Galois groups of low-dimensional abelian varieties over finite fields

Santiago Arango-Piñeros
https://sarangop1728.github.io/

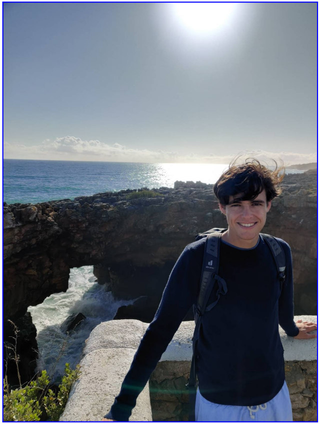
Emory University

Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation Annual Meeting

January 15, 2025

Joint work with Sam Frengley and Sameera Vemulapalli

Available at https://arxiv.org/abs/2412.03358.



Abelian varieties over finite fields in the LMFDB

Abelian variety isogeny class 3.25.aj_cm_aom over $\mathbb{F}_{5^2}$

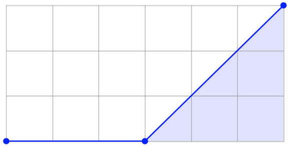
Invariants

Base field:	$\mathbb{F}_{5^2}$
Dimension:	3
L-polynomial:	$1 - 9x + 64x^2 - 376x^3 + 1600x^4 - 5625x^5 + 15625x^6$
Frobenius angles:	$\pm0.117284553158, \pm0.414402510947, \pm0.596508349316$
Angle rank:	3 (numerical)
Number field:	6.0.126826829844.1
Galois group:	$S_4 \times C_2$
Isomorphism classes:	23520

This isogeny class is simple and geometrically simple, primitive, ordinary, and not supersingular. It is principally polarizable and contains a Jacobian.

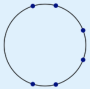
Newton polygon

This isogeny class is ordinary.



Properties

Label 3.25.aj_cm_aom



Base field	$\mathbb{F}_{5^2}$
Dimension	3
p-rank	3
Ordinary	yes
Supersingular	no
Simple	yes
Geometrically simple	yes
Primitive	yes
Principally polarizable	yes
Contains a Jacobian	yes

Related objects

L-functions

Downloads

All stored data to text

Curves to text

Underlying data

Learn more

Source and acknowledgments

The Galois group

Given A of dimension g over $\mathbf{F}_q$, the Frobenius polynomial $P_A(T)$ is the characteristic polynomial of the q-Frobenius endomorphism, acting on the Tate module $T_\ell A$, for some prime $\ell \nmid q$.

- $P_A(T) \in \mathbf{Z}[T]$ has degree $2g$.
- The Frobenius eigenvalues come in complex conjugate pairs $\alpha_1, \overline{\alpha}_1, \ldots, \alpha_g, \overline{\alpha}_g \in \overline{\mathbf{Q}}$ and satisfy $|\alpha|^2 = \alpha \cdot \overline{\alpha} = q$.

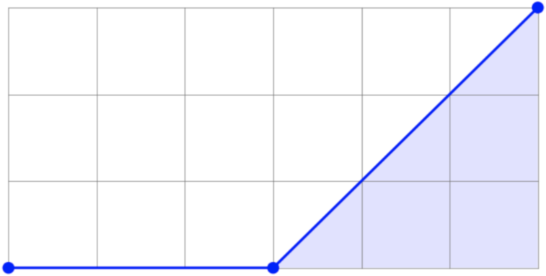
The Galois group $\mathrm{Gal}(A)$ is the Galois group of the splitting field of $P_A(T)$ over $\mathbf{Q}$.

The Newton polygon

If $p = \mathrm{char}\, \mathbf{F}_q$, let ν be the p-adic valuation of $\overline{\mathbf{Q}}$, normalized so that $\nu(q) = 1$. The Newton polygon of A is the ν-adic Newton polygon of $P_A(T)$.

Newton polygon

This isogeny class is ordinary.



p-rank:	3
Slopes:	$[0, 0, 0, 1, 1, 1]$

The Frobenius angle rank

Normalize the Frobenius eigenvalues $u_j := \alpha_j/\sqrt{q}$, so that we only remember their angles. The angle rank δ_A of $P_A(T)$ is the rank of the finitely generated abelian group $\langle u_1, \ldots, u_g \rangle \subset \overline{\mathbf{Q}}^{\times}$.

δ_A keeps track of the number of *multiplicative relations* between normalized Frobenius eigenvalues.

