# Dodecic 3-adic fields

*Chad Awtrey*

**Elon University**
cawtrey@elon.edu

December 3, 2011

# Motivation #1

## Theorem

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number.*

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question:

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$:

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  7 if $p = 2$;

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  7 if $p = 2$; 3 otherwise

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  $$7 \text{ if } p = 2; \quad 3 \text{ otherwise}$$

- Tamely ramified extensions (i.e. $p \nmid n$):

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  $$7 \text{ if } p = 2; \quad 3 \text{ otherwise}$$

- Tamely ramified extensions (i.e. $p \nmid n$):
  - let $n = ef$

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  $$7 \text{ if } p = 2; \quad 3 \text{ otherwise}$$

- Tamely ramified extensions (i.e. $p \nmid n$):
  - let $n = ef \quad g = \gcd(p^f - 1, e)$

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  7 if $p = 2$; 3 otherwise
- Tamely ramified extensions (i.e. $p \nmid n$):
  - let $n = ef$ $g = \gcd(p^f - 1, e)$
  - partition $\mathbf{Z}/g\mathbf{Z}$ into orbits under multiplication by $p$

# Motivation #1

**Theorem**

*Let $n$ be a positive integer and $p$ a prime number. There are only finitely many extensions of $\mathbf{Q}_p$ of degree $n$.*

- Obvious question: How many are there?
- In certain cases, we know the answer.
- Unramified extensions of degree $n$: only one.
- Quadratic extensions:

  7 if $p = 2$; 3 otherwise
- Tamely ramified extensions (i.e. $p \nmid n$):
  - let $n = ef$ $g = \gcd(p^f - 1, e)$
  - partition $\mathbf{Z}/g\mathbf{Z}$ into orbits under multiplication by $p$
  - #orbits = #extensions

# How many?

- What about wildly ramified extensions $(p \mid n)$?

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$:

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$: $\quad p^2 + 1$

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$: $\quad p^2 + 1$
- What if $p \mid n$ and $n$ is composite?

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$: $\quad p^2 + 1$
- What if $p \mid n$ and $n$ is composite?
- No general formula is known.

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$: $\quad p^2 + 1$
- What if $p \mid n$ and $n$ is composite?
- No general formula is known.
- Jones/Roberts have pursued some low-degree cases.

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$: $\quad p^2 + 1$
- What if $p \mid n$ and $n$ is composite?
- No general formula is known.
- Jones/Roberts have pursued some low-degree cases.

  For example,

# How many?

- What about wildly ramified extensions $(p \mid n)$?
- Degree $p$ extensions of $\mathbf{Q}_p$: $\quad p^2 + 1$
- What if $p \mid n$ and $n$ is composite?
- No general formula is known.
- Jones/Roberts have pursued some low-degree cases.

  For example,

| **(p,n)** | (2,4) | (2,6) | (3,6) | (2,8) | (3,9) | (2,10) | (5,10) |
|---|---|---|---|---|---|---|---|
| # | 59 | 47 | 75 | **1834** | 795 | 158 | 258 |

## Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.

## Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

## Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.
- To study $K$, we can determine arithmetic invariants of the $K_j$, such as

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.
- To study $K$, we can determine arithmetic invariants of the $K_j$, such as

  discriminant

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.
- To study $K$, we can determine arithmetic invariants of the $K_j$, such as

  discriminant
  ramification index

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.
- To study $K$, we can determine arithmetic invariants of the $K_j$, such as

  discriminant
  ramification index
  residue degree

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.
- To study $K$, we can determine arithmetic invariants of the $K_j$, such as

  discriminant
  ramification index
  residue degree
  subfields

# Motivation #2

- Let $K/\mathbf{Q}$ be defined by some monic irreducible $f(x) \in \mathbf{Z}[x]$.
- Factor $f$ over $\mathbf{Q}_p$ to obtain $K$'s associated $p$-adic algebra,

$$K \otimes \mathbf{Q}_p \simeq \prod_{j=1}^{m} K_j$$

- each $K_j$ is a finite extension of $\mathbf{Q}_p$, defined by the corresponding irreducible factor of $f$.
- To study $K$, we can determine arithmetic invariants of the $K_j$, such as

  discriminant
  ramification index
  residue degree
  subfields
  Galois group

# This Talk

- In this talk, we'll discuss a technique for determining

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield
     - narrow down the list of possible Galois groups

