Division polynomials with Galois group $\mathbf{SU_3(\mathbb{F}_3).2 = G_2(\mathbb{F}_2)}$

David P. Roberts
University of Minnesota, Morris

General Inverse Galois Problem. Given a finite group G, find number fields with Galois group G, preferably of small discriminant.

Our case today. $G = SU_3(\mathbb{F}_3).2 = G_2(\mathbb{F}_2)$ of order $12096 = 2^6 \cdot 3^3 \cdot 7$. We'll produce two related two-parameter polynomials:

$$\begin{aligned} F_1(p, q, x) &= x^{28} + \cdots \in \mathbb{Q}(p, q)[x], \\ F_2(a, b, x) &= x^{28} + \cdots \in \mathbb{Q}(a, b)[x]. \end{aligned}$$

Connections with:

1. Rigid four-tuples in G
2. Motives with Galois group U_3, Sp_6, G_2
3. Three-point covers with Galois group G
4. Number fields with Galois group G

Some background. The twelfth smallest non-abelian simple group is

$$G' = SU_3(\mathbb{F}_3) = G_2(\mathbb{F}_2)'.$$

of order $6048 = 2^5 3^3 7$. One has $|\mathrm{Out}(G')| = 2$ and the extended group

$$G = SU_3(\mathbb{F}_3).2 = G_2(\mathbb{F}_2)$$

embeds transitively into A_{28} and A_{36}.

Some information on conjugacy classes:

Classes in G'			
C	$\|C\|$	λ_{28}	λ_{36}
$1A$	1	1^{28}	1^{36}
$2A$	63	$2^{12}1^4$	$2^{12}1^{12}$
$3A$	56	3^91	3^{12}
$3B$	672	3^91	$3^{11}1^3$
$4AB$	$2 \cdot 63$	4^61^4	4^62^6
$4C$	378	4^62^2	$4^62^41^4$
$6A$	504	6^431	6^43^4
$7AB$	$2 \cdot 864$	7^4	7^51
$8AB$	$2 \cdot 756$	$8^32^11^2$	8^34^3
$12AB$	$2 \cdot 504$	12^231	12^26^2

Classes in $G - G'$			
C	$\|C\|$	λ_{28}	λ_{36}
$2b$	252	$2^{12}1^4$	$2^{16}1^4$
$4d$	252	4^61^4	4^62^6
$6b$	2016	6^431	$6^53^12^11$
$8c$	1512	8^34	$8^34^221^2$
$12cd$	$2 \cdot 1008$	12^231	12^26^2

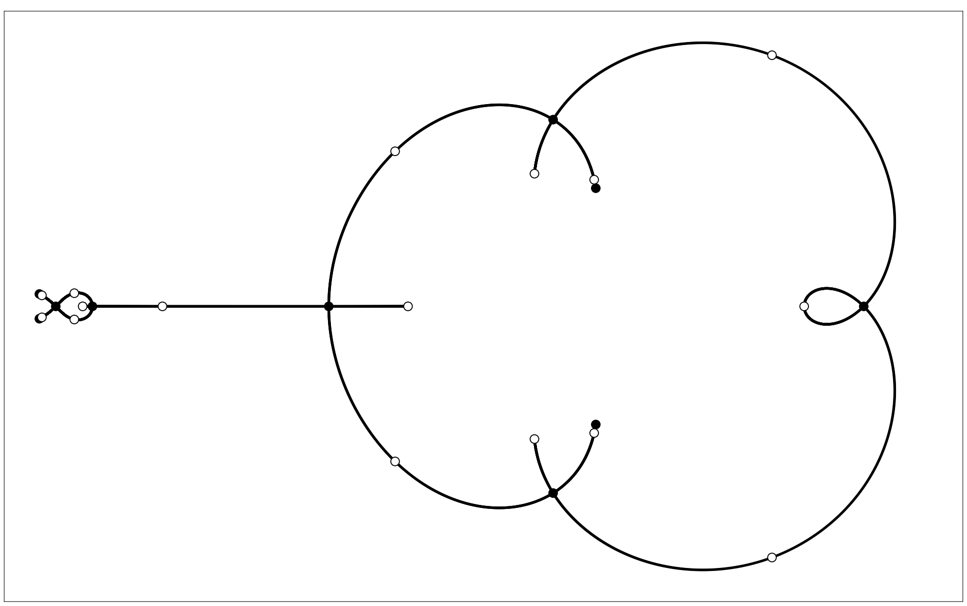
A standard way to construct number fields with prescribed Galois group is to use *rigidity.* For example, up to simultaneous G-conjugation, there is just one triple (g_0, g_1, g_∞) with

$$\begin{array}{rcl} g_0 & \in & 4d \\ g_1 & \in & 2b \\ g_\infty & \in & 12AB \end{array} \qquad \begin{array}{rcl} g_0 g_1 g_\infty & = & 1 \\ \langle g_0, g_1, g_\infty \rangle & = & G \end{array}$$

