A nonsolvable polynomial with field discriminant 5^{69}

David P. Roberts
University of Minnesota, Morris

September 24, 2009

1. Gross's observation from the mid-1990s
2. Some context and related work from ≤ 2007
3. Results of Dembélé, Serre, and (Dembélé, Greenberg, and Voight) from ≥ 2008
4. A nonsolvable polynomial $g_{25}(x)$ with field discriminant 5^{69}
5. How special is $g_{25}(x)$?
6. How was $g_{25}(x)$ found?
7. How is 5 ramified in $g_{25}(x)$?

1a. Gross's observation from the mid-1990s

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field.

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example:

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$,

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field,

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field.

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\mathrm{disc}(g(x)) \; =$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\mathrm{disc}(g(x)) = 1,240,578,719,095,233,176$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\mathrm{disc}(g(x)) \;=\; 1,240,578,719,095,233,176 \;=\; 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned} \mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 = 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(K/\mathbf{Q}) &= \end{aligned}$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned} \mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 = 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(K/\mathbf{Q}) &= \quad 356,385,727,979,096 = \end{aligned}$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned} \mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 = 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 = 2^3 \cdot 558913 \cdot 79705099 \end{aligned}$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$
\begin{aligned}
\mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 = 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 = 2^3 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(L/\mathbf{Q}) &=
\end{aligned}
$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned} \mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 &&= 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 &&= 2^3 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(L/\mathbf{Q}) &= (45,307,555,206 \text{ digits}) &&= \end{aligned}$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{array}{rcccl} \mathrm{disc}(g(x)) & = & 1,240,578,719,095,233,176 & = & 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(K/\mathbf{Q}) & = & 356,385,727,979,096 & = & 2^3 \cdot 558913 \cdot 79705099 \\ \mathrm{disc}(L/\mathbf{Q}) & = & (45,307,555,206 \text{ digits}) & = & 2^* \cdot 558913^* \cdot 79705099^* \end{array}$$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned}
\mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 &= 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 &= 2^3 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(L/\mathbf{Q}) &= (45,307,555,206 \text{ digits}) &= 2^* \cdot 558913^* \cdot 79705099^*
\end{aligned}$$

The invariants for L are

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned}
\mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 &&= 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 &&= 2^3 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(L/\mathbf{Q}) &= (45,307,555,206 \text{ digits}) &&= 2^* \cdot 558913^* \cdot 79705099^*
\end{aligned}$$

The invariants for L are $G = S_{13}$

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned}
\mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 &&= 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 &&= 2^3 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(L/\mathbf{Q}) &= (45,307,555,206 \text{ digits}) &&= 2^* \cdot 558913^* \cdot 79705099^*
\end{aligned}$$

The invariants for L are $G = S_{13}$ and $S = \{2, 558913, 79705099\}$.)

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned}
\mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 = 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 = 2^3 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(L/\mathbf{Q}) &= (45,307,555,206 \text{ digits}) = 2^* \cdot 558913^* \cdot 79705099^*
\end{aligned}$$

The invariants for L are $G = S_{13}$ and $S = \{2, 558913, 79705099\}$.)

Gross observed that there was not a single number field known for which G was nonsolvable and S consisted of a single prime ≤ 7.

1a. Gross's observation from the mid-1990s

Let $L \subset \mathbf{C}$ be a Galois number field. Then two of its most basic invariants are its Galois group $G = \mathrm{Gal}(L/\mathbf{Q})$ and the set of primes S dividing its discriminant $\mathrm{disc}(L/\mathbf{Q})$.

(Random example: Let $g(x) = x^{13} + x^2 + 2$, let $K = \mathbf{Q}[x]/g(x)$ be its stem field, and let L be its splitting field. Then

$$\begin{aligned}
\mathrm{disc}(g(x)) &= 1,240,578,719,095,233,176 = 2^3 \cdot 59^2 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(K/\mathbf{Q}) &= 356,385,727,979,096 = 2^3 \cdot 558913 \cdot 79705099 \\
\mathrm{disc}(L/\mathbf{Q}) &= (45,307,555,206 \text{ digits}) = 2^* \cdot 558913^* \cdot 79705099^*
\end{aligned}$$

The invariants for L are $G = S_{13}$ and $S = \{2, 558913, 79705099\}$.)

Gross observed that there was not a single number field known for which G was nonsolvable and S consisted of a single prime ≤ 7. He conjectured that such fields do exist.

1b. Root discriminants

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

$$\delta_F = \left|\mathrm{disc}(F/\mathbf{Q})\right|^{1/[F:\mathbf{Q}]}.$$

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

$$\delta_F = \left|\mathrm{disc}(F/\mathbf{Q})\right|^{1/[F:\mathbf{Q}]}.$$

For $g(x) \in \mathbf{Q}[x]$ with stem field K and splitting field L one has $\delta_K \leq \delta_L$.

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

$$\delta_F = |\mathrm{disc}(F/\mathbf{Q})|^{1/[F:\mathbf{Q}]}.$$

For $g(x) \in \mathbf{Q}[x]$ with stem field K and splitting field L one has $\delta_K \leq \delta_L$.

(Random example continued:

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

$$\delta_F = |\mathrm{disc}(F/\mathbf{Q})|^{1/[F:\mathbf{Q}]}.$$

For $g(x) \in \mathbf{Q}[x]$ with stem field K and splitting field L one has $\delta_K \leq \delta_L$.