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield
     - narrow down the list of possible Galois groups
  2. Compute a defining polynomial (which gives the number of extensions)

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield
     - narrow down the list of possible Galois groups
  2. Compute a defining polynomial (which gives the number of extensions)
  3. Compute the Galois group of each polynomial over $\mathbf{Q}_3$

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield
     - narrow down the list of possible Galois groups
  2. Compute a defining polynomial (which gives the number of extensions)
  3. Compute the Galois group of each polynomial over $\mathbf{Q}_3$
- Item 2. can be done using the methods of Pauli/Roblot.

# This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield
     - narrow down the list of possible Galois groups
  2. Compute a defining polynomial (which gives the number of extensions)
  3. Compute the Galois group of each polynomial over $\mathbf{Q}_3$
- Item 2. can be done using the methods of Pauli/Roblot. Our method is a slight variation, and computationally less expensive.

## This Talk

- In this talk, we'll discuss a technique for determining
  - the number of degree 12 extensions of $\mathbf{Q}_3$
  - the Galois group of the normal closure of each extension
- Here's the strategy
  1. Use ramification groups to
     - show each such extension has a unique quartic subfield
     - narrow down the list of possible Galois groups
  2. Compute a defining polynomial (which gives the number of extensions)
  3. Compute the Galois group of each polynomial over $\mathbf{Q}_3$
- Item 2. can be done using the methods of Pauli/Roblot. Our method is a slight variation, and computationally less expensive.
- Item 3. uses a mix of absolute/relative resolvents and subfield invariants.

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Higher ramification group theory gives:

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Higher ramification group theory gives:
  - $G$ is a solvable transitive subgroup of $S_{12}$ (there are 265).

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Higher ramification group theory gives:
  - $G$ is a solvable transitive subgroup of $S_{12}$ (there are 265).
  - $G$ contains a solvable normal subgroup $G_0$ such that $G/G_0$ is cyclic of order dividing 12.

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Higher ramification group theory gives:
  - $G$ is a solvable transitive subgroup of $S_{12}$ (there are 265).
  - $G$ contains a solvable normal subgroup $G_0$ such that $G/G_0$ is cyclic of order dividing 12.
  - $G_0$ contains a normal subgroup $G_1$ such that $G_1$ is a 3-group (possibly trivial).

# Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Higher ramification group theory gives:
  - $G$ is a solvable transitive subgroup of $S_{12}$ (there are 265).
  - $G$ contains a solvable normal subgroup $G_0$ such that $G/G_0$ is cyclic of order dividing 12.
  - $G_0$ contains a normal subgroup $G_1$ such that $G_1$ is a 3-group (possibly trivial).
  - $G_0/G_1$ is cyclic of order dividing $3^{[G:G_0]} - 1$.

## Ramification Groups

- Suppose $[K : \mathbf{Q}_3] = 12$.
- Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Higher ramification group theory gives:
  - $G$ is a solvable transitive subgroup of $S_{12}$ (there are 265).
  - $G$ contains a solvable normal subgroup $G_0$ such that $G/G_0$ is cyclic of order dividing 12.
  - $G_0$ contains a normal subgroup $G_1$ such that $G_1$ is a 3-group (possibly trivial).
  - $G_0/G_1$ is cyclic of order dividing $3^{[G:G_0]} - 1$.
- Only 45 of the 265 groups pass the test.