The Weyl group W_{2g}

The group W_{2g} is defined as the subgroup of the symmetries of the set of symbols $X_{2g} := \{1, \bar{1}, \ldots, g, \bar{g}\}$ that preserve the partition $\{1, \bar{1}\} \sqcup \cdots \sqcup \{g, \bar{g}\}$.

It is the centralizer in $\mathrm{Sym}(X_{2g}) \cong S_{2g}$ of the complex conjugation element

$$\iota_g := (1\bar{1}) \ldots (g\bar{g}).$$

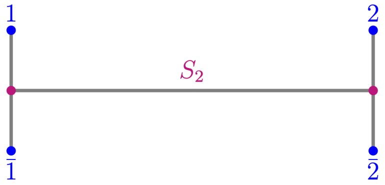


Figure: $W_4 \cong D_4$.

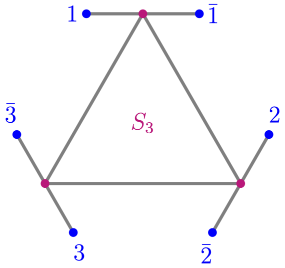


Figure: $W_6 \cong C_3 \wr S_3$

Understanding interactions between isogeny invariants

The Galois group, Newton polygon, and angle rank interact in subtle ways.

- The angle rank is zero if and only if A is supersingular.
- If the Galois group is maximal and $\delta_A > 0$, then $\delta_A = g$ is also maximal. The converse is not true.

Ahmadi and Shparlinski [AS10, Section 5] conjectured that every ordinary and geometrically simple Jacobian has maximal angle rank.[1]

Dupuy, Kedlaya, Roe, and Vincent [Dup+21] later found counterexamples to this conjecture, with the implementation of AVs over finite fields in the LMFDB.

[1] True in genus $g \leq 3$ by work of Zarhin [Zar15].

Newton slopes	Angle rank	Galois groups	Isogeny factors
$[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$	0	C_2	1.2.ac ^{3}
$[0, 0, \frac{1}{2}, \frac{1}{2}, 1, 1]$	1	C_2, C_2^2	1.2.ac × 2.2.ad_f
$[0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1]$	1	C_2, C_2	1.2.ac ^{2} × 1.2.ab
$[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$	0	C_2, C_2^2	1.2.ac × 2.2.ac_c
$[0, 0, 0, 1, 1, 1]$	1	C_6	simple
$[0, 0, \frac{1}{2}, \frac{1}{2}, 1, 1]$	2	C_2, D_4	1.2.ac × 2.2.ac_d
$[0, 0, 0, 1, 1, 1]$	2	C_2, C_2^2	1.2.ab × 2.2.ad_f
$[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$	0	C_2, C_2	1.2.ac ^{2} × 1.2.a
$[0, 0, \frac{1}{2}, \frac{1}{2}, 1, 1]$	1	C_2, C_2	1.2.ac × 1.2.ab ^{2}
$[0, 0, 0, 1, 1, 1]$	1	C_6	simple
$[0, 0, \frac{1}{2}, \frac{1}{2}, 1, 1]$	1	C_2, C_2^2	1.2.ac × 2.2.ab_ab
$[0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1]$	2	C_2, D_4	1.2.ac × 2.2.ab_a

Question

Can we explain/classify the possible triples (NP, G, δ) that occur for AVs over finite fields?

Our contribution

We explain and classify the possible triples (NP, G, δ) that occur for AVs over finite fields, for all abelian surfaces and simple abelian threefolds.

This builds on:

1. The classification of multiplicative relations between Frobenius eigenvalues, achieved in [ABS24].
2. The work of [DKZ24] in the geometrically simple case.

Our approach

1. We define a weighted permutation representation (only group theory).
   - Every A has an associated WPR $\rho\colon \mathrm{Gal}(A) \to W_{2g}$ coming from the action of the Galois group on the roots, weighting each root according to its p-adic valuation.[2]
2. Using Magma, we compute all the *admissible* weighted permutation representations.
3. We produce examples or prove that they do not occur.
   - So far, it seems like the only obstruction comes from the action of $\mathrm{Gal}(A)$ on the primes above p.

[2] A restatement of the Newton hyperplane representation of Dupuy, Kedlaya, and Zureick-Brown [DKZ24].