Malle and Matzat computed the corresponding degree 28 cover $\mathbb{P}^1_x \to \mathbb{P}^1_t$:

$$\begin{aligned} f(t,x) &= A(x)^4 B(x) - t 2^2 3^9 \left(x^2+4x+1\right)^{12}(2x+1) \\ A(x) &= x^6 - 6x^5 - 435x^4 - 308x^3 + 15x^2 + 66x + 19 \\ B(x) &= x^4 + 20x^3 + 114x^2 + 68x + 13 \end{aligned}$$

The preimage of $[0,1] = \bullet\!\!-\!\!\circ$ in $\mathbb{P}^1_x$:



The remarkable nature of the Malle-Matzat cover is reflected in its discriminant:

$$\mathrm{disc}_x(f(t,x)) = 2^{576}3^{630}t^{18}(t-1)^{12}.$$

Plugging in $t = 1/2$ gives a degree twenty-eight field with Galois group G' and discriminant $2^{84}3^{42}$. Carefully chosen other $t \in \mathbb{Q}$ give 41 fields with Galois group G and discriminant 2^j3^k.

There is an extensive literature, both theoretical and computational, on rigid three-point covers.

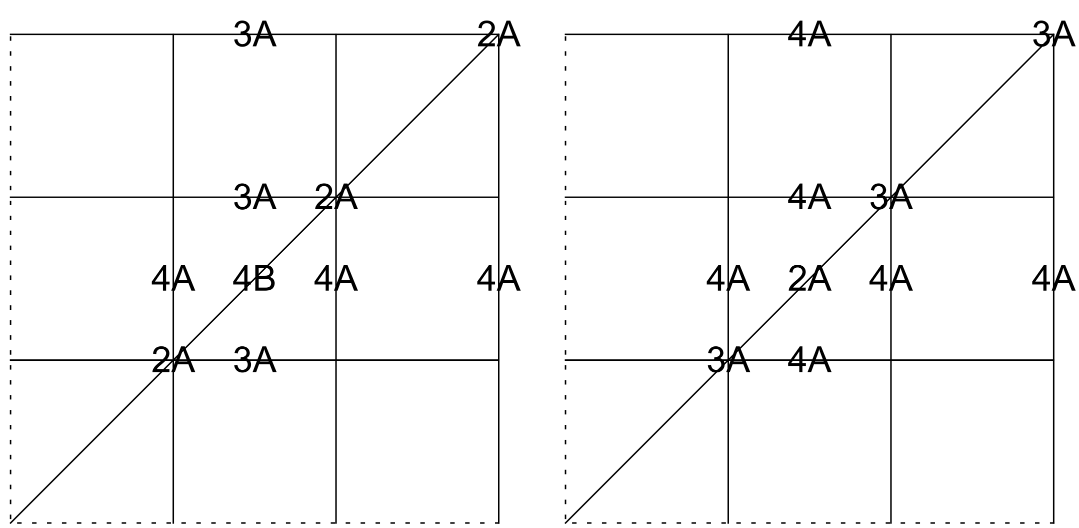
Rigid z-point covers for larger z are known to exist, for example coming from Katz's rigid local systems with coefficients in $\mathbb{F}_\ell$. However the literature is very sparse for them. This talk presents computational examples with $z = 4$.

1. Rigid four-point covers. Mass formulas give five four-tuples of conjugacy classes in G' giving rigid four-point covers of $\mathbb{P}^1(\mathbb{C})$:

$(3A, 3A, 3A, 4B)$,	$(4A, 4A, 4A, 2A)$,
$(4A, 4A, 4A, 4B)$,	
$(2A, 2A, 3A, 4A)$.	$(4A, 4A, 3A, 3A)$,

All other quadruples are far from rigid.

