Motives

Nir Elber

Spring 2024

Contents

1 Introduction

Here is the statement of the conjecture.

Conjecture 1. Fix an abelian motive A over a number field K, and let $G(A)$ denote the motivic Galois group of A. Suppose A has good reduction at a prime $\mathfrak{p}$ of K. Then there exists a class $F \in \operatorname{Conj} G(A)(\mathbb{Q})$ such that

$$F = [\rho_\ell(\operatorname{Frob}_\mathfrak{p})]$$

for each rational prime $\ell \nmid \mathfrak{p}$, where $\rho_\ell \colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{GL}\left(H^1_{\text{ét}}(A; \mathbb{Q}_\ell)\right)$ is the ℓ-adic Galois representation.

2 Background on Motives

Throughout, X denotes a smooth proper variety over a field k, which is possibly but not definitely algebraically closed.

2.1 Tannakian Formalism

Approximately speaking, the theory of (pure) motives takes the category of smooth proper varieties and attempts to give this category a long list of desirable properties. Tannakian formalism enumerates the desiderata. Our exposition follows [DM12] and [And04, Chapters 2 and 6].

Warning 2. We will not need any proofs from the theory of Tannakian formalism, so we will not provide them.

Intuitively, a Tannakian category is one that looks like the category $\mathrm{Rep}_k(G)$ of finite-dimensional representations of an affine k-group G. An important property of $\mathrm{Rep}_k(G)$ is the ability to take tensor products, so we codify how useful tensor products are.

Definition 3 (monoidal)**.** A *monoidal category* or $\otimes$*-category* is a category $\mathcal{C}$ equipped with a bifunctor $\otimes\colon \mathcal{C}\times\mathcal{C}\to\mathcal{C}$ and identity object $1\in\mathcal{C}$ with the following identities.

- Associativity: there is a natural isomorphism $\alpha\colon ((-\otimes-)\otimes-)\Rightarrow(-\otimes(-\otimes-))$.
- Identity: there are natural isomorphisms $(1\otimes-)\Rightarrow-$ and $(-\otimes 1)\Rightarrow 1$.

These isomorphisms satisfy certain coherence properties ensuring that one can associate and apply identity naturally in any suitable situation.

In fact, $\mathrm{Rep}_k(G)$ has a symmetry property.

Definition 4 (symmetric monoidal)**.** A *symmetric monoidal category* is a monoidal category $\mathcal{C}$ further equipped with a symmetry isomorphism $(-\otimes-)\Rightarrow(-\otimes-)$ such that the composite

$$(A\otimes B)\to(B\otimes A)\to(A\otimes B)$$

is the identity.

The reason we restricted $\mathrm{Rep}_k(G)$ to finite-dimensional representations is so that we can take duals.

Definition 5 (rigid)**.** A rigid symmetric monoidal category is a symmetric monoidal category $\mathcal{C}$ further equipped with a natural isomorphism $(-)^\vee\colon\mathcal{C}\to\mathcal{C}^{\mathrm{op}}$ such that each $A\in\mathcal{C}$ makes $(-\otimes A^\vee)$ is left adjoint to $(-\otimes A)$, and $(A^\vee\otimes-)$ is right adjoint to $(A\otimes-)$.

Remark 6. Rigidity permits a notion of dimension of an object $A\in\mathcal{C}$ as the composite

$$1\to A^\vee\otimes A\to A\otimes A^\vee\to 1.$$

Lastly, $\mathrm{Rep}_k(G)$ has a forgetful functor to Vec_k, akin to the forgetful functor $\mathrm{Set}(G)\to\mathrm{Set}$ which appears in Grothendieck's Galois theory (used to define the étale fundamental group).

Definition 7 (fiber functor)**.** Fix an abelian rigid symmetric monoidal category $\mathcal{C}$ such that $F:=\mathrm{End}(1)$ is a field. A *fiber functor* is a faithful exact $\otimes$-functor $\omega\colon\mathcal{C}\to\mathrm{Vec}_k$ for some finite field extension k of F. If $k=F$, then we say that $\mathcal{C}$ is *neutral Tannakian over* k.

