Computing Sato–Tate and monodromy groups

VaNTAGe Seminar, May 5th 2020

David Zywina

Cornell University

Consider an abelian variety A of dimension $g \geq 1$ defined over a number field K.

- Associated to each non-zero prime ideal $\mathfrak{p} \subseteq \mathscr{O}_K$ for which A has good reduction, there is a Frobenius polynomial

  $$P_{\mathfrak{p}}(x) \in \mathbb{Z}[x].$$

  Here is one characterization: for $n \in \mathbb{Z}$, $P_{\mathfrak{p}}(n)$ is the degree of the endomorphism $n - \pi_{\mathfrak{p}}$ of the reduction of A modulo $\mathfrak{p}$, where $\pi_{\mathfrak{p}}$ is the Frobenius endomorphism.

- For concreteness, you can think of A as being the Jacobian of an explicit smooth projective curve C over K with genus $g \geq 1$.

  If C has good reduction at $\mathfrak{p}$, the polynomial $P_{\mathfrak{p}}(x)$ is the (reverse) of the numerator of the zeta function of the reduction of C modulo $\mathfrak{p}$.

  The polynomials $P_{\mathfrak{p}}(x)$ are computable by point counting (see Drew's talk for more sophisticated methods).

- From Weil, we know that all of the roots of $P_\mathfrak{p}(x)$ in $\mathbb{C}$ have absolute value $\sqrt{N(\mathfrak{p})}$. Let

$$\widetilde{P}_\mathfrak{p}(x) \in \mathbb{R}[x]$$

be the monic polynomial obtained by scaling the roots of $P_\mathfrak{p}(x)$ so that they all have absolute value 1.

- The coefficients of $\widetilde{P}_\mathfrak{p}(x) \in \mathbb{R}[x]$ are bounded independent of $\mathfrak{p}$. It is natural to study how these polynomials vary with respect to the real topology.

The Sato–Tate conjecture (preliminary version)

As the prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ varies, the polynomials $\widetilde{P}_\mathfrak{p}(x)$ are distributed like the characteristic polynomial of a random matrix in a certain compact Lie group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$.

We will define the Sato–Tate group ST_A. First we consider the ℓ-adic representations of A.

ℓ-adic Galois representations

Take any prime ℓ.

- The set of points $A(\bar{K})$ is an abelian group with an action of $\mathrm{Gal}_K := \mathrm{Gal}(\bar{K}/K)$ that respects the group structure.
- For each positive integer n, let $A[\ell^n]$ be the ℓ^n-torsion subgroup of $A(\bar{K})$. The group $A[\ell^n]$ is a free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank $2g$ and comes with a natural Gal_K-action.
- Define

$$V_\ell := (\varprojlim_n A[\ell^n]) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell;$$

it is a $\mathbb{Q}_\ell$-vector space of dimension $2g$ with a Gal_K-action. We can express this Galois action in terms of a representation

$$\rho_\ell \colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell) = \mathrm{GL}_{V_\ell}(\mathbb{Q}_\ell)$$

Choosing a basis for V_ℓ would give a representation $\rho_\ell \colon \mathrm{Gal}_K \to \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. It is better for us not to make such a choice.

Compatibility

The representation

$$\rho_\ell \colon \mathrm{Gal}_K \to \mathrm{GL}_{V_\ell}(\mathbb{Q}_\ell)$$

encodes the Frobenius polynomials $P_\mathfrak{p}(x)$.

Take any non-zero prime ideal $\mathfrak{p} \subseteq \mathscr{O}_K$ for which A has good reduction and $\mathfrak{p} \nmid \ell$.

The representation ρ_ℓ is unramified at $\mathfrak{p}$ and we have

$$P_\mathfrak{p}(x) = \det(xI - \rho_\ell(\mathrm{Frob}_\mathfrak{p})) \in \mathbb{Q}_\ell[x].$$

Recall that $P_\mathfrak{p}(x)$ has coefficients in $\mathbb{Z}$ and is independent of ℓ.

ℓ-adic monodromy group

For each prime ℓ, we have defined a representation

$$\rho_\ell \colon \operatorname{Gal}_K \to \operatorname{GL}_{V_\ell}(\mathbb{Q}_\ell),$$

where V_ℓ is a $\mathbb{Q}_\ell$-vector space of dimension $2g$.