(Random example continued: For $g(x) = x^{13} + x^2 + 2$ the root discriminants are

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

$$\delta_F = |\mathrm{disc}(F/\mathbf{Q})|^{1/[F:\mathbf{Q}]}.$$

For $g(x) \in \mathbf{Q}[x]$ with stem field K and splitting field L one has $\delta_K \leq \delta_L$.

(Random example continued: For $g(x) = x^{13} + x^2 + 2$ the root discriminants are

$$\delta_K = 2^{3/13} 558913^{1/13} 79705099^{1/13} \approx 13.16$$

1b. Root discriminants

It is often best to work with *root discriminants* of number fields,

$$\delta_F = |\mathrm{disc}(F/\mathbf{Q})|^{1/[F:\mathbf{Q}]}.$$

For $g(x) \in \mathbf{Q}[x]$ with stem field K and splitting field L one has $\delta_K \leq \delta_L$.

(Random example continued: For $g(x) = x^{13} + x^2 + 2$ the root discriminants are

$$\begin{array}{rcl@{\quad}c@{\quad}r} \delta_K & = & 2^{3/13} 558913^{1/13} 79705099^{1/13} & \approx & 13.16 \\ \delta_L & = & 2^{3/2} 558913^{1/2} 79705099^{1/2} & \approx & 18,878,181.27) \end{array}$$

2a. Some context and related work from ≤ 2007

2a. Some context and related work from $\leq$ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p.

2a. Some context and related work from ≤ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

2a. Some context and related work from $\leq$ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

B. From classical modular forms one knows that for each prime $p \geq 11$ there exists at least one field L with $G = PGL_2(p)$ and $S = \{p\}$ (Deligne, Swinnerton-Dyer).

2a. Some context and related work from ≤ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

B. From classical modular forms one knows that for each prime $p \geq 11$ there exists at least one field L with $G = PGL_2(p)$ and $S = \{p\}$ (Deligne, Swinnerton-Dyer).

C. It is general hard to get defining equations for the fields in **B.**

2a. Some context and related work from $\leq$ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

B. From classical modular forms one knows that for each prime $p \geq 11$ there exists at least one field L with $G = PGL_2(p)$ and $S = \{p\}$ (Deligne, Swinnerton-Dyer).

C. It is general hard to get defining equations for the fields in **B.** An easy case is the unique field for $p = 11$, which comes from 11-torsion points of an elliptic curve with j-invariant $-64/297$.

2a. Some context and related work from $\leq$ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

B. From classical modular forms one knows that for each prime $p \geq 11$ there exists at least one field L with $G = PGL_2(p)$ and $S = \{p\}$ (Deligne, Swinnerton-Dyer).

C. It is general hard to get defining equations for the fields in **B.** An easy case is the unique field for $p = 11$, which comes from 11-torsion points of an elliptic curve with j-invariant $-64/297$. Then $f(x) =$

$$x^{12} + 90p^2x^6 - 640p^2x^4 + 2280p^2x^3 - 512p^2x^2 + 2432px - p^3$$

has Galois group $PGL_2(11)$

2a. Some context and related work from $\leq$ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

B. From classical modular forms one knows that for each prime $p \geq 11$ there exists at least one field L with $G = PGL_2(p)$ and $S = \{p\}$ (Deligne, Swinnerton-Dyer).

C. It is general hard to get defining equations for the fields in **B.** An easy case is the unique field for $p = 11$, which comes from 11-torsion points of an elliptic curve with j-invariant $-64/297$. Then $f(x) =$

$$x^{12} + 90p^2x^6 - 640p^2x^4 + 2280p^2x^3 - 512p^2x^2 + 2432px - p^3$$

has Galois group $PGL_2(11)$ and $f(x^2)$ has Galois group $SL_2^{\pm}(11)$ (Jones-R.).

2a. Some context and related work from ≤ 2007

A. It is easy to produce solvable fields ramified only at a single given prime p. Example (Galois): the splitting field of $x^p - p$ has $G = \mathbf{F}_p : \mathbf{F}_p^\times$.

B. From classical modular forms one knows that for each prime $p \geq 11$ there exists at least one field L with $G = PGL_2(p)$ and $S = \{p\}$ (Deligne, Swinnerton-Dyer).

C. It is general hard to get defining equations for the fields in **B.** An easy case is the unique field for $p = 11$, which comes from 11-torsion points of an elliptic curve with j-invariant $-64/297$. Then $f(x) =$

$$x^{12} + 90p^2x^6 - 640p^2x^4 + 2280p^2x^3 - 512p^2x^2 + 2432px - p^3$$

has Galois group $PGL_2(11)$ and $f(x^2)$ has Galois group $SL_2^{\pm}(11)$ (Jones-R.). Harder cases of **B** worked out by Bosman.

2b. Some context and related work from $\leq$ 2007

2b. Some context and related work from ≤ 2007

D. From the theory of three-point covers (= Belyi maps=*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7.

2b. Some context and related work from ≤ 2007

D. From the theory of three-point covers (= Belyi maps=*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7. Example (R.): $G = S_{15875}$ and $S = \{2, 5\}$.

2b. Some context and related work from $\leq$ 2007

D. From the theory of three-point covers (= Belyi maps=*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7. Example (R.): $G = S_{15875}$ and $S = \{2, 5\}$.

E. Gross's conjectures have been pursued in detail.

2b. Some context and related work from ≤ 2007

D. From the theory of three-point covers (= Belyi maps=*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7. Example (R.): $G = S_{15875}$ and $S = \{2, 5\}$.

