is a finitely generated extension of $\mathbb{Q}$ with transcendence degree 1 over $\mathbb{Q}$ and $\mathbb{Q}$ is algebraically closed in $\mathbb{F}$.
- By a well-known equivalence of categories, there are curves X, Y, W defined over $\mathbb{Q}$ corresponding to L_0, L_0^H, and K_0, respectively.
- The curve W corresponding to $K_0 = \mathbb{Q}(t)$ is $\mathbb{P}^1_{\mathbb{Q}}$, the projective line defined over $\mathbb{Q}$.

Equivalent Diagrams

- The curve Y corresponding to L_0^H is the quotient curve $X_H \equiv X/H$ whose points are H-orbits under the action of H on X.

Equivalent Diagrams

- The curve Y corresponding to L_0^H is the quotient curve $X_H \equiv X/H$ whose points are H-orbits under the action of H on X.

We therefore have equivalent diagrams

$$
\begin{tikzcd}
L_0 & & & & X \arrow[dl] \arrow[dd, "\pi_G"] \\
& L_0^H \arrow[ul, "H"'] & \begin{array}{c} \longmapsto \\ \longmapsfrom \end{array} & X_H \arrow[dr, "\pi_H"'] & \\
K_0 \arrow[uu, "G"] \arrow[ur] & & & & \mathbb{P}^1_{\mathbb{Q}}
\end{tikzcd}
$$

of function fields and curves over $\mathbb{Q}$.

Equivalent Diagrams

- The curve Y corresponding to L_0^H is the quotient curve $X_H \equiv X/H$ whose points are H-orbits under the action of H on X.

We therefore have equivalent diagrams

$$\begin{tikzcd}
L_0 & & & & X \arrow[dl] \arrow[dd, "\pi_G"] \\
& L_0^H \arrow[ul, "H"'] & \begin{array}{c}\longmapsto \\ \longmapsfrom\end{array} & X_H \arrow[dr, "\pi_H"'] & \\
K_0 \arrow[uu, "G"] \arrow[ur] & & & & \mathbb{P}^1_{\mathbb{Q}}
\end{tikzcd}$$

of function fields and curves over $\mathbb{Q}$.

- Any curve of the form X_H is called a dynatomic modular curve.

Genus of a curve

Let C be any curve defined over $\mathbb{Q}$. We will use $g(C)$ to denote the genus of C which is one measure of the geometric complexity of C.

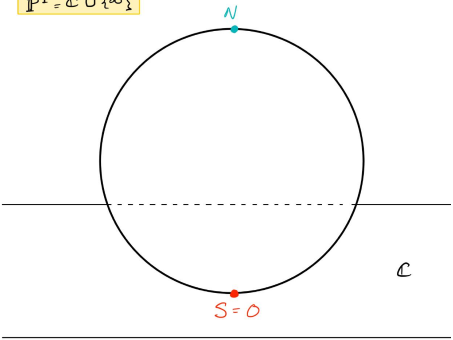
Genus of a curve

Let C be any curve defined over $\mathbb{Q}$. We will use $g(C)$ to denote the genus of C which is one measure of the geometric complexity of C.

By considering C over $\mathbb{C}$, we obtain a compact Riemann surface X; then the genus $g(C)$ counts the number of "holes/handles" of X.