Definition

The ℓ-adic monodromy group of A is the Zariski closure G_ℓ of $\rho_\ell(\operatorname{Gal}_K)$ in $\operatorname{GL}_{V_\ell}$; it is a linear algebraic group over $\mathbb{Q}_\ell$.

Aside: The group $\rho_\ell(\operatorname{Gal}_K)$ is an open subgroup of $G_\ell(\mathbb{Q}_\ell)$ with respect to the ℓ-adic topology. In particular, G_ℓ determines the image of ρ_ℓ up to commensurability.

Definition of Sato–Tate group

We have an abelian variety A of dimension $g \geq 1$ over a number field K.

- Choose a prime ℓ and an embedding $i\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.
- We have defined an algebraic group $G_\ell \subseteq \mathrm{GL}_{V_\ell}$. Using the Weil pairing on V_ℓ and a polarization, we in fact have an inclusion $G_\ell \subseteq \mathrm{GSp}_{V_\ell}$. Define

$$G_\ell^1 := G_\ell \cap \mathrm{Sp}_{V_\ell}.$$

Definition

The Sato–Tate group ST_A is a maximal compact subgroup of $G_\ell^1(\mathbb{C})$ with respect to the usual analytic topology, where we have used the embedding i.

We can view ST_A as a compact subgroup of $\mathrm{USp}(2g)$ by choosing a basis for $V_\ell \otimes_{\mathbb{Q}_\ell, i} \mathbb{C}$.

We have constructed a compact Lie group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$.

- Take any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ for which A has good reduction and $\mathfrak{p} \nmid \ell$. The matrix

$$\frac{i(\rho_\ell(\mathrm{Frob}_\mathfrak{p}))}{\sqrt{N(\mathfrak{p})}} \in G_\ell^1(\mathbb{C}). \qquad (\star)$$

  is semisimple and has characteristic polynomial $\widetilde{P}_\mathfrak{p}(x)$.
- Since the complex roots of $\widetilde{P}_\mathfrak{p}(x)$ have absolute value 1, there is an element $\vartheta_\mathfrak{p} \in \mathrm{ST}_A$ that is conjugate in $G_\ell^1(\mathbb{C})$ to $(\star)$.

  Note that $\vartheta_\mathfrak{p}$ is well-defined up to conjugacy and has characteristic polynomial $\widetilde{P}_\mathfrak{p}(x)$.

The Sato–Tate conjecture says that the elements $\{\vartheta_\mathfrak{p}\}_\mathfrak{p}$ are *equidistributed* in the conjugacy classes of ST_A with respect to the Haar measure.

The Sato–Tate conjecture says that the elements $\{\vartheta_{\mathfrak{p}}\}_{\mathfrak{p}}$ are *equidistributed* in the conjugacy classes of ST_A with respect to the Haar measure.

Equivalently:

The Sato–Tate conjecture

For any continuous central function $f\colon \mathrm{ST}_A \to \mathbb{C}$, we have

$$\lim_{x\to\infty} \frac{1}{|P(x)|} \sum_{\mathfrak{p}\in P(x)} f(\vartheta_{\mathfrak{p}}) = \int_{\mathrm{ST}_A} f\, d\mu,$$

where $P(x)$ is the set of good prime ideals $\mathfrak{p} \subseteq \mathscr{O}_K$ of norm at most x and μ is the Haar measure on ST_A normalized so that $\mu(\mathrm{ST}_A) = 1$.

A few moments

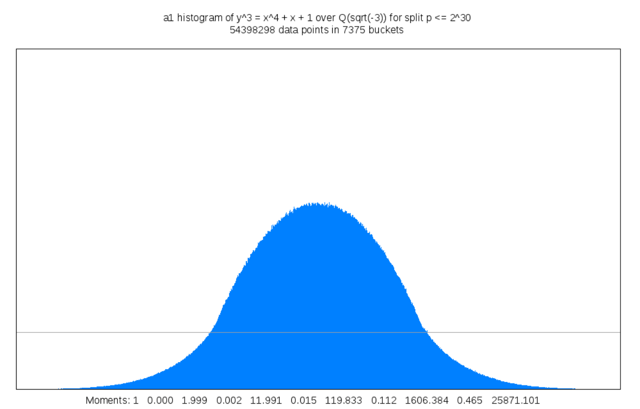
One technique that has been used to help figure out the group ST_A is to compute some moments.