# Possible Galois Groups

Using notation in `Gap`, these groups are `TransitiveGroup(12,n)`, where $n$ is one of:

# Possible Galois Groups

Using notation in `Gap`, these groups are `TransitiveGroup(12,n)`, where $n$ is one of:

*1, 2, 3, 5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 34, 35, 36, 38, 39, 40, 41, 42, 46, 47, 70, 71, 72, 73, 84, 116, 118, 119, 120, 121, 130, 131, 167, 169, 170, 171, 172, 173, 174, 212, 215, 216*

# Possible Galois Groups

Using notation in `Gap`, these groups are `TransitiveGroup(12,n)`, where $n$ is one of:

*1, 2, 3, 5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 34, 35, 36, 38, 39, 40, 41, 42, 46, 47, 70, 71, 72, 73, 84, 116, 118, 119, 120, 121, 130, 131, 167, 169, 170, 171, 172, 173, 174, 212, 215, 216*

**Note:**

# Possible Galois Groups

Using notation in `Gap`, these groups are `TransitiveGroup(12,n)`, where $n$ is one of:

*1, 2, 3, 5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 34, 35, 36, 38, 39, 40, 41, 42, 46, 47, 70, 71, 72, 73, 84, 116, 118, 119, 120, 121, 130, 131, 167, 169, 170, 171, 172, 173, 174, 212, 215, 216*

**Note:**

`TransitiveGroup(12,1)` $= C_{12}$.

# Possible Galois Groups

Using notation in `Gap`, these groups are `TransitiveGroup(12,n)`, where $n$ is one of:

*1, 2, 3, 5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 34, 35, 36, 38, 39, 40, 41, 42, 46, 47, 70, 71, 72, 73, 84, 116, 118, 119, 120, 121, 130, 131, 167, 169, 170, 171, 172, 173, 174, 212, 215, 216*

**Note:**

`TransitiveGroup(12,1)` $= C_{12}$.

`TransitiveGroup(12,301)` $= S_{12}$.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.
- Specifically,
  - Let $L$ be a subfield of $K$.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.
- Specifically,
  - Let $L$ be a subfield of $K$.
  - Let $F$ be its corresponding intermediate group,

# Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.
- Specifically,
  - Let $L$ be a subfield of $K$.
  - Let $F$ be its corresponding intermediate group,
  - Let $G$ act on the cosets of $F$.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.
- Specifically,
  - Let $L$ be a subfield of $K$.
  - Let $F$ be its corresponding intermediate group,
  - Let $G$ act on the cosets of $F$.
  - The permutation representation of this action is the Galois group of $L^{\mathrm{gal}}/\mathbf{Q}_3$. (We'll use this later)!

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.
- Specifically,
  - Let $L$ be a subfield of $K$.
  - Let $F$ be its corresponding intermediate group,
  - Let $G$ act on the cosets of $F$.
  - The permutation representation of this action is the Galois group of $L^{\mathrm{gal}}/\mathbf{Q}_3$. (We'll use this later)!
- Direct computation shows all 45 groups have a unique such intermediate group $F$ of index 4.

## Unique Quartic Subfield

- **Claim:** $K/\mathbf{Q}_3$ has a unique quartic subfield.
- **Proof:** Let $G = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbf{Q}_3)$.
- Let $E \subseteq G$ be the subgroup that fixes $K$.
- The non-isomorphic subfields of $K$ correspond to conjugacy classes of intermediate subgroups $F$ such that $E \subseteq F \subseteq G$.
- Specifically,
  - Let $L$ be a subfield of $K$.
  - Let $F$ be its corresponding intermediate group,
  - Let $G$ act on the cosets of $F$.
  - The permutation representation of this action is the Galois group of $L^{\mathrm{gal}}/\mathbf{Q}_3$. (We'll use this later)!
- Direct computation shows all 45 groups have a unique such intermediate group $F$ of index 4.
- Thus all extensions $K$ have a unique quartic subfield.

## Defining Polynomials

- **Corollary:** Every degree 12 extension of $\mathbf{Q}_3$ can be realized uniquely as a cubic extension of a quartic 3-adic field.

# Defining Polynomials

- **Corollary:** Every degree 12 extension of $\mathbf{Q}_3$ can be realized uniquely as a cubic extension of a quartic 3-adic field.
- Defining polynomials can therefore be computed by evaluating appropriate resultants.