Corollaries of our classification

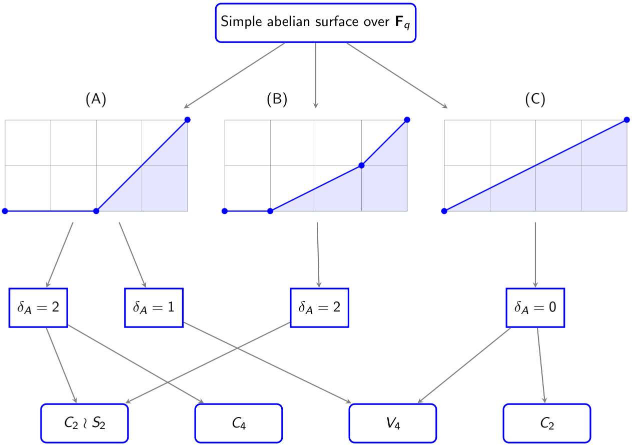


Figure: Possible isomorphism classes of Galois groups of simple abelian surfaces in terms of their Newton polygon, and angle rank δ_A.

Corollaries of our classification

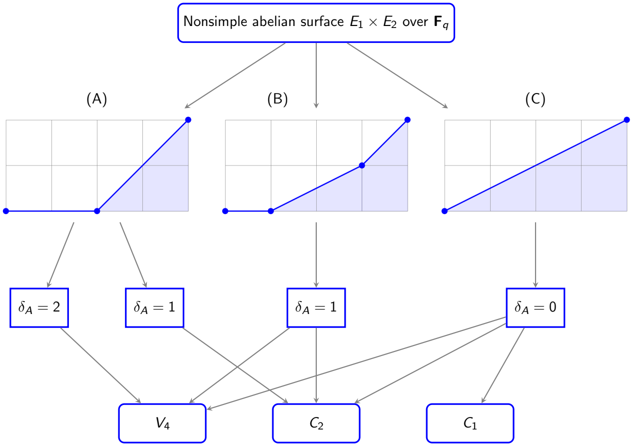


Figure: Possible isomorphism classes of Galois groups of simple abelian surfaces in terms of their Newton polygon, and angle rank δ_A.

Corollaries of our classification

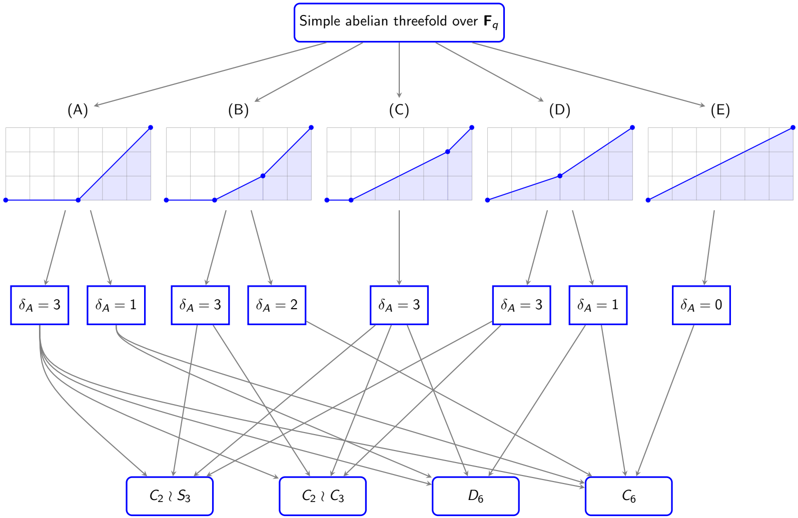


Figure: Possible isomorphism classes of Galois groups of simple abelian threefolds, in terms of their Newton polygon and angle rank δ_A.

Questions?

Table A.9

w_A-conjugacy class	Angle rank	Occurs	Geometrically simple	Example
W6.6.t.a.1	3	Yes	Yes	3.2.ab_ab_c
6T6.6.t.a.1	3	Yes	Yes	3.4.ac_ab_g
D6.6.t.a.1 D6.6.t.a.3	3	No		
D6.6.t.a.2 D6.6.t.a.4	2	Yes	Yes	3.2.ac_b_a
C6.6.t.a.1 C6.6.t.a.4	3	No		
C6.6.t.a.2 C6.6.t.a.3	2	No		

TABLE A.9. The images of the weighted permutation representations associated to simple almost ordinary abelian threefold (Newton polygon (B) in Figure 1.3).

Shioda's example

Let $q = p = 19$, and let $A = \mathrm{Jac}(C)$, where C is the smooth projective model over $\mathbf{F}_{19}$ of $y^2 = x^9 - 1$.

The curve C has genus $g = 4$ and therefore A is an abelian fourfold.