Let $\mathrm{tr}: \mathrm{ST}_A \to \mathbb{R}$ be the trace function; so $\mathrm{tr}(\vartheta_{\mathfrak{p}})$ is the sum of the roots of $P_{\mathfrak{p}}(x)$ divided by $\sqrt{N(\mathfrak{p})}$. For an integer $n \geq 0$, define the *n-th moment*

$$m_n := \int_{\mathrm{ST}_A} \mathrm{tr}^n \, d\mu.$$

By computing $\mathrm{tr}(\vartheta_{\mathfrak{p}})^n$ for *many* $\mathfrak{p}$, we get approximations for m_n (assuming the Sato–Tate conjecture).

Let A be the Jacobian of the curve $y^3 = x^4 + x + 1$ over $\mathbb{Q}(\sqrt{-3})$.
Here is a histogram[1] of $\mathrm{tr}(\vartheta_{\mathfrak{p}})$ for $\mathfrak{p}$ of norm at most 2^{30}.



The actual moments m_n are: 1, 0, 2, 0, 12, 0, 120, 0, 1610, 0, 25956, ...

[1] See https://math.mit.edu/~drew/g3SatoTateDistributions.html

Problem

Compute/predict the group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$.

- The possible Sato–Tate groups $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$ have been classified by Fité, Kedlaya, Rotger and Sutherland for small dimensions ($g \leq 3$).
- When $g = 3$, there are 410 possibilities for ST_A and 14 possibilities for the identity component ST_A°.
- The classification of the groups gets *much* harder as g grows.

When $g \geq 4$, the endomorphism ring of $A_{\overline{K}}$ need no longer determine the group ST_A.

When $g \geq 4$, we do not know if the group ST_A, as defined above, is independent of the initial choice of ℓ.

Connectedness assumption

For simplicity, we now assume that all the groups G_ℓ are connected.
Serre: this can be achieved by replacing K by an appropriate finite extension.

Equivalently, ST_A is connected.

How to describe ST_A?

- From Faltings, we know that G_ℓ is reductive. So G_ℓ over $\overline{\mathbb{Q}}_\ell$ is determined, up to isomorphism, by its root datum.
- The natural representation of G_ℓ is then determined, up to isomorphism, from the corresponding weights (with multiplicities).
- So the group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$ can be described in terms of this combinatorial data.
- Via Weyl's integration formula, this data is useful for computing integrals like those that occur in the Sato–Tate conjecture.

Idea: Look at $P_\mathfrak{p}(x)$ for a few primes $\mathfrak{p}$ and try to guess G_ℓ and hence ST_A.

Theorem (Z.)

Assume that the Mumford–Tate conjecture and the Strong compatibility conjecture for A hold. Then for "most" primes ideals $\mathfrak{p}$ and $\mathfrak{q}$ of $\mathscr{O}_K$, the polynomials

$$P_{\mathfrak{p}}(x) \quad \text{and} \quad P_{\mathfrak{q}}(x)$$

determine the Sato-Tate group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$ up to conjugacy.

Moreover, they determine the group G_ℓ and its representation V_ℓ, up to isomorphism, for all sufficiently large ℓ.

Remarks

- "most"?: the theorem holds for all $\mathfrak{p} \notin S$ and $\mathfrak{q} \notin S_{\mathfrak{p}}$, where S and $S_{\mathfrak{p}}$ have density 0 (and $S_{\mathfrak{p}}$ depends on $\mathfrak{p}$).
- Two primes suffice!!

Theorem (Z.)

Assume that the Mumford–Tate conjecture and the Strong compatibility conjecture for A hold. Then for "most" primes ideals $\mathfrak{p}$ and $\mathfrak{q}$ of $\mathscr{O}_K$, the polynomials

$$P_{\mathfrak{p}}(x) \quad \text{and} \quad P_{\mathfrak{q}}(x)$$

determine the Sato-Tate group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$ up to conjugacy.

Moreover, they determine the group G_ℓ and its representation V_ℓ, up to isomorphism, for all sufficiently large ℓ.

More remarks

The proof actually gives an algorithm (implemented with `Magma`).

Can consider more primes for confidence. It is essentially a Monte Carlo algorithm; the probability that a incorrect answer is outputted decays exponentially in terms of the number of primes considered.

Aside: what does a prediction for G_ℓ tell us?