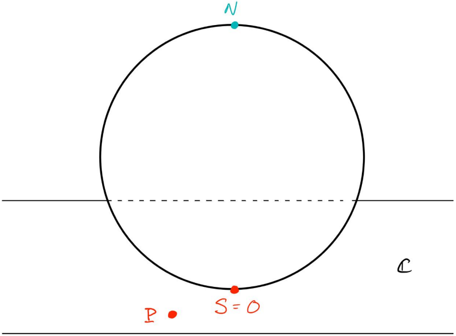
Genus of a curve

$\boxed{\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}}$



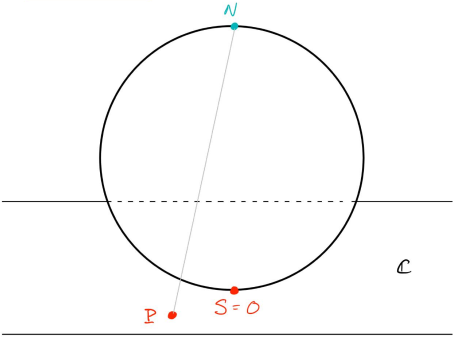
Genus of a curve

$\boxed{\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}}$



Genus of a curve

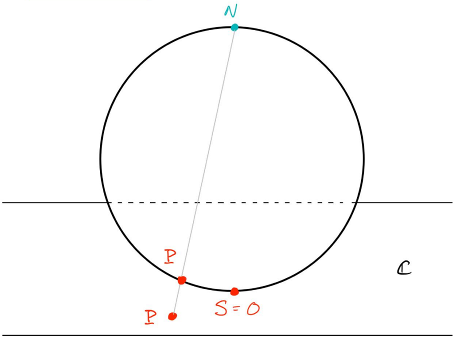
$\boxed{\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}}$



" Stereographic Projection "

Genus of a curve

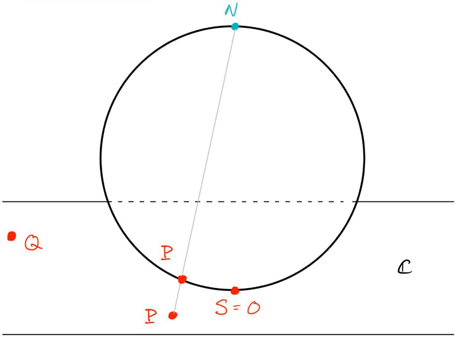
$\boxed{\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}}$



" Stereographic Projection "

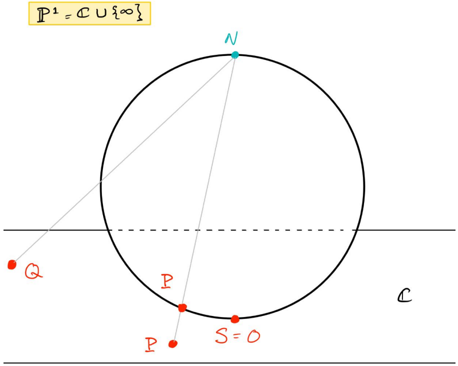
Genus of a curve

$\boxed{\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}}$



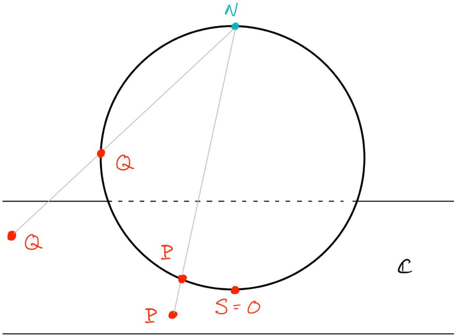
" Stereographic Projection "

Genus of a curve



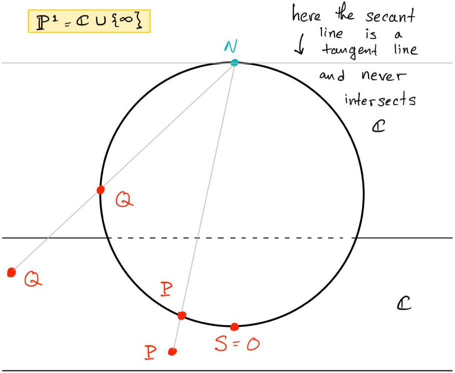
" Stereographic Projection "

$\boxed{\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}}$



" Stereographic Projection "

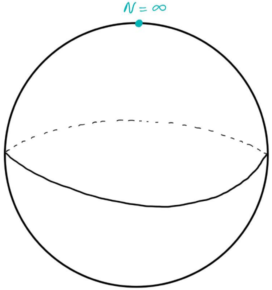
Genus of a curve



" Stereographic Projection "