E. Gross's conjectures have been pursued in detail. Example (Lansky and Pollack): there should be a field with $G = G_2(5)$ and $S = \{5\}$.

2b. Some context and related work from ≤ 2007

D. From the theory of three-point covers (= Belyi maps=*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7. Example (R.): $G = S_{15875}$ and $S = \{2, 5\}$.

E. Gross's conjectures have been pursued in detail. Example (Lansky and Pollack): there should be a field with $G = G_2(5)$ and $S = \{5\}$. Some Frobenius information for this conjectural field has been computed, but there seems to be no hope of finding a defining polynomial.

2b. Some context and related work from ≤ 2007

D. From the theory of three-point covers (= Belyi maps=*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7. Example (R.): $G = S_{15875}$ and $S = \{2, 5\}$.

E. Gross's conjectures have been pursued in detail. Example (Lansky and Pollack): there should be a field with $G = G_2(5)$ and $S = \{5\}$. Some Frobenius information for this conjectural field has been computed, but there seems to be no hope of finding a defining polynomial.

F. In the other direction, some $(G, \{p\})$ have been eliminated as possibilities by comparison with Odylzko's bounds for discriminants.

2b. Some context and related work from ≤ 2007

D. From the theory of three-point covers ($=$ Belyi maps$=$*dessins d'enfants*), it is easy to get explicit polynomials for many nonsolvable L ramified at two primes ≤ 7. Example (R.): $G = S_{15875}$ and $S = \{2, 5\}$.

E. Gross's conjectures have been pursued in detail. Example (Lansky and Pollack): there should be a field with $G = G_2(5)$ and $S = \{5\}$. Some Frobenius information for this conjectural field has been computed, but there seems to be no hope of finding a defining polynomial.

F. In the other direction, some $(G, \{p\})$ have been eliminated as possibilities by comparison with Odylzko's bounds for discriminants. Example (Jones): for $5 \leq n \leq 15$, there are no fields with $G = A_n$ or S_n and $S = \{2\}$.

3a. Results of Dembélé and Serre from 2008

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions.

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions. It has $G = SL_2(2^8)^2.8$

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions. It has $G = SL_2(2^8)^2.8$ and $S = \{2\}$.

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions. It has $G = SL_2(2^8)^2.8$ and $S = \{2\}$. Dembélé also proved that the root discriminant δ_L

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions. It has $G = SL_2(2^8)^2.8$ and $S = \{2\}$. Dembélé also proved that the root discriminant δ_L is less than $2^{5.875} \approx 58.68$.

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions. It has $G = SL_2(2^8)^2.8$ and $S = \{2\}$. Dembélé also proved that the root discriminant δ_L is less than $2^{5.875} \approx 58.68$.

Serre then improved the exponent from 5.875 to

$$\alpha = 1518251/262144 \approx 5.79.$$

3a. Results of Dembélé and Serre from 2008

In 2008, Dembélé used computations with Hilbert modular forms to prove the existence of the first field L known to satisfy Gross's conditions. It has $G = SL_2(2^8)^2.8$ and $S = \{2\}$. Dembélé also proved that the root discriminant δ_L is less than $2^{5.875} \approx 58.68$.

Serre then improved the exponent from 5.875 to

$$\alpha = 1518251/262144 \approx 5.79.$$

Thus $\delta_L \leq 2^{\alpha} \approx 55.40$.

3b. Results of Dembélé, Greenberg, and Voight

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions.

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions. For $S = \{3\}$, they have $G = PGL_2(3^k)$ with $k = 18$, 27, and 36.

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions. For $S = \{3\}$, they have $G = PGL_2(3^k)$ with $k = 18$, 27, and 36. For $S = \{5\}$, they have G involving one or more copies of the simple group $G = PSL_2(5^k)$ for $k = 1$, 2, 5, 10, 15, 25, and 40.

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions. For $S = \{3\}$, they have $G = PGL_2(3^k)$ with $k = 18$, 27, and 36. For $S = \{5\}$, they have G involving one or more copies of the simple group $G = PSL_2(5^k)$ for $k = 1$, 2, 5, 10, 15, 25, and 40.

The case $k = 1$ for $S = \{5\}$ gives an L with $G = PSL_2(5)^5.2.5$.

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions. For $S = \{3\}$, they have $G = PGL_2(3^k)$ with $k = 18, 27$, and 36. For $S = \{5\}$, they have G involving one or more copies of the simple group $G = PSL_2(5^k)$ for $k = 1, 2, 5, 10, 15, 25$, and 40.

The case $k = 1$ for $S = \{5\}$ gives an L with $G = PSL_2(5)^5.2.5$. Let

$$F = \mathbf{Q}[\pi]/(\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5)$$

be the totally real quintic subfield of $\mathbf{Q}(e^{2\pi i/25})$.

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions. For $S = \{3\}$, they have $G = PGL_2(3^k)$ with $k = 18$, 27, and 36. For $S = \{5\}$, they have G involving one or more copies of the simple group $G = PSL_2(5^k)$ for $k = 1$, 2, 5, 10, 15, 25, and 40.

The case $k = 1$ for $S = \{5\}$ gives an L with $G = PSL_2(5)^5.2.5$. Let

$$F = \mathbf{Q}[\pi]/(\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5)$$

be the totally real quintic subfield of $\mathbf{Q}(e^{2\pi i/25})$. Via $PSL_2(5) \cong A_5$, the field L is the splitting field of a quintic polynomial over F.

