Symbolic Computation and Machine Learning for Galois Group of Septics

Jurgen Mezinaj

Oakland University, Rochester, MI

June 6, 2025

5th Pythagorean Conference, Kalamata, Greece June 1-6, 2025

- We integrate classical Galois theory with machine learning to classify Galois groups of irreducible degree-7 polynomials.
- Building on Resolvent polynomials, we identify Galois groups through factorization patterns.
- Explicitly construct Symbolic formulas for the Resolvent polynomials.
- We build a database of degree-7 polynomials from projective space, filtered by height, and tested for irreducibility to identify patterns.
- We focus on degree 7 as a concrete example, aiming to generalize to degree n.

Galois Theory

Let $f(x)$ be a degree $n = \deg f$ irreducible polynomial in $\mathbb{Q}[x]$

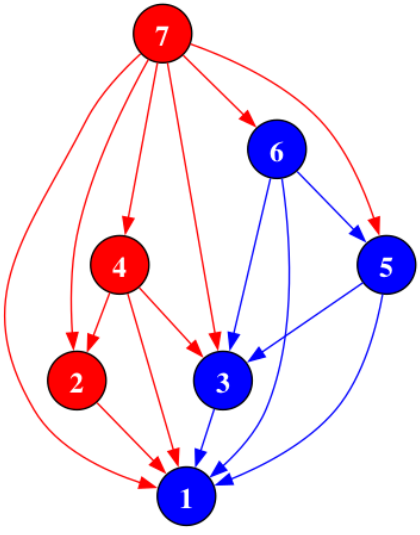
$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

in a splitting field E_f.
Then, $E_f/\mathbb{Q}$ is Galois because it is a normal extension and separable. The group $\mathrm{Gal}(E_f/\mathbb{Q})$ is called the Galois group of $f(x)$ over $\mathbb{Q}$ and denoted by $\mathrm{Gal}_{\mathbb{Q}}(f)$.
The elements of $\mathrm{Gal}_{\mathbb{Q}}(f)$ permute roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$. Thus, the Galois group of the polynomial has an isomorphic copy embedded in S_n, determined up to conjugacy by f.

Using GAP, we can compute all transitive subgroups of S_n for a given n.
For our case degree 7, these are seven transitive subgroups of S_7:

$$C_7, D_7, C_7 \rtimes C_3, C_7 \rtimes C_6, \mathrm{PSL}(3,2), A_7, S_7$$

Lattice of Transitive Subgroups of S_7



Lattice of Transitive Subgroups of S_7 .

Some Inclusions:

$$C_7 \subset D_7 \subset C_7 \rtimes C_3$$

$$C_7 \subset C_7 \rtimes C_3 \subset \mathrm{PSL}(3,2)$$

$$\subset A_7, \quad C_7 \rtimes C_3 \subset C_7 \rtimes C_6$$

Node Labels:

- 1: C_7
- 2: D_7
- 3: $C_7 \rtimes C_3$
- 4: $C_7 \rtimes C_6$
- 5: $\mathrm{PSL}(3,2)$
- 6: A_7
- 7: S_7

Resolvent Polynomials

Consider the polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x] \tag{1}$$

where its roots $\alpha_1, \ldots, \alpha_n$ are considered variables. Then S_n acts on $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ by permuting the variables.

$$\begin{aligned} S_n \times \mathbb{Q}[\alpha_1, \ldots, \alpha_n] &\to \mathbb{Q}[\alpha_1, \ldots, \alpha_n] \\ (\sigma, F(\alpha_1, \ldots, \alpha_n)) &\to F(\sigma(\alpha_1), \ldots, \sigma(\alpha_n) =: F^\sigma \end{aligned} \tag{2}$$