- A prediction for G_ℓ gives a prediction for the dimensions of the $\mathbb{Q}_\ell$-vector spaces

$$H^{2i}_{\text{ét}}(A^j_{\overline{K}}, \mathbb{Q}_\ell(i))^{\mathrm{Gal}_K}.$$

- The Tate conjecture says that this space should be spanned by classes arising from subvarieties of $A^j_{\overline{K}}$ of codimension i.
- If you can find/prove the existence of these algebraic cycles, then you should be able to actually determine G_ℓ *unconditionally*.

So another way to view the above theorem, is as a way to make predictions about the algebraic cycles of an abelian variety.

(Due to the Mumford–Tate conjecture hypothesis, similar remarks will hold for the Hodge conjecture for powers of A.)

The Mumford–Tate conjecture

- Fix an embedding $\overline{K} \subseteq \mathbb{C}$. Define the $\mathbb{Q}$-vector space $V := H_1(A(\mathbb{C}),\mathbb{Q})$.
- The Mumford–Tate group is a certain connected and reductive group

$$G \subseteq \mathrm{GL}_V$$

  defined over $\mathbb{Q}$; it is constructed using the Hodge decomposition of $(V \otimes_{\mathbb{Q}} \mathbb{C})^\vee = H^1(A(\mathbb{C}),\mathbb{C})$.
- For each prime ℓ, we have a comparison isomorphism $V_\ell = V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. So we can view $G_{\mathbb{Q}_\ell}$ as a subgroup of GL_{V_ℓ}.

The Mumford–Tate conjecture

For each prime ℓ, we have $G_\ell = G_{\mathbb{Q}_\ell}$.

So conjecturally, the G_ℓ arise from a common group G. We should try to find the root data of G!

Also the Mumford–Tate conjecture implies that our construction of ST_A does not depend on the choice of prime ℓ or embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. (The conjecture can also be used to show that ST_A is well-defined without our ongoing connected assumption.)

Strong compatibility conjecture

Choose a prime ℓ and an embedding $i\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.
Assume that the Mumford–Tate conjecture for A holds.

Take any prime ideal $\mathfrak{p} \subseteq \mathscr{O}_K$ satisfying $\mathfrak{p} \nmid \ell$ for which A has good reduction.

Strong compatibility conjecture

The conjugacy class of $G(\mathbb{C})$ containing $i(\rho_\ell(\mathrm{Frob}_\mathfrak{p}))$ does not depend on the choice of ℓ or i.

Equivalently, the conjugacy class of $\vartheta_\mathfrak{p}$ in ST_A does not depend on the choice of ℓ or i.

Remark:

- This is stronger than usual (unconditional) compatibility that says that the characteristic polynomial $P_\mathfrak{p}(x)$ of $i(\rho_\ell(\mathrm{Frob}_\mathfrak{p}))$ does not depend on ℓ or i.
- Actually known quite generally....

Frobenius torus

The first step in computing the root datum of the Mumford–Tate group G is to choose a *maximal torus*.

Assume the Mumford–Tate conjecture for A and Strong compatibility conjecture

- Take a "random" prime $\mathfrak{p} \subseteq \mathscr{O}_K$.
- Let
$$X_{\mathfrak{p}} \subseteq \overline{\mathbb{Q}}^{\times}$$
be the subgroup generated by the roots of $P_{\mathfrak{p}}(x)$. It has a $\mathrm{Gal}_{\mathbb{Q}}$-action and is computable!
- Up to isomorphism, there is a unique torus $T_{\mathfrak{p}}$ defined over $\mathbb{Q}$ for which we have an isomorphism
$$X(T_{\mathfrak{p}}) = X_{\mathfrak{p}}$$
of $\mathrm{Gal}_{\mathbb{Q}}$-modules, where $X(T_{\mathfrak{p}})$ is the group of characters $(T_{\mathfrak{p}})_{\overline{\mathbb{Q}}} \to \mathbb{G}_{m,\overline{\mathbb{Q}}}$.
- We can identify $T_{\mathfrak{p}}$ with a maximal torus of G
(this is a white lie, it might only give a maximal torus of the quasi-split inner form of G.)