3b. Results of Dembélé, Greenberg, and Voight

In 2009, Dembélé, Greenberg, and Voight also used Hilbert modular forms to prove the existence of many fields satisfying Gross's conditions. For $S = \{3\}$, they have $G = PGL_2(3^k)$ with $k = 18$, 27, and 36. For $S = \{5\}$, they have G involving one or more copies of the simple group $G = PSL_2(5^k)$ for $k = 1$, 2, 5, 10, 15, 25, and 40.

The case $k = 1$ for $S = \{5\}$ gives an L with $G = PSL_2(5)^5.2.5$. Let

$$F = \mathbf{Q}[\pi]/(\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5)$$

be the totally real quintic subfield of $\mathbf{Q}(e^{2\pi i/25})$. Via $PSL_2(5) \cong A_5$, the field L is the splitting field of a quintic polynomial over F. An overfield $\tilde{L}$ with group $\tilde{G} = SL_2(5)^5.2.5$ is the splitting field of a degree twenty-four polynomial over F.

1. Gross's observation from the mid-1990s
2. Some context and related work from ≤ 2007
3. Results of Dembélé, Serre, and (Dembélé, Greenberg, and Voight) from ≥ 2008
4. A nonsolvable polynomial $g_{25}(x)$ with field discriminant 5^{69}
5. How special is $g_{25}(x)$?
6. How was $g_{25}(x)$ found?
7. How is 5 ramified in $g_{25}(x)$?

4a. A nonsolvable polynomial with field disc. 5^{69}

4a. A nonsolvable polynomial with field disc. 5^{69}

Theorem

Let $g_{25}(x) =$

$$
\begin{aligned}
& x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} \\
& + 21750x^{16} - 57200x^{15} + 112500x^{14} - 240625x^{13} \\
& + 448125x^{12} - 1126250x^{11} + 1744825x^{10} - 1006875x^{9} \\
& - 705000x^{8} + 4269125x^{7} - 3551000x^{6} + 949625x^{5} \\
& - 792500x^{4} + 1303750x^{3} - 899750x^{2} + 291625x - 36535.
\end{aligned}
$$

4a. A nonsolvable polynomial with field disc. 5^{69}

Theorem

Let $g_{25}(x) =$

$$\begin{aligned} &x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} \\ &+21750x^{16} - 57200x^{15} + 112500x^{14} - 240625x^{13} \\ &+448125x^{12} - 1126250x^{11} + 1744825x^{10} - 1006875x^{9} \\ &-705000x^{8} + 4269125x^{7} - 3551000x^{6} + 949625x^{5} \\ &-792500x^{4} + 1303750x^{3} - 899750x^{2} + 291625x - 36535. \end{aligned}$$

Let L be the splitting field of $g_{25}(x)$.

4a. A nonsolvable polynomial with field disc. 5^{69}

Theorem

Let $g_{25}(x) =$

$$\begin{aligned}
&x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} \\
&+21750x^{16} - 57200x^{15} + 112500x^{14} - 240625x^{13} \\
&+448125x^{12} - 1126250x^{11} + 1744825x^{10} - 1006875x^{9} \\
&-705000x^{8} + 4269125x^{7} - 3551000x^{6} + 949625x^{5} \\
&-792500x^{4} + 1303750x^{3} - 899750x^{2} + 291625x - 36535.
\end{aligned}$$

Let L *be the splitting field of* $g_{25}(x)$. *Then*

- $G = Gal(L/\mathbf{Q}) \cong A_5^5.2.5.$

4a. A nonsolvable polynomial with field disc. 5^{69}

Theorem

Let $g_{25}(x) =$

$$\begin{aligned}
&x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} \\
&+21750x^{16} - 57200x^{15} + 112500x^{14} - 240625x^{13} \\
&+448125x^{12} - 1126250x^{11} + 1744825x^{10} - 1006875x^{9} \\
&-705000x^{8} + 4269125x^{7} - 3551000x^{6} + 949625x^{5} \\
&-792500x^{4} + 1303750x^{3} - 899750x^{2} + 291625x - 36535.
\end{aligned}$$

Let L be the splitting field of $g_{25}(x)$. Then

- $G = Gal(L/\mathbf{Q}) \cong A_5^5.2.5.$
- *The discriminant of* $K = \mathbf{Q}[x]/g_{25}(x)$ *is* 5^{69} *and thus* $S = \{5\}$.

4a. A nonsolvable polynomial with field disc. 5^{69}

Theorem

Let $g_{25}(x) =$

$$\begin{aligned} &x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18} - 3625x^{17} \\ &+21750x^{16} - 57200x^{15} + 112500x^{14} - 240625x^{13} \\ &+448125x^{12} - 1126250x^{11} + 1744825x^{10} - 1006875x^{9} \\ &-705000x^{8} + 4269125x^{7} - 3551000x^{6} + 949625x^{5} \\ &-792500x^{4} + 1303750x^{3} - 899750x^{2} + 291625x - 36535. \end{aligned}$$

Let L be the splitting field of $g_{25}(x)$. Then

- $G = Gal(L/\mathbf{Q}) \cong A_5^5.2.5.$
- *The discriminant of* $K = \mathbf{Q}[x]/g_{25}(x)$ *is* 5^{69} *and thus* $S = \{5\}$.
- *L coincides with the DGV field.*