For any $G \subseteq S_n$ a polynomial $F(\alpha_1, \ldots, \alpha_n)$ is called *symmetric under G* if $F = F^\sigma$ for all $\sigma \in G$. Let H denote the stabilizer of F in G

$$H = \{\sigma \in G \mid F = F^\sigma\}.$$

Resolvent Polynomials

The **resolvent polynomial of** $f(x)$ **with respect to** F , denoted by $R_G(f, F)$, is defined as

$$R_G(f, F) = \prod_{\sigma \in G/H} (x - F^\sigma(\alpha_1, \ldots, \alpha_n)) .$$

The product is over coset representatives of G/H, and the degree of the resolvent is $k = |G|/|H|$.
The resolvent's factorization over $\mathbb{Q}$ reveals information about the Galois group $\mathrm{Gal}(f)$, as its irreducible factors correspond to the orbits of $\mathrm{Gal}(f)$ acting on G/H.

Resolvent Polynomials: Symbolic Computation

Let H be the stabilizer of F. Denote by $k = |G|/|H|$ the index of H in G. The roots $\theta_\sigma = F(\alpha_{\sigma(1)}, \ldots, x_{\sigma(n)})$ are functions of the roots α_i. Use Vieta's formulas for the elementary symmetric sums of $f(x)$:

$$\begin{aligned} s_1 &= \alpha_1 + \cdots + \alpha_n = -a_{n-1}, \\ s_2 &= \sum_{i<j} \alpha_i \alpha_j = a_{n-2}, \\ &\vdots \\ s_n &= \alpha_1 \cdots \alpha_n = (-1)^n a_0. \end{aligned}$$

Define the power sums

$$p_m = \sum_{\sigma \in G/H} \theta_\sigma^m = \sum_{\sigma} [F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})]^m.$$

Expand $F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})^m$, sum over coset representatives, and express the result in terms of $s_1, \ldots, s_n$ using symmetric polynomial identities.

Resolvent Polynomials: Symbolic Computation

Apply Newton's Identities: Relate p_m to e_j via Newton's identities:

$$
\begin{aligned}
e_1 &= p_1, \\
e_2 &= \frac{1}{2}(e_1 p_1 - p_2), \\
e_3 &= \frac{1}{3}\left(e_2 p_1 - e_1 p_2 + p_3\right), \\
&\vdots \\
e_j &= \frac{1}{j}\left(\sum_{i=1}^{j-1}(-1)^{i-1} e_{j-i} p_i + (-1)^{j-1} p_j\right).
\end{aligned}
$$

Solve recursively to obtain $e_1, \ldots, e_k$.
Construct the Resolvent: Form the polynomial using the computed e_j.
With $e_1, e_2, \ldots, e_k$ computed, the resolvent is

$$R_G(f, F) = x^k - e_1 x^{k-1} + e_2 x^{k-2} - \cdots + (-1)^k e_k.$$

This polynomial has degree k, and its coefficients are fully symbolic in the coefficients of $f(x)$.

The Quadratic Resolvent

The **quadratic resolvent**, which checks if the Galois group of our polynomial lies in the alternating group A_7

Definition

Let

- $G = S_7$
- $H = A_7$
- $F_1 = \sqrt{\Delta}$, where $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$ is the discriminant.

The quadratic resolvent is:

$$R_1(x) = R_{S_7}(f, F_1) = \prod_{\sigma \in S_7/A_7} (x - F_1^\sigma).$$

Since $|S_7|/|A_7| = \frac{5040}{2520} = 2$, this is a quadratic polynomial. The discriminant Δ is symmetric, but $\sqrt{\Delta}$ changes under permutations:

- If $\sigma \in A_7$ (even), $F_1^\sigma = \sqrt{\Delta}$.
- If $\sigma \notin A_7$ (odd), $F_1^\sigma = -\sqrt{\Delta}$.

Thus:

$$R_1(x) = (x - \sqrt{\Delta})(x - (-\sqrt{\Delta})) = x^2 - \Delta.$$

The 30-ic Resolvent

The **30-ic resolvent**, which tests if the Galois group is contained in $\mathrm{PSL}(3,2)$, a group of order 168.