# Defining Polynomials

- **Corollary:** Every degree 12 extension of $\mathbf{Q}_3$ can be realized uniquely as a cubic extension of a quartic 3-adic field.
- Defining polynomials can therefore be computed by evaluating appropriate resultants.
- Quartic 3-adic fields are tamely ramified, therefore easily classified.

# Defining Polynomials

- **Corollary:** Every degree 12 extension of $\mathbf{Q}_3$ can be realized uniquely as a cubic extension of a quartic 3-adic field.
- Defining polynomials can therefore be computed by evaluating appropriate resultants.
- Quartic 3-adic fields are tamely ramified, therefore easily classified.

| **e** | **f** | **poly** |
|---|---|---|
| 1 | 4 | $x^4 - x + 2$ |
| 2 | 2 | $x^4 + 9x^2 + 36$ |
| 2 | 2 | $x^4 - 3x^2 + 18$ |
| 4 | 1 | $x^4 + 3$ |
| 4 | 1 | $x^4 - 3$ |

## Ramification Groups

- We use Amano's methods for determining cubic extensions of the quartic 3-adic fields.

## Ramification Groups

- We use Amano's methods for determining cubic extensions of the quartic 3-adic fields.
- Using resultants, we produce a list of degree 12 polynomials.

# Ramification Groups

- We use Amano's methods for determining cubic extensions of the quartic 3-adic fields.
- Using resultants, we produce a list of degree 12 polynomials.
- Panayi's $p$-adic root-finding algorithm is used to discard isomorphic extensions.

## Ramification Groups

- We use Amano's methods for determining cubic extensions of the quartic 3-adic fields.
- Using resultants, we produce a list of degree 12 polynomials.
- Panayi's $p$-adic root-finding algorithm is used to discard isomorphic extensions.
- We get 785 degree 12 extensions of $\mathbf{Q}_3$.

## Ramification Groups

- We use Amano's methods for determining cubic extensions of the quartic 3-adic fields.
- Using resultants, we produce a list of degree 12 polynomials.
- Panayi's $p$-adic root-finding algorithm is used to discard isomorphic extensions.
- We get 785 degree 12 extensions of $\mathbf{Q}_3$.
- Krasner's mass formula proves that these are all such extensions.

## Ramification Groups

- We use Amano's methods for determining cubic extensions of the quartic 3-adic fields.
- Using resultants, we produce a list of degree 12 polynomials.
- Panayi's $p$-adic root-finding algorithm is used to discard isomorphic extensions.
- We get 785 degree 12 extensions of $\mathbf{Q}_3$.
- Krasner's mass formula proves that these are all such extensions.

$$\text{mass}(K/\mathbf{Q}_3) = \frac{12}{|\text{Aut}(K/\mathbf{Q}_3)|}$$

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.
- The strategy:

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.
- The strategy:
  - Divide the list of 45 groups into smaller pieces that are easily distinguished from each other.

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.
- The strategy:
  - Divide the list of 45 groups into smaller pieces that are easily distinguished from each other.
  - First, use centralizer order.

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.
- The strategy:
  - Divide the list of 45 groups into smaller pieces that are easily distinguished from each other.
  - First, use centralizer order.

$$|C_{S_{12}}(G)| = |\mathrm{Aut}(K/\mathbf{Q}_3)|$$

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.
- The strategy:
  - Divide the list of 45 groups into smaller pieces that are easily distinguished from each other.
  - First, use centralizer order.

$$|C_{S_{12}}(G)| = |\mathrm{Aut}(K/\mathbf{Q}_3)|$$

  - Next use Galois groups of subfields and parity.

# Distinguishing Galois Groups

- We follow the standard approach for determining Galois groups.
- Compute enough group-theoretic and field-theoretic invariants so as to uniquely identify a polynomial with its corresponding Galois group.
- The strategy:
  - Divide the list of 45 groups into smaller pieces that are easily distinguished from each other.
  - First, use centralizer order.

$$|C_{S_{12}}(G)| = |\mathrm{Aut}(K/\mathbf{Q}_3)|$$

  - Next use Galois groups of subfields and parity.
  - When this information is not enough, introduce various resolvent polynomials.