4b. The factorization of $g_{25}(x)$ over F

4b. The factorization of $g_{25}(x)$ over F

Let

4b. The factorization of $g_{25}(x)$ over F

Let

$$\alpha = -\frac{5}{7}\left(3\pi^4 + 10\pi^3 - 19\pi^2 - 62\pi + 5\right)$$

4b. The factorization of $g_{25}(x)$ over F

Let

$$\begin{aligned}\alpha &= -\frac{5}{7}\left(3\pi^4 + 10\pi^3 - 19\pi^2 - 62\pi + 5\right)\\ \beta &= \frac{1}{7}(-79\pi^5 - 331\pi^4 + 288\pi^3 + 1803\pi^2 + 566\pi).\end{aligned}$$

4b. The factorization of $g_{25}(x)$ over F

Let

$$\begin{aligned} \alpha &= -\frac{5}{7}\left(3\pi^4 + 10\pi^3 - 19\pi^2 - 62\pi + 5\right) \\ \beta &= \frac{1}{7}(-79\pi^5 - 331\pi^4 + 288\pi^3 + 1803\pi^2 + 566\pi). \end{aligned}$$

Let

$$\sigma(\pi) = 7^{-1}(-4\pi^4 - 18\pi^3 + 9\pi^2 + 92\pi + 40)$$

be a generator of $\mathrm{Gal}(F/\mathbf{Q})$.

4b. The factorization of $g_{25}(x)$ over F

Let

$$\begin{aligned}\alpha &= -\frac{5}{7}\left(3\pi^4 + 10\pi^3 - 19\pi^2 - 62\pi + 5\right)\\ \beta &= \frac{1}{7}(-79\pi^5 - 331\pi^4 + 288\pi^3 + 1803\pi^2 + 566\pi).\end{aligned}$$

Let

$$\sigma(\pi) = 7^{-1}(-4\pi^4 - 18\pi^3 + 9\pi^2 + 92\pi + 40)$$

be a generator of $\mathrm{Gal}(F/\mathbf{Q})$. Then

$$g_{25}(x) = \prod_{i=0}^{4} f_5^{\sigma^i}(x)$$

4b. The factorization of $g_{25}(x)$ over F

Let

$$\begin{aligned}\alpha &= -\frac{5}{7}\left(3\pi^4 + 10\pi^3 - 19\pi^2 - 62\pi + 5\right) \\ \beta &= \frac{1}{7}(-79\pi^5 - 331\pi^4 + 288\pi^3 + 1803\pi^2 + 566\pi).\end{aligned}$$

Let

$$\sigma(\pi) = 7^{-1}(-4\pi^4 - 18\pi^3 + 9\pi^2 + 92\pi + 40)$$

be a generator of $\mathrm{Gal}(F/\mathbf{Q})$. Then

$$g_{25}(x) = \prod_{i=0}^{4} f_5^{\sigma^i}(x)$$

where

$$f_5(x) = x^5 + \alpha x^2 - \alpha x + \beta.$$

5. How special is $g_{25}(x)$?

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S?

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S? Applying a local-global heuristic (Bhargava) and local computations (R.):

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S? Applying a local-global heuristic (Bhargava) and local computations (R.):

	Ground Field $\mathbf{Q}$			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	2.9	56	120	$2,200$

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S? Applying a local-global heuristic (Bhargava) and local computations (R.):

	Ground Field $\mathbf{Q}$			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	2.9	56	120	$2,200$
Actual:	0	28	43	$1,415$

Number field searches (Jones-R.) give the actual numbers.

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S? Applying a local-global heuristic (Bhargava) and local computations (R.):

	Ground Field $\mathbf{Q}$			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	2.9	56	120	$2,200$
Actual:	0	28	43	$1,415$

Number field searches (Jones-R.) give the actual numbers.

Analogous question and answer over our quintic ground field F:

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S? Applying a local-global heuristic (Bhargava) and local computations (R.):

	Ground Field $\mathbf{Q}$			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	2.9	56	120	$2,200$
Actual:	0	28	43	$1,415$

Number field searches (Jones-R.) give the actual numbers.

Analogous question and answer over our quintic ground field F:

	Ground field F			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	3.7	$5,400$	$490,000$	$720,000,000$

5. How special is $g_{25}(x)$?

How many fields should one expect with say $G = A_5$ or S_5 and given S? Applying a local-global heuristic (Bhargava) and local computations (R.):

	Ground Field $\mathbf{Q}$			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	2.9	56	120	$2,200$
Actual:	0	28	43	$1,415$

Number field searches (Jones-R.) give the actual numbers.

Analogous question and answer over our quintic ground field F:

	Ground field F			
S	$\{5\}$	$\{3,5\}$	$\{2,5\}$	$\{2,3,5\}$
Predicted:	3.7	$5,400$	$490,000$	$720,000,000$
Actual:	≥ 1	$\gg 33$	$\gg 154$	$\gg 905$

6a. How was $g_{25}(x)$ found?

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j,x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group.

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j, x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \quad = \quad 2^{24}3^{12}5^5 j^2 (j-1)^2.$$

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j,x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \;\; = \;\; 2^{24}3^{12}5^5 j^2 (j-1)^2.$$

Since L lifts to an $SL_2(5)^5.2.5$ field $\tilde{L}$

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j,x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \;\; = \;\; 2^{24}3^{12}5^5 j^2 (j-1)^2.$$

Since L lifts to an $SL_2(5)^5.2.5$ field $\tilde{L}$ and the corresponding Galois representation has cyclotomic determinant,

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j, x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \quad = \quad 2^{24}3^{12}5^5j^2(j-1)^2.$$

Since L lifts to an $SL_2(5)^5.2.5$ field $\tilde{L}$ and the corresponding Galois representation has cyclotomic determinant, L is guaranteed to arise for some $j \in F$ (Shepherd-Barron and Taylor).