Definition

Let

- $G = S_7$
- $H = \mathrm{PSL}(3,2)$
- $F_2 = \alpha_3\alpha_1\alpha_4 + \alpha_4\alpha_2\alpha_5 + \alpha_5\alpha_3\alpha_6 + \alpha_6\alpha_4\alpha_7 + \alpha_7\alpha_5\alpha_1 + \alpha_1\alpha_6\alpha_2 + \alpha_2\alpha_7\alpha_3$, invariant under $\mathrm{PSL}(3,2)$.

The 30-ic resolvent is:

$$R_2(x) = R_{S_7}(f, F_2) = \prod_{\sigma \in S_7/\mathrm{PSL}(3,2)} (x - F_2^{\sigma}).$$

Degree:k= $\frac{|S_7|}{|\mathrm{PSL}(3,2)|} = \frac{5040}{168} = 30$.

Factorization

The factorization of $R_2(x)$ depends on $\mathrm{Gal}(f)$:

- If $\mathrm{Gal}(f) \subseteq \mathrm{PSL}(3,2)$, $R_2(x)$ **splits** into factors of degrees 1, 7, 8, and 14, reflecting orbits of $\mathrm{PSL}(3,2)$ on $S_7/\mathrm{PSL}(3,2)$.
- If $\mathrm{Gal}(f) = S_7$, $R_2(x)$ is **irreducible**, as S_7 acts transitively on the 30 cosets.

The 120-ic Resolvent

The **120-ic resolvent**, a degree 120 polynomial, tests if the Galois group lies in $C_7 \rtimes C_6$.

Definition

Let

- $G = S_7$
- $H = C_7 \rtimes C_6$
- $F_3 = \alpha_3\alpha_1(\alpha_4 + \alpha_7) + \alpha_2\alpha_5(\alpha_4 + \alpha_3) + \alpha_5\alpha_6(\alpha_3 + \alpha_7) + \alpha_4\alpha_6(\alpha_7 + \alpha_3) + \alpha_5\alpha_1(\alpha_7 + \alpha_6) + \alpha_1\alpha_2(\alpha_6 + \alpha_4) + \alpha_2\alpha_7(\alpha_3 + \alpha_6)$,

The resolvent is:

$$R_3(x) = R_{S_7}(f, F_3) = \prod_{\sigma \in S_7/(C_7 \rtimes C_6)} (x - F_3^\sigma).$$

Degree: k=$\frac{|S_7|}{|C_7 \rtimes C_6|} = \frac{5040}{42} = 120$.

Factorization

Factorization of $R_3(x)$:

- If $\mathrm{Gal}(f) \subseteq C_7 \rtimes C_6$, $R_3(x)$ **splits** into factors of degrees 1, 7, 14, 21, 21, and 42.
- If $\mathrm{Gal}(f) = S_7$, $R_3(x)$ is **irreducible**

Resolvent Factorization Patterns

The factorization of R_1, R_2, R_3 over $\mathbb{Q}$ determines $\mathrm{Gal}(f)$:

G	R_1	R_2	R_3
S_7	2	30	120
A_7	1, 1	15, 15	120
PSL(3, 2)	1, 1	1, 7, 8, 14	8, 56, 56
$C_7 \rtimes C_6$	2	2, 14, 14	1, 7, 14, 21, 21, 42
$C_7 \rtimes C_3$	1, 1	1, 7, 7, 7, 7	1, 7, 7, 7, 7, 21, 21, 21, 21
D_7	2	2, 14, 14	1, 7, 7, 7, 7, 7, 7, 14, 14, 14, 14, 14
C_7	1, 1	1, 7, 7, 7, 7	1, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7

Table: Factorization degrees of resolvents for each transitive subgroup of S_7.