Let $M_{0,5}$ be the moduli space of five labeled points in the projective line. The left three four-tuples give the same cover of $M_{0,5}$ and this cover has S_3 symmetry. The right two give a cover of $M_{0,5}$ having $S_3 \times S_2$ symmetry:



Our covers descend to covers of bases

$$\begin{aligned} U_{3,1,1} &:= M_{0,5}/S_3, \\ U_{3,2} &:= M_{0,5}/(S_3 \times S_2). \end{aligned}$$

They are correlated by a cubic correspondence:

$$\begin{tikzcd}
 & X_0 \arrow[dl, "3"'] \arrow[dr, "3"] \arrow[dd, "\pi_0"'] & \\
X_1 \arrow[ddd, "\pi_1"'] & & X_2 \arrow[ddd, "\pi_2"] \\
 & & \\
 & U \arrow[dl, "3"] \arrow[dr, "3"'] & \\
U_{3,1,1} & & U_{3,2}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(x_0, y_0) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
\mathbb{Q}(x_1, y_1) \arrow[ddd, dash] & & \mathbb{Q}(x_2, y_2) \arrow[ddd, dash] \\
 & & \\
 & \mathbb{Q}(u, v) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(p, q) & & \mathbb{Q}(a, b)
\end{tikzcd}$$

It is remarkable that the three fields upstairs are also rational.

We seek to algebraically describe π_1 and π_2 by polynomial relations

$$\begin{aligned} F_1(p, q, x_1) &= x_1^{28} + \cdots = 0, \\ F_2(a, b, x_2) &= x_2^{28} + \cdots = 0. \end{aligned}$$

2A. Motives with Galois group U_3. Deligne and Mostow studied families of covers

$$y^d = f(u_1, \ldots, u_n, x)$$

of the x-line. Two of their first examples are

$$\begin{aligned} y^4 &= (x-1)^3 x^2 \left(x^2 + ux - vx - x + v\right) \\ &\quad \text{(genus 4)}, \\[1em] y^4 &= \left(x^2 + 2x + 1 - 4u\right)^2 \left(x^2 - 2x + 1 - 4v\right) \\ &\quad \text{(genus 3)}. \end{aligned}$$

They prove that the Jacobian J_2 of the second is a factor of the Jacobian J_1 of the first.

The 3-torsion points of either cover correspond to our $\pi_0 : X_0 \to U$. There are natural descents to families of curves

$$\Pi_1 : C_1 \to U_{3,1,1}, \quad \Pi_2 : C_2 \to U_{3,2}.$$

On 3-torsion, these become our

$$\pi_1 : X_1 \to U_{3,1,1}, \quad \pi_2 : X_2 \to U_{3,2}.$$

We get explicit polynomials for the π_i via this connection; hundreds of terms in each case.

2B. Motives with Galois group Sp_6. Shioda studied the family of degree four plane curves

$$x^3+(y^3+cy+e)x+(ay^4+by^3+dy^2+fy+g)=0$$

in the x-y plane.

He obtained an explicit 1784-term polynomial with Galois group $Sp_6(\mathbb{F}_2)$ corresponding to their 2-torsion:

$$S(a,b,c,d,e,f,g;z)=z^{28}-8az^{27}+72bz^{25}+\cdots$$

This polynomial is universal for $Sp_6(\mathbb{F}_2)$ and so, via $G=G_2(\mathbb{F}_2)\subset Sp_6(\mathbb{F}_2)$, our polynomials must be specializations.

In fact, our π_0 is given via $w=u-v+1$ by

$$S(1,w,-3u,0,-uw,-uw,-u^2;z)=0.$$

Our π_1 and π_2 are given by much more complicated formulas.

2C. Motives with Galois group G_2. Define matrices a, b, c, and d:

$$\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ -3 & 1 & & 1 & & & \\ 3 & -1 & & & 1 & & \\ 9 & -3 & & & & 1 & \\ -1 & & 3 & -1 & 2 & -1 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & & & & 3 & -1 & \\ & 1 & & & 9 & -3 & \\ & & -2 & 1 & & & \\ & & -9 & 4 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & -3 & 1 & & & 1 \end{pmatrix}$$