Genus of a curve

$\mathbb{P}^1 =$

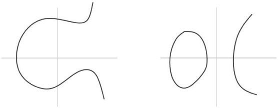


Thus, $g(\mathbb{P}^1) = g($  $) = 0$

Genus of a curve

" elliptic curves "

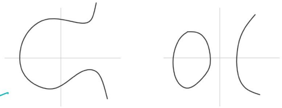
$y^2 = x^3 + ax + b$



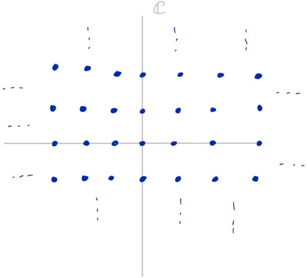
Genus of a curve

" elliptic curves "

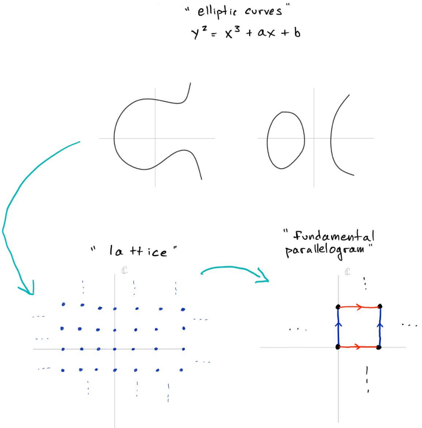
$y^2 = x^3 + ax + b$



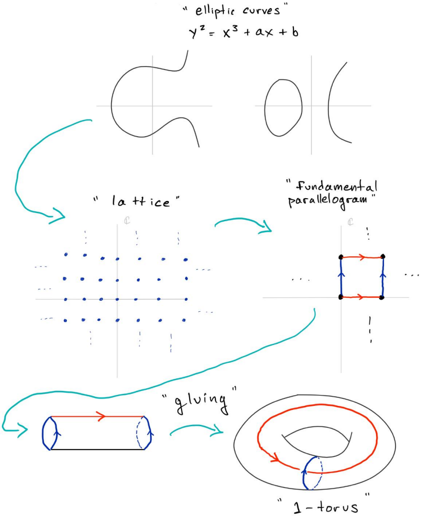
" lattice "



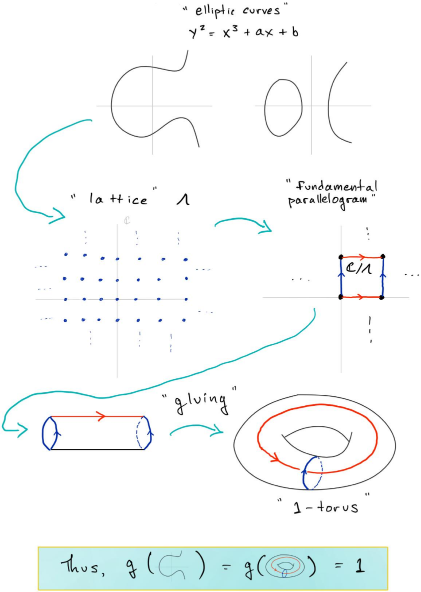
Genus of a curve



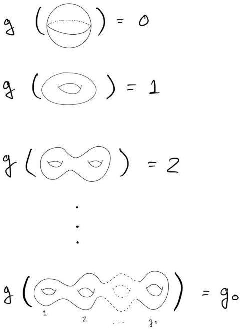
Genus of a curve



Genus of a curve



Genus of a curve



Rational Points and Exceptions

Let C be any curve defined over $\mathbb{Q}$. Let $g(C)$ denote the genus of C, and let $C(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of C.

Rational Points and Exceptions

Let C be any curve defined over $\mathbb{Q}$. Let $g(C)$ denote the genus of C, and let $C(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of C.