An example

- Let A be the Jacobian of the curve $y^2 = x^9 - 1$ over $K = \mathbb{Q}(\zeta_9)$; it has dimension 4.
- A has CM, so G is a torus. Therefore,

$$G = T_{\mathfrak{p}}$$

  for "most" $\mathfrak{p}$.
- Without more info, one expects that G is a torus of dimension 5. Note that the group $X(T_{\mathfrak{p}}) = X_{\mathfrak{p}}$ has rank at most 5 when one takes into account the relations $\pi\overline{\pi} = N(\mathfrak{p})$ for a root π of $P_{\mathfrak{p}}(x)$.
- Actually G has dimension 4 which implies that there is an unexpected multiplicative relation in the roots of $P_{\mathfrak{p}}(x)$.

An example (continued)

- A is the Jacobian of the curve $y^2 = x^9 - 1$ over $K = \mathbb{Q}(\zeta_9)$. We have

$$A \sim B \times E,$$

where B is a simple abelian variety of dimension 3 and E is an elliptic curve. So

$$P_{\mathfrak{p}}(x) = P_{B,\mathfrak{p}}(x) \cdot P_{E,\mathfrak{p}}(x).$$

- There are roots $a, b, c \in \overline{\mathbb{Q}}$ of $P_{B,\mathfrak{p}}(x)$ such that

$$-abc/N(\mathfrak{p})$$

is a root of $P_{E,\mathfrak{p}}(x)$. This is our unexpected relation between the roots of $P_{\mathfrak{p}}(x)$.

- Geometric explanation: A has an exceptional algebraic cycle.

The Weyl group

- Back to our general setting: A is a non-zero abelian variety over a number field K and G is the Mumford–Tate group.

  For a "random" $\mathfrak{p}$, we have a maximal torus $T_\mathfrak{p} \subseteq G$, where we have an isomorphism $X(T_\mathfrak{p}) = X_\mathfrak{p}$ that respects the $\mathrm{Gal}_\mathbb{Q}$-actions.

- The Weyl group of G is

  $$W(G, T_\mathfrak{p}) := N_G(T_\mathfrak{p})(\overline{\mathbb{Q}})/T_\mathfrak{p}(\overline{\mathbb{Q}}),$$

  where $N_G(T_\mathfrak{p})$ is the normalizer of $T_\mathfrak{p}$ in G.

  The group $W(G, T_\mathfrak{p})$ is finite and conjugation induces a faithful action on $T_\mathfrak{p}$ and $X(T_\mathfrak{p})$.

The Weyl group (continued)

- Recall, the Weyl group $W(G,T_{\mathfrak{p}})$ acts faithfully on $X(T_{\mathfrak{p}}) = X_{\mathfrak{p}}$.
- Now choose a second prime $\mathfrak{q}$. Let L be the splitting field of $P_{\mathfrak{q}}(x)$ over $\mathbb{Q}$.

Theorem

For "most" $\mathfrak{p}$ and $\mathfrak{q}$, Gal_L acts on $X(T_{\mathfrak{p}})$ as the Weyl group $W(G,T_{\mathfrak{p}})$.

So the first prime $\mathfrak{p}$ gives us a maximal torus $T_{\mathfrak{p}}$ of G.

The second prime $\mathfrak{q}$ gives us the Weyl group $W(G,T_{\mathfrak{p}})$ with its action on $X(T_{\mathfrak{p}})$.

- We have now described how to find a maximal torus $T_{\mathfrak{p}}$ of G and have found the Weyl group $W(G,T_{\mathfrak{p}})$ via its action on $X(T_{\mathfrak{p}})$.
- The next major step is to find the set of roots

$$R(G,T_{\mathfrak{p}}) \subseteq X(T_{\mathfrak{p}})$$

of G with respect to $T_{\mathfrak{p}}$.
- From the triple

$$\big(X(T_{\mathfrak{p}}), W(G,T_{\mathfrak{p}}), R(G,T_{\mathfrak{p}})\big)$$

one can recover the root datum of G; this describes G up to isomorphism over $\overline{\mathbb{Q}}$.

We can also describe the natural representation of $G_{\overline{\mathbb{Q}}}$ on $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$. The *weights* in $X(T_{\mathfrak{p}}) = X_{\mathfrak{p}}$ of the representation $G \subseteq \mathrm{GL}_V$ are given by the roots of $P_{\mathfrak{p}}(x)$ (with multiplicities).

From this information, we can compute the Sato–Tate group $\mathrm{ST}_A \subseteq \mathrm{USp}(2g)$.