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j,x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \quad = \quad 2^{24}3^{12}5^5 j^2(j-1)^2.$$

Since L lifts to an $SL_2(5)^5.2.5$ field $\tilde{L}$ and the corresponding Galois representation has cyclotomic determinant, L is guaranteed to arise for some $j \in F$ (Shepherd-Barron and Taylor).

Trying to get $S = \{5\}$.

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j,x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \;=\; 2^{24}3^{12}5^5 j^2(j-1)^2.$$

Since L lifts to an $SL_2(5)^5.2.5$ field $\tilde{L}$ and the corresponding Galois representation has cyclotomic determinant, L is guaranteed to arise for some $j \in F$ (Shepherd-Barron and Taylor).

Trying to get $S = \{5\}$. The easiest way to kill 2 and 3 is to take $j \in F$ with $\mathrm{ord}_2(j) = \pm 6$ and $\mathrm{ord}_3(j-1) = \pm 3$.

6a. How was $g_{25}(x)$ found?

For $j \in F$ the polynomial

$$f(j, x) = x^5 + 5x^4 + 40x^3 - 1728j$$

coming from 5-torsion points on an elliptic curve with j-invariant j generically has the right Galois group. The discriminant is just

$$D(j) \;=\; 2^{24}3^{12}5^5 j^2 (j-1)^2.$$

Since L lifts to an $SL_2(5)^5.2.5$ field $\tilde{L}$ and the corresponding Galois representation has cyclotomic determinant, L is guaranteed to arise for some $j \in F$ (Shepherd-Barron and Taylor).

Trying to get $S = \{5\}$. The easiest way to kill 2 and 3 is to take $j \in F$ with $\mathrm{ord}_2(j) = \pm 6$ and $\mathrm{ord}_3(j-1) = \pm 3$. These are very demanding conditions which force j to have large height and make it highly likely that $f(j, x)$ ramifies above some prime > 5.

6b. How was $g_{25}(x)$ found?

6b. How was $g_{25}(x)$ found?

A search over many j with low height found 647 non-conjugate non-rational j-invariants yielding 647 fields with $G = PSL_2(5)^5.2.5$ and S within $\{2, 3, 5\}$.

6b. How was $g_{25}(x)$ found?

A search over many j with low height found 647 non-conjugate non-rational j-invariants yielding 647 fields with $G = PSL_2(5)^5.2.5$ and S within $\{2, 3, 5\}$.

	$\mathrm{ord}_2(j)$											
	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
1					5	5	4					
0	1	2	4	67	63	$\boxed{248}$	74	66	12	4		**1**
-1			1		16	35	12				1	
-2						5	9	8	3			
-3						1						

6b. How was $g_{25}(x)$ found?

A search over many j with low height found 647 non-conjugate non-rational j-invariants yielding 647 fields with $G = PSL_2(5)^5.2.5$ and S within $\{2,3,5\}$.

	$\mathrm{ord}_2(j)$											
	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
1					5	5	4					
0	1	2	4	67	63	$\boxed{248}$	74	66	12	4		**1**
-1			1		16	35	12				1	
-2						5	9	8	3			
-3						1						

In particular, $j_1 =$

$$\frac{-2^6}{5 \cdot 7^6}(68155\pi^4 + 288368\pi^3 - 125935\pi^2 - 1495535\pi - 1089160)$$

yields a field with $S = \{3,5\}$.

6b. How was $g_{25}(x)$ found?

A search over many j with low height found 647 non-conjugate non-rational j-invariants yielding 647 fields with $G = PSL_2(5)^5.2.5$ and S within $\{2, 3, 5\}$.

	$\mathrm{ord}_2(j)$											
	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
1					5	5	4					
0	1	2	4	67	63	$\boxed{248}$	74	66	12	4		**1**
-1			1		16	35	12				1	
-2						5	9	8	3			
-3						1						

In particular, $j_1 =$

$$\frac{-2^6}{5 \cdot 7^6}(68155\pi^4 + 288368\pi^3 - 125935\pi^2 - 1495535\pi - 1089160)$$

yields a field with $S = \{3, 5\}$. (Also have a field with $S = \{2, 5\}$).

6c. How was $g_{25}(x)$ found?

6c. How was $g_{25}(x)$ found?

Now use base-change operators

$$BC_3(j) = \frac{(4j-1)^3}{27j}, \qquad BC_4(j) = \frac{(9j-1)^3(1-j)}{64j}$$

6c. How was $g_{25}(x)$ found?

Now use base-change operators

$$BC_3(j) = \frac{(4j-1)^3}{27j}, \qquad BC_4(j) = \frac{(9j-1)^3(1-j)}{64j}$$

to get 508 new j's (mostly of much larger height).

6c. How was $g_{25}(x)$ found?

Now use base-change operators

$$BC_3(j) = \frac{(4j-1)^3}{27j}, \qquad BC_4(j) = \frac{(9j-1)^3(1-j)}{64j}$$

to get 508 new j's (mostly of much larger height).