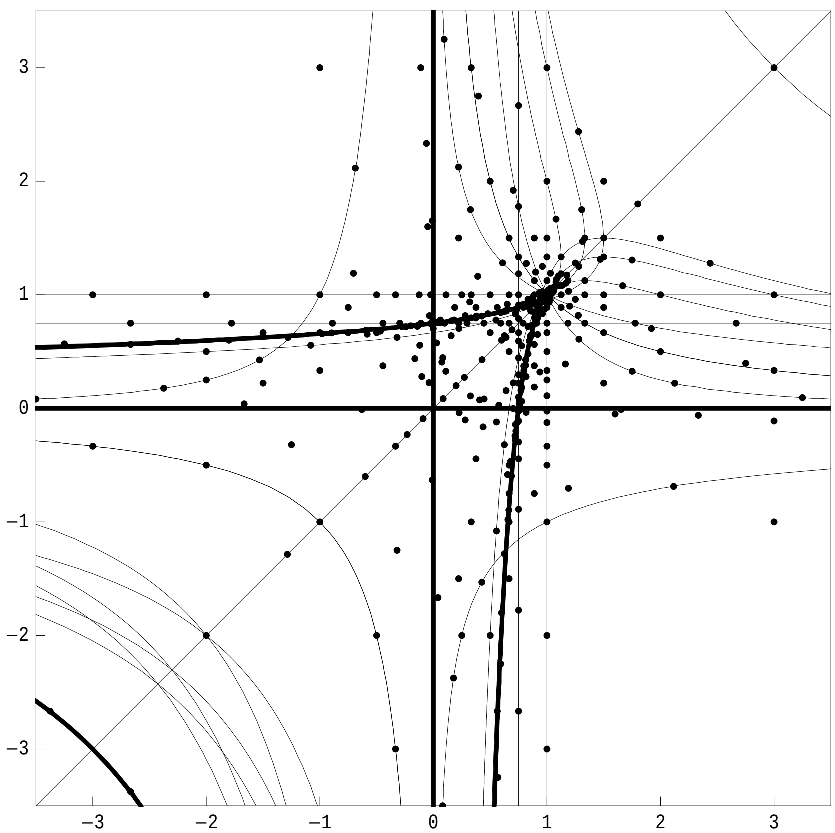
$$\begin{pmatrix} 1 & -1 & & & & & -3 \\ 3 & -2 & & & & & \\ & & 1 & -1 & & & 3 \\ & & 3 & -2 & & & 6 \\ & & & & 1 & -1 & -3 \\ & & & & 3 & -2 & \\ & & & & & & 1 \end{pmatrix} \quad \begin{pmatrix} 10 & -5 & & & 9 & -5 & -6 \\ 15 & -8 & & & 18 & -9 & -9 \\ & & 1 & & & & \\ -3 & 2 & -3 & 1 & -6 & 3 & 3 \\ 9 & -5 & & & 10 & -5 & -6 \\ 18 & -9 & & & 15 & -8 & -9 \\ -2 & 1 & & & -2 & 1 & 1 \end{pmatrix}$$

Then $abcd = 1$ and the Zariski-closure of the group $\langle a, b, c, d \rangle$ is the algebraic group G_2. This monodromy representation underlies a family of G_2 motives appearing in a classification of similar families by Dettweiler and Reiter.

In $GL_7(\mathbb{F}_2)$, the matrices generate $G_2(\mathbb{F}_2)'$ and (a, b, c, d) is in our rigid class $(2A, 2A, 3A, 4A)$. Hence $\pi_1 : X_1 \to U_{3,1,1}$ also functions as a division polynomial for a family of G_2 motives.

In all three cases, our explicit division polynomials aid in studying the source motives.

3. Specialization to three-point covers. A picture of $U_{3,1,1}(\mathbb{R})$ inside the p-q plane and its complementary discriminant locus (thick):



To review, the drawn space is the base of our degree twenty-eight cover $\pi_1 : X_1 \to U_{3,1,1}$.

Preimages of the thin curves are three-point covers, all of positive genus. It would be hard to construct these three-point covers directly.

Table of three-point covers obtained from π_1 and π_2 by specialization. The last fourteen have monodromy group G', Galois group G, and bad reduction set $\{2, 3\}$. The constant field extension is always $\mathbb{Q}(i)/\mathbb{Q}$.