Finding roots

- Let $\Omega \subseteq X(T_\mathfrak{p})$ be the set of weights of the representation V_ℓ of G_ℓ.
- The set Ω corresponds with the roots of $P_\mathfrak{p}(x)$ under the isomorphism $X(T_\mathfrak{p}) = X_\mathfrak{p}$. Set
$$W := W(G, T_\mathfrak{p}).$$
- Let $\Omega_1, \ldots, \Omega_s$ be the W-orbits in Ω. One can show that
$$R(G, T_\mathfrak{p}) \subseteq \bigcup_{i=1}^{s} \mathscr{C}_i,$$
where $\mathscr{C}_i := \{\alpha\beta^{-1} : \alpha, \beta \in \Omega_i, \alpha \neq \beta\}$.

This gives $R(G, T_\mathfrak{p})$ in a computable finite set. Now need to "sieve" it out.

KEY INPUT: the irreducible representations of $G_{\overline{\mathbb{Q}}}$ on $V \otimes_\mathbb{Q} \overline{\mathbb{Q}}$ are minuscule.

Sieving for roots (technical slide 1/3)

Let's give some details on the first step to pick out $R(G, T_{\mathfrak{p}})$ from $\cup_i \mathscr{C}_i$.

- Choose a W-orbit $\mathscr{O}$ in $\cup_i \mathscr{C}_i$ of minimal cardinality. We have $\mathscr{O} \subseteq \mathscr{C}_i$ for some i.
- Let S_1 be the set of elements in $\mathscr{C}_i$ that are in the span of $\mathscr{O}$ in $X(T_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{Q}$.
  Let r be the dimension of the span of $\mathscr{O}$ in $X(T_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition

There is a unique irreducible component R_1 of the root system $R(G, T_{\mathfrak{p}})$ with $R_1 \subseteq S_1$; it has rank r.

Sieving for roots (technical slide 2/3)

We can determine the Lie type of R_1!

Proposition

i) If $r \geq 1$, then R_1 has type A_r if and only if $|W| = (r+1)!$.

ii) If $r \geq 3$, then R_1 has type B_r if and only if $|W| = 2^r r!$ and S_1 consists of at least three W-orbits.

iii) If $r \geq 2$, then R_1 has type C_r if and only if $|W| = 2^r r!$ and S_1 consists of two W-orbits.

iv) If $r \geq 4$, then R_1 has type D_r if and only if $|W| = 2^{r-1} r!$.

Note: exceptional Lie types do not occur.

Sieving for roots (technical slide 3/3)

We can finally determine R_1.

Proposition

i) If $r \geq 1$ and R_1 is of type A_r, then R_1 is the unique W-orbit of S_1 of cardinality $r(r+1)$.

ii) If $r \geq 3$ and R_1 is of type B_r, then R_1 is the union of the unique W-orbits of S_1 of cardinality $2r$ and $2r(r-1)$.

iii) If $r \geq 2$ and R_1 is of type C_r, then $R_1 = S_1$.

iv) If $r \geq 4$ and R_1 is of type D_r, then R_1 is the unique W-orbit of S_1 with cardinality $2r(r-1)$.

Working in the orthogonal complement in $X(T_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ of R_1, we can continue in a similar manner and find $R(G, T_{\mathfrak{p}})$ and its decomposition into irreducible components.

- We now have root datum for G and a natural $\mathrm{Gal}_{\mathbb{Q}}$-action on it. Unfortunately, this is not enough to recover G.
- It is enough info to determine the quasi-split inner form G_0 of G.
- For ℓ sufficiently large, we have

$$(G_0)_{\mathbb{Q}_\ell} = G_{\mathbb{Q}_\ell}$$

and hence $(G_0)_{\mathbb{Q}_\ell} = G_\ell$.

So we have found G_ℓ for all ℓ sufficiently large.

Another example

Let A be the Jacobian of the curve

$$y^3 = x^4 + x + 1$$

over $K := \mathbb{Q}(\sqrt{-3})$. The groups G_ℓ are in fact connected.