Theorem: Faltings–1983; [2]

If $g(C) \geq 2$, then $C(\mathbb{Q})$ is finite.

Rational Points and Exceptions

Let C be any curve defined over $\mathbb{Q}$. Let $g(C)$ denote the genus of C, and let $C(\mathbb{Q})$ denote the set of $\mathbb{Q}$-rational points of C.

Theorem: Faltings–1983; [2]

If $g(C) \geq 2$, then $C(\mathbb{Q})$ is finite.

Theorem: (see Propositions 3.3.1 and 3.3.5 of [8])

Let $c \in \mathbb{Q} - D_n$. Then $c \in E_n$ if and only if $c \in \pi_H(X_H(\mathbb{Q}))$ for some proper subgroup $H \lneq G$.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

1. Suffices that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

1. Suffices that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$.
   - If this holds, then $X_H(\mathbb{Q})$ is finite for every $H \lneq G$ by Faltings.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

1. Suffices that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$.
    - If this holds, then $X_H(\mathbb{Q})$ is finite for every $H \lneq G$ by Faltings.
    - Thus $\pi_H(X_H(\mathbb{Q})) \subset \mathbb{P}^1_{\mathbb{Q}}$ is finite.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

1. Suffices that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$.
   - If this holds, then $X_H(\mathbb{Q})$ is finite for every $H \lneq G$ by Faltings.
   - Thus $\pi_H(X_H(\mathbb{Q})) \subset \mathbb{P}^1_{\mathbb{Q}}$ is finite.
   - Thus E_n is finite by the previous Theorem.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

1. Suffices that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$.
   - If this holds, then $X_H(\mathbb{Q})$ is finite for every $H \lneq G$ by Faltings.
   - Thus $\pi_H(X_H(\mathbb{Q})) \subset \mathbb{P}^1_{\mathbb{Q}}$ is finite.
   - Thus E_n is finite by the previous Theorem.
2. For every $H \lneq G$, there is some maximal subgroup M of G containing H.

Rational Points and Exceptions

Proposition

If $g(X_M) \geq 2$ for every maximal subgroup M of G, then E_n is finite.

Proof sketch:

1. Suffices that $g(X_H) \geq 2$ for every proper subgroup $H \lneq G$.
   - If this holds, then $X_H(\mathbb{Q})$ is finite for every $H \lneq G$ by Faltings.
   - Thus $\pi_H(X_H(\mathbb{Q})) \subset \mathbb{P}^1_{\mathbb{Q}}$ is finite.
   - Thus E_n is finite by the previous Theorem.
2. For every $H \lneq G$, there is some maximal subgroup M of G containing H.
3. $M \supseteq H \iff L^M \subseteq L^H \iff X_H \to X_M$, and genus is non-decreasing along curve morphisms: $g(X_H) \geq g(X_M)$.

Flavors of Maximal Subgroups and Genus Bounds

Semi-Direct Product Structure

Recall our earlier

Corollary

$Z = \sqcup_{i=1}^{r} A_i$, where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ is the i-th f-orbit for every $i \in [r] := \{1, \ldots, r\}$.

Semi-Direct Product Structure

Recall our earlier

Corollary

$Z = \sqcup_{i=1}^{r} A_i$, where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ is the i-th f-orbit for every $i \in [r] := \{1, \ldots, r\}$.

- Let $\Omega := \{A_1, \ldots, A_r\}$ the set of all f-orbits, and let $\Gamma := \mathrm{Sym}(\Omega) \cong S_r$.

Semi-Direct Product Structure

Recall our earlier

Corollary

$Z = \sqcup_{i=1}^{r} A_i$, where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ is the i-th f-orbit for every $i \in [r] := \{1, \ldots, r\}$.

- Let $\Omega := \{A_1, \ldots, A_r\}$ the set of all f-orbits, and let $\Gamma := \mathrm{Sym}(\Omega) \cong S_r$.
- For every $\sigma \in G = \mathrm{Gal}(L_0/K_0)$ we have that $\sigma \circ f^j = f^j \circ \sigma$ for every j.