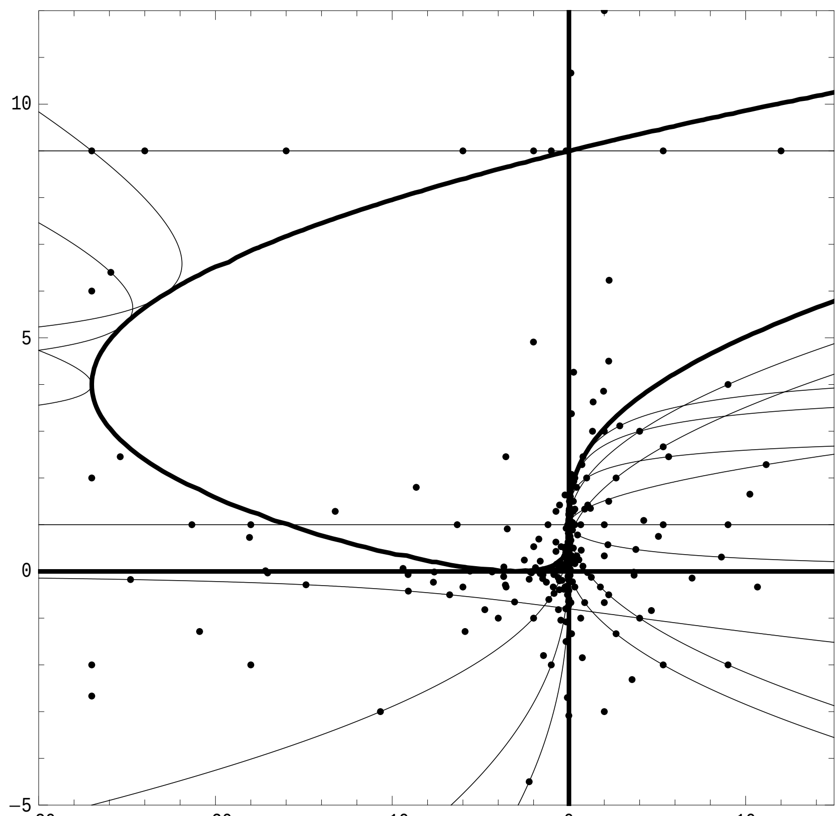
X_0	X_{311}	X_{32}	C_0	C_1	C_∞	g_{28}	g_{36}	$\bar{\mu}$	μ
	H''		$4A$	$4B$	$3B$	–	–	$0.\overline{3}$	0
	I''		$4A$	$12A$	$2A$	–	–	$0.\overline{3}$	0
b	B^*	B	$6A$	$2A$	$8A$	1	0	1	1
		M	$12A$	$2A$	$8B$	2	2	1	1
		G	$4A$	$6A$	$3B$	2	2	1	1
	H', G''		$12A$	$4A$	$3B$	2	5	1	1
e	L'	E, K	$4C$	$4A$	$8A$	3	3	1	1
	G'	H	$3A$	$12A$	$3B$	3	5	1	1
a	K'	A	$4A$	$8A$	$8B$	4	7	1	1
c	K''	C, I	$3A$	$8A$	$6A$	4	6	1	1
d	L''		$6A$	$4A$	$6A$	4	5	1	1
f	F^*, I'	F	$4A$	$8B$	$12B$	5	8	1	1
	J'		$4A$	$12A$	$8B$	5	8	1	1
		L	$12A$	$3A$	$8A$	5	8	1	1
	M^*	J	$6A$	$12A$	$8B$	7	10	5	5
	J''		$12A$	$12A$	$6A$	8	11	$4.08\overline{3}$	3

The degree 36 resolvent of the third cover:

$$\begin{aligned} f_{36}(t,x) &= \left(4x^4-3\right)^3\left(4x^4-12x^2+12x-3\right)^6 \\ &\quad -3^9t(x-1)^4\left(2x^2-1\right)^8\left(2x^2-2x+1\right)^4 \end{aligned}$$

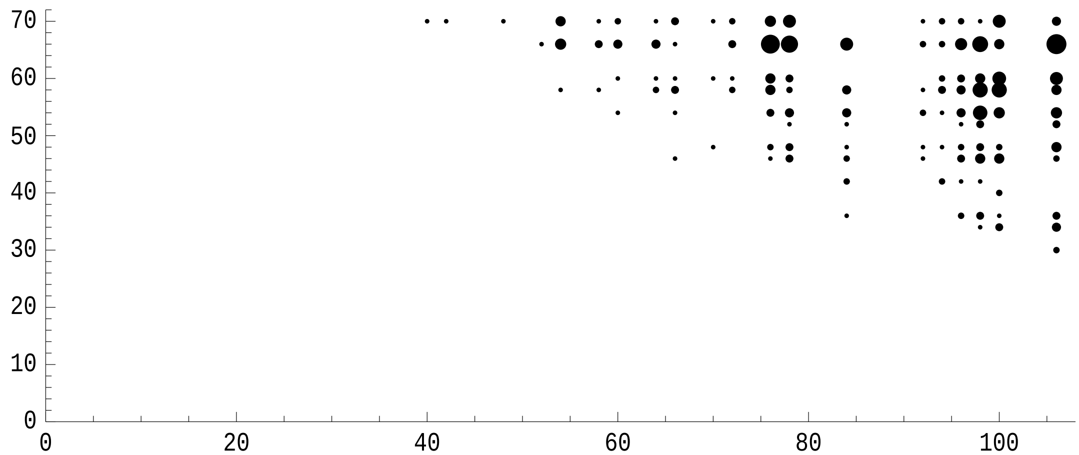
In general, the one-parameter equations for specialization are much simpler than the two-parameter polynomials for the whole family.