- Let $\mathfrak{p} \subseteq \mathscr{O}_K$ be one of the prime ideals that divides 109. We have

$$P_\mathfrak{p}(x) = x^6 - 14x^5 + 224x^4 - 1871x^3 + 109 \cdot 224x^2 - 14 \cdot 109^2 x + 109^3.$$

- Choose roots $\pi_1, \pi_2, \pi_3 \in \overline{\mathbb{Q}}$ of $P_\mathfrak{p}(x)$ such that all the roots of $P_\mathfrak{p}(x)$ are either π_i or $\overline{\pi_i} = 109/\pi_i$. Moreover, we may choose the π_i so that they are roots of a cubic with coefficients in $\mathbb{Q}(\sqrt{-3})$.
- The group $X_\mathfrak{p} \subseteq \overline{\mathbb{Q}}^\times$ generated by the roots of $P_\mathfrak{p}(x)$ is free abelian of rank 4. In particular, it has basis

$$\pi_1, \pi_2, \pi_3, 109.$$

  With respect to the basis, we fix an isomorphism $X_\mathfrak{p} = \mathbb{Z}^4$.

We have fixed an isomorphism $X_{\mathfrak{p}} = \mathbb{Z}^4$. The roots of $P_{\mathfrak{p}}(x)$ is given by the set

$$\Omega = \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(-1,0,0,1),(0,-1,0,1),(0,0,-1,1)\}.$$

- Now choose a prime ideal $\mathfrak{q} \subseteq \mathscr{O}_K$ dividing 127; the group $X_{\mathfrak{q}}$ also has rank 4. Let L be the splitting field of $P_{\mathfrak{q}}(x)$ and let W be the Galois group of $P_{\mathfrak{p}}(x)$ over L.
  With respect to the action on $X_{\mathfrak{p}} = \mathbb{Z}^4$, we have

$$W = \left\{ \begin{pmatrix} B & \\ & 1 \end{pmatrix} : B \in \mathrm{GL}_3(\mathbb{Z}) \text{ a permutation matrix} \right\} \cong S_3.$$

- The set Ω has two W-orbits Ω_1 and Ω_2, and $R(G,T_{\mathfrak{p}})$ is a subset of

$$\bigcup_{i=1}^{2} \{\alpha - \beta : \alpha, \beta \in \Omega_i, \alpha \neq \beta\} = \{\pm(1,-1,0,0), \pm(1,0,-1,0), \pm(0,1,-1,0)\}.$$

- We find that the Lie type of the root system $R(G,T_{\mathfrak{p}})$ is of type A_2 and

$$R(G,T_{\mathfrak{p}}) = \{\pm(1,-1,0,0), \pm(1,0,-1,0), \pm(0,1,-1,0)\}.$$

Summary of our example

Recall that A is the Jacobian of the curve

$$y^3 = x^4 + x + 1$$

over $\mathbb{Q}(\sqrt{-3})$.

The root datum of G is determined by the following:

- $X(T_\mathfrak{p}) = \mathbb{Z}^4$,
- $W(G, T_\mathfrak{p})$ acts on $\mathbb{Z}^4$ by arbitrarily permuting the first three terms and fixing the last one,
- $R(G, T_\mathfrak{p}) = \{\pm(1,-1,0,0), \pm(1,0,-1,0), \pm(0,1,-1,0)\}$.

The weights are

$$\Omega = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (-1,0,0,1), (0,-1,0,1), (0,0,-1,1)\}.$$

One can then show that, up to conjugacy,

$$\mathrm{ST}(A) = \left\{ \left(\begin{smallmatrix} B & 0 \\ 0 & \overline{B} \end{smallmatrix}\right) : B \in U(3) \right\} \subseteq \mathrm{USp}(6).$$

Conclusions

Some pros to our approach for determining ST_A of an abelian variety A:

- Requires fewer primes.
- Does not require a classification and so one can consider higher g; I have done a lot of computations with $g = 8$.
- Root data gives a concise description. Moments are easy to compute (via Weyl integration formula).

Major con:

- Only computes ST_A°.
  [But ideally this would be useful info to then compute ST_A]

Conclusions

Some pros to our approach for determining ST_A of an abelian variety A:

- Requires fewer primes.
- Does not require a classification and so one can consider higher g; I have done a lot of computations with $g = 8$.
- Root data gives a concise description. Moments are easy to compute (via Weyl integration formula).

Major con:

- Only computes ST_A°.
  [But ideally this would be useful info to then compute ST_A]

Request

Do you have some interesting examples of abelian varieties over number fields? In particular, some which might have exceptional algebraic cycles.

Please send me an equation (or even better, a few dozen Frobenius polynomials!).

The end.