By calculating $\#C(\mathbf{F}_{19^r})$ for $r = 1, 2, 3, 4$, we are able to estimate the zeta function of C to enough precision to recover the Frobenius polynomial $P_A(T)$.

$$\begin{aligned} P_A(T) = T^8 &+ 8T^7 + 28T^6 + 8T^5 - 170T^4 \\ &+ 152T^3 + 10108T^2 + 54872T + 130321. \end{aligned}$$

This polynomial factors as $P_A(T) = P_E(T)P_B(T)$, where E is the elliptic curve $y^2 = x^3 - 1$ in the isogeny class 1.19.i, and B is an abelian threefold in the isogeny class 3.19.a_j_acm.

By the Honda–Tate theorem $A \sim E \times B$.

Shioda's example: multiplicative entanglement of the roots

Notice that $a_4 = -170$ is not divisible by $p = 19$, so A is ordinary.

The splitting field of $P_A(T)$ is $L_A = \mathbf{Q}(\zeta_9)$, where ζ_9 is a primitive 9^{th}-root of unity.

Let $R_E = \{\eta, 19/\eta\}$ and $R_B = \{\alpha, \beta, \gamma, 19/\alpha, 19/\beta, 19/\gamma\}$ the sets of roots of $P_E(T)$ and $P_B(T)$.

Recalling that $A \sim E \times B$, observe that $L_E = \mathbf{Q}(\sqrt{-3})$, which is contained in $L_B = \mathbf{Q}(\zeta_9)$. Note that $\mathrm{Gal}(L_A/\mathbf{Q})$ is a permutation group acting on the 8 element set $R_A = R_E \sqcup R_B$.

But, as abstract groups, $\mathrm{Gal}(L_A/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{Q}(\zeta_9)/\mathbf{Q}) \cong C_6$.

For an appropriate such labelling, we have

$$\eta = \frac{\alpha \cdot \beta \cdot \gamma}{19}\,.$$

Shioda's example: indexing the roots

An indexing of the roots R_A is for example

$$\alpha_1 = \alpha, \quad \alpha_2 = \beta, \quad \alpha_3 = \eta, \quad \alpha_4 = \gamma.$$

If we ensure that $\nu(\alpha) = \nu(\beta) = \nu(\gamma) = \nu(\eta) = 0$. The indexing remembers the valuations (weights) of the roots.

With this indexing, the weighted permutation representation $\rho \colon \mathrm{Gal}(L_A/\mathbf{Q}) \to W_8$ has image $H = \langle h \rangle$, where h is the permutation $(1\bar{2}\bar{4}\bar{1}24)(3\bar{3})$.

Warning. The image is unique up to conjugation by an element of W_{2g} that stabilizes "the slopes" of the Newton polygon.

The multiplicative relation from before becomes[3]

$$\alpha_3 = \frac{\alpha_1\alpha_2\bar{\alpha}_4}{19} = \frac{\alpha_1\alpha_2}{\alpha_4}.$$

[3] One can find this multiplicative relation by considering the Newton hyperplane matrix of this weighted permutation representation, and computing its kernel.

Bibliography I

[AS10] Omran Ahmadi and Igor E. Shparlinski. “On the distribution of the number of points on algebraic curves in extensions of finite fields”. In: *Math. Res. Lett.* 17.4 (2010), pp. 689–699. ISSN: 1073-2780. DOI: 10.4310/MRL.2010.v17.n4.a9. URL: https://doi.org/10.4310/MRL.2010.v17.n4.a9.

[Zar15] Yuri G. Zarhin. “Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension”. In: *Journal of Pure and Applied Algebra* 219.6 (2015), pp. 2076–2098. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2014.07.024. URL: https://www.sciencedirect.com/science/article/pii/S0022404914002199.

[Dup+21] Taylor Dupuy et al. “Counterexamples to a Conjecture of Ahmadi and Shparlinski”. In: *Experimental Mathematics* (2021), pp. 1–5.

Bibliography II

[ABS24] Santiago Arango-Piñeros, Deewang Bhamidipati, and Soumya Sankar. “Frobenius Distributions of Low Dimensional Abelian Varieties Over Finite Fields”. In: *Int. Math. Res. Not. IMRN* 16 (2024), pp. 11989–12020. ISSN: 1073-7928,1687-0247. DOI: 10.1093/imrn/rnae148. URL: https://doi.org/10.1093/imrn/rnae148.

[DKZ24] Taylor Dupuy, Kiran S. Kedlaya, and David Zureick-Brown. “Angle ranks of abelian varieties”. In: *Math. Ann.* 389.1 (2024), pp. 169–185. ISSN: 0025-5831,1432-1807. DOI: 10.1007/s00208-023-02633-7. URL: https://doi.org/10.1007/s00208-023-02633-7.