Semi-Direct Product Structure

Recall our earlier

Corollary

$Z = \sqcup_{i=1}^{r} A_i$, where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ is the i-th f-orbit for every $i \in [r] := \{1, \ldots, r\}$.

- Let $\Omega := \{A_1, \ldots, A_r\}$ the set of all f-orbits, and let $\Gamma := \mathrm{Sym}\,(\Omega) \cong S_r$.
- For every $\sigma \in G = \mathrm{Gal}(L_0/K_0)$ we have that $\sigma \circ f^j = f^j \circ \sigma$ for every j.
- Thus $\sigma(A_i) \in \Omega$ for every $i \in [r]$ and there's a permutation σ on $\Omega \equiv [r]$ given by $A_i \mapsto \sigma(A_i) \equiv A_{\sigma(i)}$

Semi-Direct Product Structure

Recall our earlier

Corollary

$Z = \sqcup_{i=1}^{r} A_i$, where $A_i = \{\alpha_i, f(\alpha_i), \ldots, f^{n-1}(\alpha_i)\}$ is the i-th f-orbit for every $i \in [r] := \{1, \ldots, r\}$.

- Let $\Omega := \{A_1, \ldots, A_r\}$ the set of all f-orbits, and let $\Gamma := \mathrm{Sym}(\Omega) \cong S_r$.
- For every $\sigma \in G = \mathrm{Gal}(L_0/K_0)$ we have that $\sigma \circ f^j = f^j \circ \sigma$ for every j.
- Thus $\sigma(A_i) \in \Omega$ for every $i \in [r]$ and there's a permutation σ on $\Omega \equiv [r]$ given by $A_i \mapsto \sigma(A_i) \equiv A_{\sigma(i)}$
- Get a permutation representation $\phi : G \to \Gamma$; let $N := \ker(\phi)$.

Semi-Direct Product Structure

Claim

The following hold:

Semi-Direct Product Structure

Claim

The following hold:

1. $N \cong (\mathbb{Z}/n)^r$;

Semi-Direct Product Structure

Claim

The following hold:

1. $N \cong (\mathbb{Z}/n)^r$;
2. ϕ is surjective. Thus ϕ is precisely the quotient homomorphism $\pi : G \twoheadrightarrow G/N \cong \Gamma$;

Semi-Direct Product Structure

Claim

The following hold:

1. $N \cong (\mathbb{Z}/n)^r$;
2. ϕ is surjective. Thus ϕ is precisely the quotient homomorphism $\pi : G \twoheadrightarrow G/N \cong \Gamma$;
3. $\Gamma = S_r$ acts by automorphisms on $N = (\mathbb{Z}/n)^r$ via ${}^{\tau}(a_1, \ldots, a_r) := (a_{\tau(1)}, \ldots, a_{\tau(r)})$;

Semi-Direct Product Structure

Claim

The following hold:

1. $N \cong (\mathbb{Z}/n)^r$;
2. ϕ is surjective. Thus ϕ is precisely the quotient homomorphism $\pi : G \twoheadrightarrow G/N \cong \Gamma$;
3. $\Gamma = S_r$ acts by automorphisms on $N = (\mathbb{Z}/n)^r$ via ${}^{\tau}(a_1, \ldots, a_r) := (a_{\tau(1)}, \ldots, a_{\tau(r)})$;
4. The semi-direct product $N \rtimes \Gamma = (\mathbb{Z}/n)^r \rtimes S_r$ is defined, and in fact $G \cong N \rtimes \Gamma$ [1].

Flavors of Maximal Subgroups

We partition the maximal subgroups M of G according to whether $\pi(M) = \Gamma$, or $\pi(M) \lneq \Gamma$.

Flavors of Maximal Subgroups

We partition the maximal subgroups M of G according to whether $\pi(M) = \Gamma$, or $\pi(M) \lneq \Gamma$.