Resolvent Polynomials of Septics

Let $f(x)$ be an irreducile septic given by

$$f(x) = x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

with roots $(\alpha_1, \ldots, \alpha_7)$. Denote by $G = S_7$ and

$$F = \alpha_1 + \alpha_2 + \alpha_3$$

Determine $\mathrm{Res}_{S_7}(f, F)(x)$.
The stabilizer is $H = S_3 \times S_4$, where S_3 permutes $\{1, 2, 3\}$ and S_4 permutes $\{4, 5, 6, 7\}$. Thus, $|H| = 3! \cdot 4! = 6 \cdot 24 = 144$, and

$$k = \frac{5040}{144} = 35 = \binom{7}{3}.$$

Hence,

$$R(f, F) = \prod_{1 \le i < j < k \le 7} (x - F^\sigma)$$

Symbolic computation Resolvent Polynomials of Septics

The symmetric sums:

$$s_1 = -a_6, \quad s_2 = a_5, \quad s_3 = -a_4, \quad s_4 = a_3, \quad s_5 = -a_2, \quad s_6 = a_1, \quad s_7 = -a_0.$$

Compute power sums

$$p_m = \sum_{i<j<k} (\alpha_i + \alpha_j + \alpha_k)^m.$$

Hence, we have:

$$\begin{aligned}
p_1 &= 15s_1 = -15a_6, \\
p_2 &= 15(s_1^2 - 2s_2) + 10s_2 = 15a_6^2 - 30a_5 + 10a_5 = 15a_6^2 - 20a_5, \\
p_3 &= 15(s_1^3 - 3s_1s_2 + 3s_3) + 45(s_1s_2 - 3s_3) + s_3 \\
&= -15a_6^3 + 45a_6a_5 - 45a_4 - 45a_6a_5 + 135a_4 - a_4 = -15a_6^3 + 89a_4, \\
p_4 &= 15(s_1^4 - 4s_1^2s_2 + 2s_2^2 + 4s_1s_3 - 4s_4) + 60(s_1^2s_2 - 2s_2^2 - s_1s_3 + s_4) + 15s_2^2 + 4s_4 \\
&= 15a_6^4 - 80a_6^2a_5 + 20a_5^2 + 56a_6a_4 - 56a_3, \\
p_5 &= 15(s_1^5 - 5s_1^3s_2 + 5s_1^2s_3 + 5s_1s_2^2 - 5s_2s_3 - 5s_1s_4 + 5s_5) + 75(s_1^3s_2 - 2s_1s_2^2 - s_1^2s_3 \\
&\quad + s_3^2 + s_1s_4 - s_5) + 10s_1s_2^2 + 45(s_1^2s_3 - 2s_1s_4 + s_2s_3) + 5s_5 \\
&= -15a_6^5 + 125a_6^3a_5 - 75a_6^2a_4 - 50a_6a_5^2 + 178a_6a_3 - 56a_2, \\
&\vdots \\
p_{35} &= -35a_0^5 + 175a_0^4(-a_6a_1 + a_5a_2 - a_4a_3) + \cdots
\end{aligned}$$

Symbolic computation Resolvent Polynomials of Septics

Using Newton's identities we have

$$
\begin{aligned}
e_1 &= -15a_6,\\
e_2 &= 105a_6^2 + 10a_5,\\
e_3 &== -455a_6^3 + 150a_6a_5 + \frac{89}{3}a_4,\\
e_4 &= 1365a_6^4 - 980a_6^2a_5 - \frac{80}{3}a_5^2 - \frac{596}{3}a_6a_4 + \frac{56}{3}a_3,\\
e_5 &= -4095a_6^5 + 3675a_6^3a_5 + 200a_6^2a_4 - 900a_6a_5^2 - 56a_5a_4 - \frac{2972}{5}a_6a_3 + \frac{356}{5}a_2,\\
e_6 &= 12285a_6^6 - 14175a_6^4a_5 - 910a_6^3a_4 + 5775a_6^2a_5^2 + 672a_6a_5a_4 + 80a_5^3 + 1660a_6^2a_3\\
&\quad - 672a_5a_3 - 252a_6a_2 + \frac{1068}{5}a_1,\\
e_{35} &= -843124185927587655a_6^{35} + 2581639930256873850a_6^{33}a_5 + 5237060773262740053a_6^{32}a_4\\
&\quad - 900570717176801865 00a_6^{31}a_5^2 - 3057764699596385747a_6^{30}a_5a_4 - 2747071717680186000 00a_6^{29}a_5^3\\
&\quad - 1200245779080946137 0a_6^{31}a_3 + 4011409893325719832a_6^{29}a_5a_3 + 1235966677377682877a_6^{28}a_5^2a_4\\
&\quad + 164795556983691051a_6^{27}a_5^3a_4 + 1298532235951804536a_6^{30}a_2 - 2963846288730429167a_6^{28}a_5a_2\\
&\quad - 328591113967382076a_6^{27}a_5^2a_3 - 328591113967382076a_6^{26}a_5^3a_2 + 492886670951073114a_6^{29}a_1\\
&\quad - 985773341902146228a_6^{27}a_5a_1 + 328591113967382076a_6^{28}a_0 - 164295556983691038a_6^{26}a_5a_0 - a_0^5.
\end{aligned}
$$