# Centralizer Order 12

| **T** | $\mathbf{\lvert C_{S_{12}}(G)\rvert}$ | **subfields** | $\mathbf{\#Q_3^{12}}$ |
|---|---|---|---|
| 1 | 12 | 2T1,3T1,4T1,6T1 | 8 |
| 2 | 12 | 2T1,2T1,2T1,3T1,4T2,6T1,6T1,6T1 | 4 |
| 3 | 12 | 2T1,2T1,2T1,3T2,4T2,6T2,6T3,6T3 | 6 |
| 5 | 12 | 2T1,3T2,4T1,6T2 | 2 |

# Centralizer Order 4 or 6

| **T** | $\|\mathbf{C_{S_{12}}(G)}\|$ | **subfields** | $\#\mathbf{Q}_3^{12}$ |
|---|---|---|---|
| 11 | 4 | 2T1, 3T2, 4T1, 6T3 | 10 |
| 14 | 6 | 2T1, 3T1, 4T3, 6T1 | 8 |
| 15 | 6 | 2T1, 3T2, 4T3, 6T2 | 5 |
| 16 | 6 | 2T1, 2T1, 2T1, 4T2, 6T9 | 9 |
| 17 | 6 | 2T1, 4T1, 6T10 | 4 |
| 18 | 6 | 2T1, 2T1, 2T1, 4T2, 6T5 | 24 |
| 19 | 6 | 2T1, 4T1, 6T5 | 8 |
| 35 | 6 | 2T1, 4T3, 6T13 | 8 |
| 42 | 6 | 2T1, 4T3, 6T5 | 40 |

# Centralizer Order 3

- Nine groups have centralizer order equal to three.

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.
  - Then $f_{66}(x) = g(\sqrt{x})$.

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.
  - Then $f_{66}(x) = g(\sqrt{x})$.
  - Equivalently, let $r_1, \ldots, r_{12}$ be the roots of $f$.

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.
  - Then $f_{66}(x) = g(\sqrt{x})$.
  - Equivalently, let $r_1, \ldots, r_{12}$ be the roots of $f$.

$$f_{66}(x) = \prod_{i=1}^{11} \prod_{j=i+1}^{12} (x - r_i - r_j)$$

# Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.
  - Then $f_{66}(x) = g(\sqrt{x})$.
  - Equivalently, let $r_1, \ldots, r_{12}$ be the roots of $f$.

$$f_{66}(x) = \prod_{i=1}^{11} \prod_{j=i+1}^{12} (x - r_i - r_j)$$

  - Factor $f_{66}$ over $\mathbf{Q}_3$, and consider degree 18 factors.

## Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.
  - Then $f_{66}(x) = g(\sqrt{x})$.
  - Equivalently, let $r_1, \ldots, r_{12}$ be the roots of $f$.

$$f_{66}(x) = \prod_{i=1}^{11} \prod_{j=i+1}^{12} (x - r_i - r_j)$$

  - Factor $f_{66}$ over $\mathbf{Q}_3$, and consider degree 18 factors.
  - Compute Galois groups of polynomials defining cubic subfields.

## Centralizer Order 3

- Nine groups have centralizer order equal to three.
- Galois groups of subfields are not enough.
- We use the following degree 66 absolute resolvent $f_{66}(x)$,
  - Let $g(x) = \text{Resultant}_y(f(y), f(x+y))/x^{12}$.
  - Then $f_{66}(x) = g(\sqrt{x})$.
  - Equivalently, let $r_1, \ldots, r_{12}$ be the roots of $f$.

$$f_{66}(x) = \prod_{i=1}^{11} \prod_{j=i+1}^{12} (x - r_i - r_j)$$

  - Factor $f_{66}$ over $\mathbf{Q}_3$, and consider degree 18 factors.
  - Compute Galois groups of polynomials defining cubic subfields.
  - In the next table, we call this column **Cubic Subs**.