Lemma: Vanilla Maximal Subgroups

If $\pi(M) = \Gamma$, then $N \cap M$ is maximal amongst all Γ-invariant subgroups of N.

Flavors of Maximal Subgroups

We partition the maximal subgroups M of G according to whether $\pi(M) = \Gamma$, or $\pi(M) \lneq \Gamma$.

Lemma: Vanilla Maximal Subgroups

If $\pi(M) = \Gamma$, then $N \cap M$ is maximal amongst all Γ-invariant subgroups of N.

We call any maximal M of G with $\pi(M) = \Gamma$ a vanilla maximal subgroup of G.

Flavors of Maximal Subgroups

We partition the maximal subgroups M of G according to whether $\pi(M) = \Gamma$, or $\pi(M) \lneq \Gamma$.

Lemma: Vanilla Maximal Subgroups

If $\pi(M) = \Gamma$, then $N \cap M$ is maximal amongst all Γ-invariant subgroups of N.

We call any maximal M of G with $\pi(M) = \Gamma$ a vanilla maximal subgroup of G.

Lemma: Chocolate Maximal Subgroups

If $\pi(M) \lneq \Gamma$, then $N \subseteq M$ and $\pi(M)$ is a maximal subgroup of Γ.

Flavors of Maximal Subgroups

We partition the maximal subgroups M of G according to whether $\pi(M) = \Gamma$, or $\pi(M) \lneq \Gamma$.

Lemma: Vanilla Maximal Subgroups

If $\pi(M) = \Gamma$, then $N \cap M$ is maximal amongst all Γ-invariant subgroups of N.

We call any maximal M of G with $\pi(M) = \Gamma$ a vanilla maximal subgroup of G.

Lemma: Chocolate Maximal Subgroups

If $\pi(M) \lneq \Gamma$, then $N \subseteq M$ and $\pi(M)$ is a maximal subgroup of Γ.

We call any maximal M of G with $\pi(M) \lneq \Gamma$ a chocolate maximal subgroup of G.

Genus Bounds for Chocolate Maximals

Theorem

For every $n \geq 5$ and every chocolate maximal subgroup M of G we have $g(X_M) \geq 2$.

Genus Bounds for Chocolate Maximals

Theorem

For every $n \geq 5$ and every chocolate maximal subgroup M of G we have $g(X_M) \geq 2$.

Ideas:

Genus Bounds for Chocolate Maximals

Theorem

For every $n \geq 5$ and every chocolate maximal subgroup M of G we have $g(X_M) \geq 2$.

Ideas:

1. Krumm ([5]) showed that for $n \in \{5, 6, 7, 9\}$, we have $g(X_M) \geq 2$ for *every* maximal subgroup M of G; in particular this holds for the chocolate maximals.

Genus Bounds for Chocolate Maximals

Theorem

For every $n \geq 5$ and every chocolate maximal subgroup M of G we have $g(X_M) \geq 2$.

Ideas:

1. Krumm ([5]) showed that for $n \in \{5, 6, 7, 9\}$, we have $g(X_M) \geq 2$ for *every* maximal subgroup M of G; in particular this holds for the chocolate maximals.
2. For $n \geq 8$, we can use a powerful theorem of Guralnick and Shareshian ([4]) to show that $g(X_M) \geq 2$ for every chocolate maximal M.

Genus Bounds for Vanilla Maximals

Theorem

For every $n \geq 10$, we have that $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G.

Genus Bounds for Vanilla Maximals

Theorem

For every $n \geq 10$, we have that $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G.

Ideas:

Genus Bounds for Vanilla Maximals

Theorem

For every $n \geq 10$, we have that $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G.

Ideas:

1. For every vanilla maximal M, there is a prime ℓ dividing n and a positive integer e such that $[G : M] = \ell^e$.

Genus Bounds for Vanilla Maximals

Theorem

For every $n \geq 10$, we have that $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G.