	−12	−11	−10	−9	−8	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5
1						3	4				1							
0	4			8	3	7	50				7	4	$\boxed{2}$	3	4			
−1				3			4				1							
−2																		
−3							1	3	5	55	31	146	30	45			2	
−4										1	2	9	19	5				
−5												5	22	10	6			
−6																		
−7										1	6	2	3					

6d. How was $g_{25}(x)$ found?

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$.

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$. Explicitly, $j_2 =$

$$\frac{-1}{2^6 3^3 5^1 7^{11}} \left(1686352437277476\pi^4 + 8854036993798358 8\pi^3 - 1124791466055321 5\pi^2 - 4643993605154835 72\pi - 3535058667383836 80\right).$$

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$. Explicitly, $j_2 =$

$$\frac{-1}{2^6 3^3 5^1 7^{11}} \left(16863524372777476\pi^4 + \right.$$
$$8854036993798358 8\pi^3 - 11247914660553215\pi^2$$
$$\left. -464399360515483572\pi - 3535058667383836 80\right).$$

The actual order of events:

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$. Explicitly, $j_2 =$

$$\frac{-1}{2^6 3^3 5^1 7^{11}} \left(1686352437277476\pi^4 + 8854036993798358 8\pi^3 - 1124791466055321 5\pi^2 - 4643993605154835 72\pi - 3535058667383836 80\right).$$

The actual order of events:

$f(j_2, x)$ is the sought relative quintic,

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$. Explicitly, $j_2 =$

$$\frac{-1}{2^6 3^3 5^1 7^{11}} \left(1686352437277476\pi^4 + 8854036993798358\pi^3 - 1124791466055321\pi^2 - 4643993605154835 72\pi - 3535058667383836 80\right).$$

The actual order of events:

$f(j_2, x)$ is the sought relative quintic,

$G(x) = \prod_{i=0}^{4} f(j_2^{\sigma^i}, x) \in \mathbf{Q}[x]$ defines the right field,

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$. Explicitly, $j_2 =$

$$\frac{-1}{2^6 3^3 5^1 7^{11}} \left(1686352437277476\pi^4 + \right.$$
$$8854036993798358 8\pi^3 - 11247914660553215\pi^2$$
$$\left. -4643993605154835 72\pi - 35350586673838368 0\right).$$

The actual order of events:

$f(j_2, x)$ is the sought relative quintic,

$G(x) = \prod_{i=0}^{4} f(j_2^{\sigma^i}, x) \in \mathbf{Q}[x]$ defines the right field,

$g_{25}(x)$ is `polredabs`$(G(x)) \in \mathbf{Z}[x]$,

6d. How was $g_{25}(x)$ found?

The desired specialization point is $j_2 = BC_3(j_1)$. Explicitly, $j_2 =$

$$\frac{-1}{2^6 3^3 5^1 7^{11}} \big(1686352437277476\pi^4 + 8854036993798358 8\pi^3 - 11247914660553215\pi^2 - 46439936051548357 2\pi - 35350586673838368 0\big).$$

The actual order of events:

$f(j_2, x)$ is the sought relative quintic,

$G(x) = \prod_{i=0}^{4} f(j_2^{\sigma^i}, x) \in \mathbf{Q}[x]$ defines the right field,

$g_{25}(x)$ is `polredabs`$(G(x)) \in \mathbf{Z}[x]$, and

$x^5 + \alpha x^2 - \alpha x + \beta \in F[x]$ is a quintic factor of $g_{25}(x)$.

7a. How is 5 ramified in $g_{25}(x)$?

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$.

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$. A general theory applies, giving one resolvent 5-adic fields

$$K_5^{(i)} = F_5[x]/(x^5 - \gamma^{(i)})$$

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$. A general theory applies, giving one resolvent 5-adic fields

$$K_5^{(i)} = F_5[x]/(x^5 - \gamma^{(i)})$$

with $\gamma^{(5)} = \gamma$ and

$$\gamma^{(i)} = \frac{\sigma\left(\gamma^{(i+1)}\right)}{\gamma^{(i+1)}}$$

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$. A general theory applies, giving one resolvent 5-adic fields

$$K_5^{(i)} = F_5[x]/(x^5 - \gamma^{(i)})$$

with $\gamma^{(5)} = \gamma$ and

$$\gamma^{(i)} = \frac{\sigma\left(\gamma^{(i+1)}\right)}{\gamma^{(i+1)}}$$

For $i = 5, 4, 3, 2, 1$, the discriminant $\mathrm{disc}(K_5^{(i)}/\mathbf{Q}_5)$ is 5^c with $c = 69, 65, 61, 57, 53$.

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$. A general theory applies, giving one resolvent 5-adic fields

$$K_5^{(i)} = F_5[x]/(x^5 - \gamma^{(i)})$$

with $\gamma^{(5)} = \gamma$ and

$$\gamma^{(i)} = \frac{\sigma(\gamma^{(i+1)})}{\gamma^{(i+1)}}$$

For $i = 5, 4, 3, 2, 1$, the discriminant $\mathrm{disc}(K_5^{(i)}/\mathbf{Q}_5)$ is 5^c with $c = 69, 65, 61, 57, 53$. From

$$\frac{c}{p^2} = \frac{p-1}{p} s_b + \frac{p-1}{p^2} s_a.$$

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$. A general theory applies, giving one resolvent 5-adic fields

$$K_5^{(i)} = F_5[x]/(x^5 - \gamma^{(i)})$$

with $\gamma^{(5)} = \gamma$ and

$$\gamma^{(i)} = \frac{\sigma(\gamma^{(i+1)})}{\gamma^{(i+1)}}$$

For $i = 5, 4, 3, 2, 1$, the discriminant $\mathrm{disc}(K_5^{(i)}/\mathbf{Q}_5)$ is 5^c with $c = 69, 65, 61, 57, 53$. From

$$\frac{c}{p^2} = \frac{p-1}{p} s_b + \frac{p-1}{p^2} s_a.$$

and $s_a = 2$ (from $\mathrm{disc}(F_5/\mathbf{Q}_5) = 5^8$)

7a. How is 5 ramified in $g_{25}(x)$?