What is remarkable is that it turns out that one can recover the affine k-group G from the (forgetful) fiber functor $\omega\colon\mathrm{Rep}_k(G)\to\mathrm{Vec}_k$ as "$\underline{\mathrm{Aut}}^\otimes(\omega)$." Explicitly, for a k-algebra R, an element of $\underline{\mathrm{Aut}}^\otimes(\omega)(R)$ is a collection of automorphisms $(g_X)_{X\in\mathrm{Rep}_k(G)}$ where g_X is an R-linear automorphism of $\omega(X)\otimes_k R$, and these automorphisms are natural in G-linear maps $X\to Y$.

This process can in general recover a group G from a neutral Tannakian category.

Theorem 8. Fix a neutral Tannakian category $\mathcal{C}$ over a field k equipped with fiber functor $\omega\colon\mathcal{C}\to\mathrm{Vec}_k$.

(a) The functor $\underline{\mathrm{Aut}}^\otimes(\omega)$ (defined analogously as above) is represented by an affine k-group G.

(b) The fiber functor ω then upgrades to a $\otimes$-equivalence $\mathcal{C}\to\mathrm{Rep}_k(G)$.

Proof. See [DM12, Theorem 2.11]. ■

It will be helpful to have some more concrete ways to understand G from its Tannakian category. For example, if the Tannakian category is small, then G should also be small. The following two propositions examine two versions of smallness.

Definition 9 ($\otimes$-subcategory)**.** Fix an abelian rigid symmetric monoidal category $\mathcal{C}$. Then the *full* $\otimes$*-subcategory* generated by a subset $S \subseteq \mathcal{C}$ of objects, denoted $\langle S \rangle^{\otimes}$ is the smallest abelian rigid monoidal subcategory.

Proposition 10. Fix an affine k-group G.

(a) Then G is finite if and only if there is an object X such that every object of $\mathrm{Rep}_k(G)$ is a subquotient of $X^{\oplus n}$ for some nonnegative n.

(b) Then G is algebraic (namely, finite type over k) if and only if $\mathrm{Rep}_k(G)$ equals $\langle X \rangle^{\otimes}$ for some object X.

Proof. See [DM12, Proposition 2.20]. ■

Proposition 11. Fix a field k of characteristic 0 and an affine k-group G. Then $G^{\circ} \subseteq G$ is a projective limit of reductive k-groups if and only if $\mathrm{Rep}_k(G)$ is semisimple.

Proof. See [DM12, Remark 2.28]. ■

Lastly, we will also want some functoriality. Approximately speaking, we expect surjections/injections of groups to correspond to "surjections/injections" of categories.

Proposition 12. Fix a morphism $f\colon G \to G'$ of affine k-groups G, and let $\omega\colon \mathrm{Rep}_k(G') \to \mathrm{Rep}_k(G)$ be the corresponding functor.

(a) Suppose $\mathrm{Rep}_k(G)$ is semisimple and that k has characteristic 0. Then f is faithfully flat if and only if the following holds: for given $X' \in \mathrm{Rep}_k(G')$, every subobject of $\omega(X')$ is isomorphic to $\omega(Y')$ for some subobject Y' of X'.

(b) Then f is a closed embedding if and only if every object $X \in \mathrm{Rep}_k(G)$ is isomorphic to a subquotient of $\omega(X')$ for some $X' \in \mathrm{Rep}_k(G')$.

Proof. Combine [DM12, Remark 2.29] with [DM12, Proposition 2.21]. ■

2.2 Review of Cohomology

In this subsection, we review various cohomology theories, approximately following [Del18, Section 1]. We begin by discussing what is expected from a cohomology theory.

Definition 13 (Weil cohomology)**.** Let $\mathcal{P}(k)$ denote the category of smooth proper k-varieties.

2.3 Hodge Structures

The previous subsection mentioned that the cohomology $H^\bullet(X,\mathbb{C})$ of a complex projective variety X admits a "Hodge structure" meaning that one has a decomposition

$$H^n(X,\mathbb{C}) \cong \bigoplus_{p+q=n} H^{p,q}$$

where $H^{p,q} = \overline{H^{q,p}}$. What is interesting about this situation is that we begin with a $\mathbb{Q}$-vector space $H^n(X,\mathbb{C})$, which then inherits the above decomposition only after base-change to $\mathbb{C}$. This structure is what makes our complex-analytic cohomology interesting, so we give it a name.