Ideas:

1. For every vanilla maximal M, there is a prime ℓ dividing n and a positive integer e such that $[G : M] = \ell^e$.
2. Further, for one type of ramified point of $X_M \to \mathbb{P}^1$ we will always have ramification index ℓ, and there will be $\varphi(n)$ many such ramified points.

Genus Bounds for Vanilla Maximals

Theorem

For every $n \geq 10$, we have that $g(X_M) \geq 2$ for every vanilla maximal subgroup M of G.

Ideas:

1. For every vanilla maximal M, there is a prime ℓ dividing n and a positive integer e such that $[G : M] = \ell^e$.
2. Further, for one type of ramified point of $X_M \to \mathbb{P}^1$ we will always have ramification index ℓ, and there will be $\varphi(n)$ many such ramified points.
3. Plug this data into the Riemann-Hurwitz genus formula to prove the Theorem in the cases $n = 11$ and $n \geq 13$.

Genus Bounds for Vanilla Maximals

Ideas:

1. For every vanilla maximal M, there is a prime ℓ dividing n and a positive integer e such that $[G : M] = \ell^e$.
2. Further, for one type of ramified point of $X_M \to \mathbb{P}^1$ we will always have ramification index ℓ, and there will be $\varphi(n)$ many such ramified points.
3. Plug this data into the Riemann-Hurwitz genus formula to prove the Theorem for $n = 11$ and $n \geq 13$.
4. For $n = 10$ and $n = 12$, we have $\varphi(n) = 4$ and $\ell = 2$ is a possibility—these values do not contribute enough in Riemann-Hurwitz to deduce $g(X_M) \geq 2$

Genus Bounds for Vanilla Maximals

Ideas:

1. For every vanilla maximal M, there is a prime ℓ dividing n and a positive integer e such that $[G : M] = \ell^e$.
2. Further, for one type of ramified point of $X_M \to \mathbb{P}^1$ we will always have ramification index ℓ, and there will be $\varphi(n)$ many such ramified points.
3. Plug this data into the Riemann-Hurwitz genus formula to prove the Theorem for $n = 11$ and $n \geq 13$.
4. For $n = 10$ and $n = 12$, we have $\varphi(n) = 4$ and $\ell = 2$ is a possibility—these values do not contribute enough in Riemann-Hurwitz to deduce $g(X_M) \geq 2$
5. In these cases we consider a second type of ramified point corresponding to prime divisors p of n other than 2, i.e., $p = 5$ for $n = 10$ and $p = 3$ for $n = 12$.

[1] Thierry Bousch. “Sur quelques problemes de dynamique holomorphe”. PhD thesis. Paris 11, 1992.

[2] G. Faltings. “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern”. In: *Invent. Math.* 73.3 (1983), pp. 349–366.

[3] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer. “Cycles of quadratic polynomials and rational points on a genus-2 curve”. In: *Duke Math. J.* 90.3 (1997), pp. 435–463.

[4] Robert M. Guralnick and John Shareshian. "Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points". In: *Mem. Amer. Math. Soc.* 189.886 (2007), pp. vi+128.

[5] David Krumm. "A finiteness theorem for specializations of dynatomic polynomials". In: *Algebra & Number Theory* 13.4 (2019), pp. 963–993.

[6] Patrick Morton. "Arithmetic properties of periodic points of quadratic maps, II". In: *Acta Arithmetica* 87.2 (1998), pp. 89–102.

[7] Patrick Morton and Pratiksha Patel. "The Galois theory of periodic points of polynomial maps". In: *Proc. London Math. Soc. (3)* 68.2 (1994), pp. 225–263. ISSN: 0024-6115.

[8] Jean-Pierre Serre. *Topics in Galois theory*. Second. Vol. 1. Research Notes in Mathematics. A K Peters, Ltd., Wellesley, MA, 2008.

[9] Michael Stoll. "Rational 6-cycles under iteration of quadratic polynomials". In: *LMS Journal of Computation and Mathematics* 11 (2008), pp. 367–380.

THE
END