Resolvent Polynomials of Septics

For irreducible f of degree 7, the following table is used to determine candidates for $\mathrm{Gal}(f)$ given the factorization of a linear resolvent, which in turn determines the orbit-length partition of r-sets under $\mathrm{Gal}(f)$:

G	3-sets
S_7	35
A_7	35
$L(3,2)$	$7, 28$
$C_7 \rtimes C_6$	$14, 21$
$C_7 \rtimes C_3$	$7, 7, 21$
D_7	$7, 7, 7, 7, 14$
C_7	$7, 7, 7, 7, 7$

Database of the irreducible polynomials

We build a database of irreducible polynomials $f \in \mathbb{Q}[x]$ of degree $\deg f = n$. The data is organized in a Python dictionary. Each polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ is represented by its corresponding binary form $f(x, y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$. In this way, each polynomial is identified with a point in the projective space $\mathbb{P}^n$, represented by the integer coordinates

$$\mathbf{p} = [a_n : \cdots : a_0] \in \mathbb{P}^n,$$

where $\gcd(a_0, \ldots, a_n) = 1$.
Since $f(x)$ is irreducible over $\mathbb{Q}$ and has degree n, we must have $a_n \neq 0$ and $a_0 \neq 0$. Moreover, its discriminant Δ_f is nonzero.
Next, we generate a dataset of these polynomials with a bounded height h. Let denote by $\mathcal{P}_h^n$ the set of points corresponding to these polynomials, i.e.,

$$\mathcal{P}_h^n := \{\mathbf{p} = [a_n : \cdots : a_0] \in \mathbb{P}^n \mid a_0 a_n \neq 0, \Delta_f \neq 0\}.$$

To guarantee that each entry in the database is unique, we index the Python dictionary by the tuple $(a_0, \ldots, a_n)$. This approach ensures that polynomials are not recorded more than once in the Python dictionary.
For fixed h and n, the cardinality of $\mathcal{P}_h^n$ is bounded by

$$|\mathcal{P}_h^n| \leq 4h^2(2h+1)^{n-2}.$$

Database of the irreducible septics

For the case of degree $d \geq 7$ and a given height h, we construct these sets using SageMath as illustrated below:

$$PP = ProjectiveSpace(d, QQ)$$

$$rational.points = PP.rational.points(h)$$

After generating the points, the data is normalized by clearing denominators so that all coordinates become integers. We then retain only those polynomials that are irreducible over $\mathbb{Q}$. For each point $\mathbf{p} \in \mathbb{P}^n$, we compute the following:

$$(a_0, \ldots, a_n) : [H(f), [\xi_0, \ldots, \xi_n, \Delta_f], \quad \text{sig}, \text{Gal}_Q(f)].$$

Here, $H(f)$ denotes the height of $f(x)$, $[\xi_0, \ldots, \xi_n]$ are the generators of the ring of invariants for binary forms of degree n, the discriminant Δ_f, sig is the signature, and $\text{Gal}_Q(f)$ indicates the GAP identifier of the Galois group.