Definition 14 (Hodge structure)**.** A $\mathbb{Q}$-*Hodge structure* of weight $m \in \mathbb{Z}$ is a finite-dimensional vector space $V \in \mathrm{Vec}_{\mathbb{Q}}$ such that $V_{\mathbb{C}}$ admits a decomposition

$$V_{\mathbb{C}} = \bigoplus_{p+q=m} V_{\mathbb{C}}^{p,q}$$

where $V_{\mathbb{C}}^{p,q} = \overline{V_{\mathbb{C}}^{q,p}}$. We let $\mathrm{HS}_{\mathbb{Q}}$ denote the category of $\mathbb{Q}$-Hodge structures, where a morphism of Hodge structures is a linear map preserving the decomposition over $\mathbb{C}$.

Example 15. Give the Tate twist $\mathbb{Q}(1) = 2\pi i\mathbb{Q}$ a Hodge structure of weight -2 where $\mathbb{Q}(1)^{-1,-1} = \mathbb{Q}(1)$ is nonzero.

The category $\mathrm{HS}_{\mathbb{Q}}$ becomes a faithful rigid tensor abelian subcategory of $\mathrm{Vec}_{\mathbb{Q}}$, where the forgetful functor is able to act as a fiber functor. As such, so we expect $\mathrm{HS}_{\mathbb{Q}}$ should arise from representations of some group. Let's explain how this is done.

Notation 16 (Deligne torus)**.** Let $\mathbb{S} \coloneqq \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\,\mathbb{G}_{m,\mathbb{C}}$ denote the Deligne torus. We also let $w\colon \mathbb{G}_{m,\mathbb{R}} \to \mathbb{S}$ denote the *weight cocharacter* given by $w(r) \coloneqq r \in \mathbb{C}$ on $\mathbb{R}$-points.

Remark 17. One can realize $\mathbb{S}$ more concretely as

$$\mathbb{S}(R) = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathrm{GL}_2(R) : a^2 + b^2 \in R^\times \right\},$$

where R is an $\mathbb{R}$-algebra. Indeed, there is a ring isomorphism from $R \otimes_{\mathbb{R}} \mathbb{C}$ to $\left\{ \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] : a,b \in R \right\}$ by sending $1 \otimes 1 \mapsto \left[\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right]$ and $1 \otimes i \mapsto \left[\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right]$.

We now explain how a representation of $\mathbb{S}$ converts to a Hodge structure.

Lemma 18. Fix some $V \in \mathrm{Vec}_{\mathbb{Q}}$. Then a Hodge structure on V has equivalent data to a representation $h\colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}}$.

Proof. Remark 17 informs us that the character group $X^*(\mathbb{S})$ of group homomorphisms $\mathbb{S} \to \mathbb{G}_m$ is a rank-2 free $\mathbb{Z}$-module generated by $z\colon \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] \mapsto a + bi$ and $\overline{z}\colon \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] \mapsto a - bi$ on $\mathbb{C}$-points.[1] Without too many details, upon passing to the Hopf algebra, one is essentially looking for units in $\mathbb{R}\left[a, b, \left(a^2+b^2\right)^{-1}\right]$, of which there are not many. Note that there is a Galois action by $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on these two characters $\{z, \overline{z}\}$, given by swapping them. Let $\iota \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ denote complex conjugation, for brevity.

[1] Alternatively, note one has an isomorphism $(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C})^\times \cong \mathbb{C}^\times \times \mathbb{C}^\times$ by sending $(z,w) \mapsto z \otimes w$. Then these two characters are $(z,w) \mapsto z$ and $(z,w) \mapsto w$.