# Centralizer Order 3

| **T** | **subfields** | $\mathbf{f_{66}}$ | **Cubic Subs** | $\#\mathbf{Q}_3^{12}$ |
|---|---|---|---|---|
| 70 | 2T1, 2T1, 2T1, 4T2 | [12,18,18,18] | 3T1, 3T2, 3T2 | 36 |
| 71 | 2T1, 2T1, 2T1, 4T2 | [12,18,18,18] | 3T2, 3T2, 3T2 | 4 |
| 130 | 2T1, 2T1, 2T1, 4T2 | [12,18,18,18] | none | 32 |
| 72 | 2T1, 4T1 | [12,18,36] | 3T2 | 4 |
| 73 | 2T1, 4T1 | [12,18,36] | 3T1 | 16 |
| 131 | 2T1, 4T1 | [12,18,36] | none | 32 |
| 116 | 2T1, 4T3 | [12,18,36] | 3T2 | 20 |
| 121 | 2T1, 4T3 | [12,18,36] | 3T1 | 32 |
| 167 | 2T1, 4T3 | [12,18,36] | none | 160 |

# Centralizer Order 2

- Eight groups have centralizer order equal to 2.

# Centralizer Order 2

- Eight groups have centralizer order equal to 2.
- All but the groups 12T12 and 12T13 can be distinguished by their subfield content.

# Centralizer Order 2

- Eight groups have centralizer order equal to 2.
- All but the groups 12T12 and 12T13 can be distinguished by their subfield content.
- For these two groups, their corresponding fields each have a unique cubic and quartic subfield.

# Centralizer Order 2

- Eight groups have centralizer order equal to 2.
- All but the groups 12T12 and 12T13 can be distinguished by their subfield content.
- For these two groups, their corresponding fields each have a unique cubic and quartic subfield.
- If the Galois group is 12T12, the discriminant of the cubic subfield times the discriminant of the quartic subfield is a not a square.

# Centralizer Order 2

- Eight groups have centralizer order equal to 2.
- All but the groups 12T12 and 12T13 can be distinguished by their subfield content.
- For these two groups, their corresponding fields each have a unique cubic and quartic subfield.
- If the Galois group is 12T12, the discriminant of the cubic subfield times the discriminant of the quartic subfield is a not a square.
- For the group 12T13, this quantity is a square.

# Centralizer Order 2

- Eight groups have centralizer order equal to 2.
- All but the groups 12T12 and 12T13 can be distinguished by their subfield content.
- For these two groups, their corresponding fields each have a unique cubic and quartic subfield.
- If the Galois group is 12T12, the discriminant of the cubic subfield times the discriminant of the quartic subfield is a not a square.
- For the group 12T13, this quantity is a square.
- See column $\mathbf{d_3} \cdot \mathbf{d_4} = \square$.

# Centralizer Order 2

| **T** | **subfields** | $\mathbf{d_3 \cdot d_4 = \square}$ | $\#\mathbf{Q}_3^{12}$ |
|---|---|---|---|
| 12 | 2T1, 3T2, 4T3, 6T3 | no | 2 |
| 13 | 2T1, 3T2, 4T3, 6T3 | yes | 5 |
| 34 | 2T1, 2T1, 2T1, 4T2, 6T13 | | 8 |
| 36 | 2T1, 4T3, 6T13 | | 8 |
| 38 | 2T1, 4T3, 6T9 | | 10 |
| 39 | 2T1, 4T1, 6T9 | | 8 |
| 40 | 2T1, 2T1, 2T1, 4T2, 6T10 | | 4 |
| 41 | 2T1, 4T1, 6T10 | | 4 |

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.
- We divide the 15 candidates into three sets:

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.
- We divide the 15 candidates into three sets:
  - those with two subfields and where $G \subseteq A_{12}$

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.
- We divide the 15 candidates into three sets:
  - those with two subfields and where $G \subseteq A_{12}$
  - those with two subfields and where $G \nsubseteq A_{12}$

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.
- We divide the 15 candidates into three sets:
  - those with two subfields and where $G \subseteq A_{12}$
  - those with two subfields and where $G \nsubseteq A_{12}$
  - those with four subfields.