The field $K = F[x]/(x^5 + \alpha x^2 - \alpha x + \beta)$ has a 5-adic binomial-over-abelian presentation $K_5 = F_5[x]/(x^5 - \gamma)$. A general theory applies, giving one resolvent 5-adic fields

$$K_5^{(i)} = F_5[x]/(x^5 - \gamma^{(i)})$$

with $\gamma^{(5)} = \gamma$ and

$$\gamma^{(i)} = \frac{\sigma(\gamma^{(i+1)})}{\gamma^{(i+1)}}$$

For $i = 5, 4, 3, 2, 1$, the discriminant $\mathrm{disc}(K_5^{(i)}/\mathbf{Q}_5)$ is 5^c with $c = 69, 65, 61, 57, 53$. From

$$\frac{c}{p^2} = \frac{p-1}{p} s_b + \frac{p-1}{p^2} s_a.$$

and $s_a = 2$ (from $\mathrm{disc}(F_5/\mathbf{Q}_5) = 5^8$) one gets slopes $s_b = 3.05$, 2.85, 2.65, 2.45, 2.25.

7b. How is 5 ramified in $g_{25}(x)$?

7b. How is 5 ramified in $g_{25}(x)$?

As a consequence:

7b. How is 5 ramified in $g_{25}(x)$?

As a consequence:

Theorem

The 5*-adic decomposition group* D *inside* $Gal(L/\mathbf{Q})$ *has size* $4 \cdot 5^6 = 62500$.

7b. How is 5 ramified in $g_{25}(x)$?

As a consequence:

Theorem

The 5*-adic decomposition group* D *inside* $Gal(L/\mathbf{Q})$ *has size* $4 \cdot 5^6 = 62500$*. Its unramified, tame, and wild subquotients have size* 1, 4, *and* 5^6*.*

7b. How is 5 ramified in $g_{25}(x)$?

As a consequence:

Theorem

The 5*-adic decomposition group* D *inside* $Gal(L/\mathbf{Q})$ *has size* $4 \cdot 5^6 = 62500$. *Its unramified, tame, and wild subquotients have size* 1, 4, *and* 5^6. *The six wild slopes* s_5, s_4, s_3, s_2, s_1, s_0 *are* 3.05, 2.85, 2.65, 2.45, 2.25, 2.00.

7b. How is 5 ramified in $g_{25}(x)$?

As a consequence:

Theorem

The 5*-adic decomposition group D inside Gal*$(L/\mathbf{Q})$ *has size* $4 \cdot 5^6 = 62500$. *Its unramified, tame, and wild subquotients have size* 1, 4, *and* 5^6. *The six wild slopes* s_5, s_4, s_3, s_2, s_1, s_0 *are* 3.05, 2.85, 2.65, 2.45, 2.25, 2.00. *The mean slope is*

$$\begin{aligned}\alpha &= \frac{4}{5}s_5 + \frac{4}{5^2}s_4 + \frac{4}{5^3}s_3 + \frac{4}{5^4}s_2 + \frac{4}{5^5}s_1 + \frac{4}{5^6}s_0 + \frac{3}{4 \cdot 5^6} \\ &= 3 - \frac{1}{12500}\end{aligned}$$

7b. How is 5 ramified in $g_{25}(x)$?

As a consequence:

Theorem

The 5*-adic decomposition group* D *inside* $Gal(L/\mathbf{Q})$ *has size* $4 \cdot 5^6 = 62500$. *Its unramified, tame, and wild subquotients have size* 1, 4, *and* 5^6. *The six wild slopes* s_5, s_4, s_3, s_2, s_1, s_0 *are* 3.05, 2.85, 2.65, 2.45, 2.25, 2.00. *The mean slope is*

$$\begin{aligned} \alpha &= \frac{4}{5}s_5 + \frac{4}{5^2}s_4 + \frac{4}{5^3}s_3 + \frac{4}{5^4}s_2 + \frac{4}{5^5}s_1 + \frac{4}{5^6}s_0 + \frac{3}{4 \cdot 5^6} \\ &= 3 - \frac{1}{12500} \end{aligned}$$

and the root discriminant of L *is* $5^\alpha \approx 124.984$.

Main References

Main References

L. Dembélé, M. Greenberg, and J. Voight. Nonsolvable number fields ramified only at 3 and 5. Preprint, June 2009.

Main References

L. Dembélé, M. Greenberg, and J. Voight. Nonsolvable number fields ramified only at 3 and 5. Preprint, June 2009.

D. P. Roberts. Nonsolvable polynomials with field discriminant 5^A. Preprint, August 2009.

Main References

L. Dembélé, M. Greenberg, and J. Voight. Nonsolvable number fields ramified only at 3 and 5. Preprint, June 2009.

D. P. Roberts. Nonsolvable polynomials with field discriminant 5^A. Preprint, August 2009.

Thanks for coming!