Database of the irreducible septics

We create a database of all rational points $\mathbf{p} \in \mathbb{P}^7$ with projective height $h \leq 4$ such that

$$f(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

Table: Counts for Groups with Height ≤ 4

Galois Group	Count
S_7	584,324
A_7	138
PSL$(3,2)$	136
D_7	18
$C_7 \rtimes C_6$	4
$C_7 \rtimes C_3$	0
C_7	0

Dominance of S_7; absence of $C_7 \rtimes C_3$ and C_7 at low heights.

Database of the irreducible septics

- No polynomials with Galois groups C_7 or F_{21} found for height ≤ 4.
- Searched Jürgen-Klüner database and found one C_7 polynomial at height 28:

$$f(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1.$$

To solve this problem we construct explicit septic polynomials via the framework of constructive Galois theory. Our approach marries geometric insights from branched coverings and Hurwitz spaces with an algebraic construction using cyclotomic fields.

Constructing C_7 Polynomials

Table: Irreducible degree-7 polynomials with Galois group C_7.

Coefficients	Height	p	Galois
$(1, 1, -12, -7, 28, 14, -9, 1)$	28	29	C_7
$(1, 1, -18, -35, 38, 104, 7, -49)$	104	43	C_7
$(1, 1, -30, 3, 254, -246, -245, 137)$	254	71	C_7
$(1, 1, -48, 37, 312, -12, -49, -1)$	312	113	C_7
$(1, 1, -54, -31, 558, -32, -1713, 1121)$	1713	127	C_7
$(1, 1, -84, -217, 1348, 3988, -1433, -1163)$	3988	197	C_7
$(1, 1, -90, 69, 1306, 124, -5249, -4663)$	5249	211	C_7
$(1, 1, -102, -195, 1850, 978, -8933, 5183)$	8933	239	C_7
$(1, 1, -120, -711, -784, 1956, 2863, -343)$	2863	281	C_7
$(1, 1, -144, 399, 2416, -10808, 10831, -1237)$	10831	337	C_7
$(1, 1, -162, -201, 7822, 12322, -107717, -193369)$	193369	379	C_7
$(1, 1, -180, -103, 6180, 11596, -25209, -49213)$	49213	421	C_7
$(1, 1, -192, 275, 3952, 4136, -81, -863)$	4136	449	C_7
$(1, 1, -198, -907, 4302, 20582, -18973, -56911)$	56911	463	C_7
$(1, 1, -210, 1423, -1410, -8538, 9203, 19427)$	19427	491	C_7
$(1, 1, -234, 335, 13254, -42874, -55309, 71879)$	71879	547	C_7
$(1, 1, -264, -151, 13288, 18556, -69425, 34621)$	69425	617	C_7

Machine Learning for Galois Group Classification

- Dataset: 584,724 degree-7 polynomials.
- Random Forest classifier using polynomial coefficients.
- Imbalanced data led to near 100% accuracy but poor performance on minority classes.
- Improve Dataset by excluding S_7, and computing the invariants $\xi_0, \ldots, \xi_4$.
- Accuracy improved to 91% (from 54%); strong performance.

Challenges for Higher Degrees

- Degree 7 is Implemented in SageMath, but challenges arise for $n > 10$.
- Determining the set of resolvents that uniquely identify Galois groups for any degree n.
- Finding polynomial classes for each transitive subgroup of S_n.
- Computing invariants becomes computationally intensive for $n > 10$
- Study degrees ≤ 16 to train machine learning models for higher-degree patterns.

Thank You for Your Attention!

References


Foulkes, H. O. (1930). The resolvents of an equation of the seventh degree. *Quart. J. of Math.*, 2, 9–19.


Soicher, L., & McKay, J. (1985). Computing Galois groups over the rationals. *Journal of Number Theory*, 20(3), 273–281.


Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Springer-Verlag.