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.
- We divide the 15 candidates into three sets:
  - those with two subfields and where $G \subseteq A_{12}$
  - those with two subfields and where $G \nsubseteq A_{12}$
  - those with four subfields.
- There are six groups in the first set.

# Centralizer Order 1

- 15 groups have centralizer order equal to 1.
- Corresponding fields have either two or four proper nontrivial subfields.
- We divide the 15 candidates into three sets:
  - those with two subfields and where $G \subseteq A_{12}$
  - those with two subfields and where $G \nsubseteq A_{12}$
  - those with four subfields.
- There are six groups in the first set.
- We use two resolvents, $f_{220}$ and $f_8$.

# Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.

# Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

# Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k)$$

## Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k)$$

- The other resolvent makes use of the unique quartic subfield.

## Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k)$$

- The other resolvent makes use of the unique quartic subfield.
  - Let $L$ be the unique quartic subfield of $K$.

## Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k)$$

- The other resolvent makes use of the unique quartic subfield.
  - Let $L$ be the unique quartic subfield of $K$.
  - Let $g$ be a cubic polynomial obtained by factoring $f$ over $L$.

## Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k)$$

- The other resolvent makes use of the unique quartic subfield.
  - Let $L$ be the unique quartic subfield of $K$.
  - Let $g$ be a cubic polynomial obtained by factoring $f$ over $L$.
  - Let $f_8(x)$ be the norm of $x^2 - \mathrm{disc}(g(x))$ from $L$ down to $\mathbf{Q}_3$.

## Centralizer Order 1

- Let $f(x)$ define a degree 12 extension over $\mathbf{Q}_3$.
- Let $r_1, \ldots, r_{12}$ be its roots.

$$f_{220}(x) = \prod_{i=1}^{10} \prod_{j=i+1}^{11} \prod_{k=j+1}^{12} (x - r_i - r_j - r_k)$$

- The other resolvent makes use of the unique quartic subfield.
  - Let $L$ be the unique quartic subfield of $K$.
  - Let $g$ be a cubic polynomial obtained by factoring $f$ over $L$.
  - Let $f_8(x)$ be the norm of $x^2 - \mathrm{disc}(g(x))$ from $L$ down to $\mathbf{Q}_3$.
  - Compute the Galois group of $f_8(x)$ over $\mathbf{Q}_3$, (easy since it defines a tamely ramified extension).

# Centralizer Order 1

| **T** | **subfields** | $\mathbf{f_{220}}$ | $\mathbf{f_8}$ | $\#\mathbf{Q}_3^{12}$ |
|---|---|---|---|---|
| 46 | 2T1, 4T1 | [4,36,36,36,36,72] | 8T1 | 4 |
| 173 | 2T1, 4T1 | [4,36,36,36,108] | 8T1 | 16 |
| 215 | 2T1, 4T1 | [4,36,36,36,108] | 8T7 | 20 |
| 84 | 2T1, 4T3 | [4,36,36,72,72] | 8T8 | 16 |
| 212 | 2T1, 4T3 | [4,36,72,108] | 8T8 | 48 |
| 216 | 2T1, 4T3 | [4,36,72,108] | 8T6 | 16 |

# Centralizer Order 1

- The second set has five groups.

# Centralizer Order 1

- The second set has five groups.
- We make use of $f_{66}$, from before.

# Centralizer Order 1

- The second set has five groups.
- We make use of $f_{66}$, from before.
- Factor $f_{66}$ over $\mathbf{Q}_3$.

# Centralizer Order 1

- The second set has five groups.
- We make use of $f_{66}$, from before.
- Factor $f_{66}$ over $\mathbf{Q}_3$.
- We get three factors of degrees 12, 18, and 36, respectively.

