Computing ℓ-adic monodromy groups

CNTA XV, July 9th 2018

David Zywina

Cornell University

Abelian varieties

- Let A be an abelian variety of dimension $g \geq 1$ defined over a number field K. It will be fixed throughout the talk.
- You should think of A as being explicitly given. For example, A could be the Jacobian of the smooth projective curve over K with genus g. For example,

$$y^2 = x^9 + x^3 + 7x^2 + 5$$

  gives an abelian variety of dimension 4.
- Let $\overline{K}$ be a fixed algebraic closure of K and define $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$.

  The set of points $A(\overline{K})$ is an abelian group with a Gal_K-action that respects the group structure.

ℓ-adic Galois representations

- For each positive integer m, let $A[m]$ be the m-torsion subgroup of $A(\overline{K})$. We have $A[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2g}$ and it comes with a natural $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$ action.
- Take any prime ℓ. 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 gives $\mathrm{GL}_{V_\ell} \cong \mathrm{GL}_{2g}$ over $\mathbb{Q}_\ell$ and hence $\rho_\ell \colon \mathrm{Gal}_K \to \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. It is better for us not to make such a choice.

Compatibility

For each prime ℓ, we have defined a representation

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

- Take any non-zero prime ideal $\mathfrak{p} \subseteq \mathscr{O}_K$ for which A has good reduction.
- If $\mathfrak{p} \nmid \ell$, then ρ_ℓ is unramified at ℓ. Define the polynomial

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

  We have $P_\mathfrak{p}(x) \in \mathbb{Z}[x]$ and it is independent of ℓ.
- We view the polynomials $P_\mathfrak{p}(x)$ as being computable for our given A.
- The polynomials $P_\mathfrak{p}(x)$ know *a lot*; from Faltings we know that they determine ρ_ℓ up to isomorphism and A up to isogeny.

For each prime ℓ, we have defined a representation

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

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 $\rho_\ell(\mathrm{Gal}_K)$ in GL_{V_ℓ}; it is a linear algebraic group over $\mathbb{Q}_\ell$.

The algebraic group G_ℓ *almost* determines the image of ρ_ℓ (and it is much easier to study!). For example, $\rho_\ell(\mathrm{Gal}_K)$ is an open subgroup of $G_\ell(\mathbb{Q}_\ell)$ with respect to the ℓ-adic topology.

For each prime ℓ, we have defined a representation

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

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 $\rho_\ell(\mathrm{Gal}_K)$ in GL_{V_ℓ}; it is a linear algebraic group over $\mathbb{Q}_\ell$.

The algebraic group G_ℓ *almost* determines the image of ρ_ℓ (and it is much easier to study!). For example, $\rho_\ell(\mathrm{Gal}_K)$ is an open subgroup of $G_\ell(\mathbb{Q}_\ell)$ with respect to the ℓ-adic topology.

Moreover, there is a constant C such that

$$[G_\ell(\mathbb{Q}_\ell) \cap \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell) : \rho_\ell(\mathrm{Gal}_K)] \le C$$

holds for all ℓ, where $T_\ell := \varprojlim_n A[\ell^n]$.

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

Problem:

Can you compute G_ℓ? At least give an educated guess.

- Idea: Look at a few $P_\mathfrak{p}(x)$ and try to guess G_ℓ.
- How to describe G_ℓ?
  From Faltings, we know that G_ℓ is reductive. So G_ℓ over $\overline{\mathbb{Q}}_\ell$ is given, up to isomorphism, by its root datum.
  To pin down G_ℓ requires the root datum and a little more info.

Theorem

Assume the Mumford–Tate conjecture for A and assume that A has ordinary reduction at a set of primes of density 1.

For "random" 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 group G_ℓ and its representation V_ℓ, up to isomorphism, for all sufficiently large ℓ.

Remarks

- "Random"?: 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 $\mathfrak{p}$).
- The proof gives a practical algorithm; implemented!
- Two primes suffice!! Can use more primes for confidence.

Aside: what good is a guess for G_ℓ?

- A guess 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 of codimension i.
- If you can find/prove the existence of the predicted algebraic cycles, then you will get G_ℓ unconditionally.

  So computing G_ℓ is linked to interesting geometry of A.

The Mumford–Tate group

- Fix an embedding $\bar{K} \subseteq \mathbb{C}$. 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.

Frobenius torus

Assume the Mumford–Tate conjecture for A and assume that A has ordinary reduction at a set of primes of density 1.

- Take a “random” prime $\mathfrak{p} \subseteq \mathscr{O}_K$.
- Let
$$\Phi_{\mathfrak{p}} \subseteq \overline{\mathbb{Q}}^{\times}$$
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
$$X(T_{\mathfrak{p}}) = \Phi_{\mathfrak{p}}$$
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.

A maximal torus is the first step in finding the root datum 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 "random" $\mathfrak{p}$.
- Without more info, one expects that G is a torus of dimension 5. Note that the group $X(T_{\mathfrak{p}}) = \Phi_{\mathfrak{p}}$ 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 $P_{B,\mathfrak{p}}$ 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 Tate class.

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 $X(T_{\mathfrak{p}}) = \Phi_{\mathfrak{p}}$ 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 $X(T_{\mathfrak{p}}) = \Phi_{\mathfrak{p}}$.
- Now choose a second prime $\mathfrak{q}$. Let L be the splitting field of $P_{\mathfrak{q}}(x)$ over $\mathbb{Q}$.

Proposition

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

- 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

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

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

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 $X(T_{\mathfrak{p}}) = \Phi_{\mathfrak{p}}$.
  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 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 $R_1 \subseteq S$; 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 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 consists of two W-orbits.

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

Sieving for roots (technical slide 3/3)

We can 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 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 of cardinality $2r$ and $2r(r-1)$.

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

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

- 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.

The end.