4. Specialization to number fields. A similar picture of $U_{3,2}(\mathbb{R})$ inside the a-b plane:



The drawn points $(a, b) \in U_{3,2}(\mathbb{Q}) \subset \mathbb{Q}^2$ are chosen so that $K = \mathbb{Q}[x]/F_2(a, b, x)$ has discriminant of the form $2^j 3^k$. Counting contributions from the first cover too, 376 such fields with Galois group $SU_3(\mathbb{F}_3).2 = G_2(\mathbb{F}_2)$ are obtained. It would be hard to construct these fields by purely number-theoretic methods.

Pairs (j,k) arising from discriminants $d = 2^j 3^k$ from specializations of $F_1(p,q,x)$ and $F_2(a,b,x)$ to G number fields:



376 fields contribute to the picture, with multiplicities in discriminants indicated by area.

Considering the Malle-Matzat cover and other sources as well, there are at least 408 fields with Galois group G and discriminant $2^j 3^k$. The distribution by the quadratic field $\mathbb{Q}(\sqrt{-d})$ associated to G/G' is

∂	-6	-3	-2	-1	2	3	6
#	5	6	6	381	7	2	1

A particular specialization. Eight specialization points

$$\begin{aligned}
(u,v) &= (-4,-3),(-\frac{1}{2},1),(\frac{1}{2},3),(4,-3),(-32,1),(-\frac{32}{81},\frac{49}{81}),\\
(p,q) &= (1,\frac{1}{2}),\\
(a,b) &= (-\frac{27}{4},-\frac{1}{2})
\end{aligned}$$

give rise to the same number field with Galois group $SU_3(\mathbb{F}_3).2 = G_2(\mathbb{F}_2)$ and the very small field discriminant $2^{66}3^{46}$. A defining polynomial is

$$\begin{aligned}
&x^{28}-4x^{27}+18x^{26}-60x^{25}+165x^{24}-420x^{23}\\
&+798x^{22}-1440x^{21}+2040x^{20}-2292x^{19}\\
&+2478x^{18}-756x^{17}-657x^{16}+1464x^{15}\\
&-4920x^{14}+3072x^{13}-1068x^{12}+3768x^{11}\\
&+1752x^{10}-4680x^{9}-1116x^{8}+672x^{7}+1800x^{6}\\
&-240x^{5}-216x^{4}-192x^{3}+24x^{2}+32x+4.
\end{aligned}$$

Close 2- and 3-adic analysis says that the root discriminant of the Galois closure is

$$2^{43/16}3^{125/72} \approx 43.39$$

For comparison, extensive searches have been done on the smaller group S_7 and the larger group S_8, with smallest known Galois root discriminants being 40.49 and 43.99, respectively.

Main reference. David P. Roberts. *Division Polynomials with Galois group $SU_3(\mathbb{F}_3).2 = G_2(\mathbb{F}_2)$.* To appear in Proceedings of CNTA-XIII. See this paper for other references.

References for the three parts of §2:

A. Pierre Deligne and George Daniel Mostow. *Commensurabilities among lattices in PU(1,n).* Annals of Mathematics Studies, 132. Princeton University Press, 1993. viii+183 pp.

B. Tetsuji Shioda. *Plane quartics and Mordell-Weil lattices of type E7.* Comment. Math. Univ. St. Paul. 42 (1993), no. 1, 61–79.

C. Michael Dettweiler and Stefan Reiter. *The classification of orthogonally rigid G2-local systems and related differential operators.* Trans. of the AMS 366 (2014) 5821-5851. (Relevant family is P5.1 in §6.4. Matrices from e-mail from Reiter)