## Centralizer Order 1

- The second set has five groups.
- We make use of $f_{66}$, from before.
- Factor $f_{66}$ over $\mathbf{Q}_3$.
- We get three factors of degrees 12, 18, and 36, respectively.
- Consider sextic subfields of the field defined by the degree 18 factor.

## Centralizer Order 1

- The second set has five groups.
- We make use of $f_{66}$, from before.
- Factor $f_{66}$ over $\mathbf{Q}_3$.
- We get three factors of degrees 12, 18, and 36, respectively.
- Consider sextic subfields of the field defined by the degree 18 factor.
- Compute the Galois groups of the polynomials defining these sextic fields.

## Centralizer Order 1

- The second set has five groups.
- We make use of $f_{66}$, from before.
- Factor $f_{66}$ over $\mathbf{Q}_3$.
- We get three factors of degrees 12, 18, and 36, respectively.
- Consider sextic subfields of the field defined by the degree 18 factor.
- Compute the Galois groups of the polynomials defining these sextic fields.

# Centralizer Order 1

| **T** | **subfields** | $\mathbf{f_{66}}$ | **Sextic Subs** | $\#\mathbf{Q}_3^{12}$ |
|---|---|---|---|---|
| 118 | 2T1, 4T3 | [12,18,36] | 6T3 | 8 |
| 120 | 2T1, 4T3 | [12,18,36] | 6T13 | 20 |
| 169 | 2T1, 4T3 | [12,18,36] | 6T9 | 40 |
| 119 | 2T1, 4T1 | [12,18,36] | 6T3 | 20 |
| 170 | 2T1, 4T1 | [12,18,36] | 6T9 | 32 |

# Centralizer Order 1

- There are four groups in the third and final set.

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,
  - Factor $f_{66}$ over $\mathbf{Q}_3$.

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,
  - Factor $f_{66}$ over $\mathbf{Q}_3$.
  - We get four factors of degrees 12, 18, 18, and 18, respectively.

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,
  - Factor $f_{66}$ over $\mathbf{Q}_3$.
  - We get four factors of degrees 12, 18, 18, and 18, respectively.
  - Consider again sextic subfields of the fields defined by the degree 18 factors.

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,
  - Factor $f_{66}$ over $\mathbf{Q}_3$.
  - We get four factors of degrees 12, 18, 18, and 18, respectively.
  - Consider again sextic subfields of the fields defined by the degree 18 factors.
  - Compute Galois groups of the polynomials defining these sextic subfields.

# Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,
  - Factor $f_{66}$ over $\mathbf{Q}_3$.
  - We get four factors of degrees 12, 18, 18, and 18, respectively.
  - Consider again sextic subfields of the fields defined by the degree 18 factors.
  - Compute Galois groups of the polynomials defining these sextic subfields.
  - This distinguishes two groups.

## Centralizer Order 1

- There are four groups in the third and final set.
- We use $f_{66}$ and $f_{220}$ from before.
- First,
  - Factor $f_{66}$ over $\mathbf{Q}_3$.
  - We get four factors of degrees 12, 18, 18, and 18, respectively.
  - Consider again sextic subfields of the fields defined by the degree 18 factors.
  - Compute Galois groups of the polynomials defining these sextic subfields.
  - This distinguishes two groups.
- For other two groups, use the list of degrees of the irreducible factors of $f_{220}$.

# Centralizer Order 1

| **T** | $\mathbf{f_{66}}$ | $\mathbf{f_{220}}$ | **Sextic Subs** | $\#\mathbf{Q}_3^{12}$ |
|---|---|---|---|---|
| 47 | [12,18,18,18] | [4,36,36,36,36,72] | none | 4 |
| 171 | [12,18,18,18] | [4,36,36,36,108] | 6T10,6T10 | 8 |
| 172 | [12,18,18,18] | [4,36,36,36,108] | 6T13,6T13,6T13,6T13 | 6 |
| 174 | [12,18,18,18] | [4,36,36,36,108] | none | 6 |

# THANK YOU!