Now, a representation $h\colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}}$ must have $V_{\mathbb{C}}$ decompose into eigenspaces according to the characters $X^*(\mathbb{S})$, so one admits a decomposition

$$V_{\mathbb{C}} = \bigoplus_{\chi \in X^*(\mathbb{S})} V_{\mathbb{C}}^{\chi}.$$

However, one also needs $V_{\mathbb{C}}^{\iota\chi} = \overline{V_{\mathbb{C}}^{\chi}}$ because ι swaps $\{\chi, \iota\chi\}$. By Galois descent, this is enough data to (conversely) define a representation $h\colon \mathbb{S} \to \mathrm{Gal}(V)_{\mathbb{R}}$.

To relate the previous paragraph to Hodge structures, we recall that $X^*(\mathbb{S})$ is a rank-2 free $\mathbb{Z}$-module, so write $\chi_{p,q} \coloneqq z^{-p}\overline{z}^{-q}$ so that $\iota\chi_{p,q} = \chi_{q,p}$. Setting $V_{\mathbb{C}}^{p,q} \coloneqq V_{\mathbb{C}}^{\chi_{p,q}}$ now explains how to relate the previous paragraph to a Hodge structure, as desired. ■

Remark 19. The weight of a Hodge structure on some $V \in \mathrm{HS}_{\mathbb{Q}}$ can be read off of h as follows: note the weight cocharacter $h \circ w$ equals the $(-m)$th power map if and only if the weight is m.

Thus, we see that one has tensor products and duals of Hodge structures by tracking through the representation of h. For example, if $V \in \mathrm{HS}_{\mathbb{Q}}$ has $V^\vee$ inherit a Hodge structure by $(V^\vee)^{p,q} \coloneqq (V^{-p,-q})^\vee$. In particular, $\mathrm{HS}_{\mathbb{Q}}$ becomes Tannakian.

2.4 The Mumford–Tate Group

We are now ready to define the main character of the present subsection, which is the Mumford–Tate group.

Definition 20 (Mumford–Tate group)**.** For some $V \in \mathrm{HS}_{\mathbb{Q}}$, we define the *Mumford–Tate group* $\mathrm{MT}(V)$ as the smallest algebraic $\mathbb{Q}$-group containing the image of the corresponding representation $h\colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}}$.

Fix

Remark 21. Because $\mathbb{S}$ is connected, we see that h is also connected. Namely, $\mathrm{MT}(V)^\circ \subseteq \mathrm{MT}(V)$ will be an algebraic $\mathbb{Q}$-group containing the image of h if $\mathrm{MT}(V)$ does too, so equality is forced.

It will turn out that $\mathrm{MT}(V)$ is the algebraic group corresponding the full Tannakian subcategory $\langle V \rangle^{\otimes}$ of $\mathrm{HS}_{\mathbb{Q}}$. Unraveling the formalism, the key point is the following proposition.

Proposition 22. Fix $V \in \mathrm{HS}_{\mathbb{Q}}$. Suppose $T \in \mathrm{HS}_{\mathbb{Q}}$ can be written as

$$T = \bigoplus_{i=1}^{N} \left(V^{\otimes m_i} \otimes (V^\vee)^{\otimes n_i}\right)(p_i),$$

where $m_i, n_i \geq 0$ are nonnegative integers and $p_i \in \mathbb{Z}$. Then $W \subseteq T$ is a Hodge substructure if and only if the action of $\mathrm{MT}(V)$ on T stabilizes W.

Proof. For each vector space in $\mathrm{HS}_{\mathbb{Q}}$, we let $h_\bullet$ denote the corresponding representation. Quickly, note that h_T In the backwards direction, we note that $\mathrm{MT}(V)$ stabilizing W implies that $h(s)$ stabilizes $W_{\mathbb{R}}$ for any s. We can thus view $W_{\mathbb{R}} \subseteq T_{\mathbb{R}}$ as a subrepresentation of $\mathbb{S}$, so taking eigenspaces reveals that W can be given the structure of a Hodge substructure of T.

The converse will have to use the construction of T. Indeed, suppose that $W \subseteq T$ is a Hodge substructure, and let $M \subseteq \mathrm{GL}(V)$ be the smallest algebraic $\mathbb{Q}$-group stabilizing $W \subseteq T$. We would like to show that $\mathrm{MT}(V) \subseteq M$. By definition of $\mathrm{MT}(V)$, it is enough to show that h factors through $M_{\mathbb{R}}$, meaning we must show that $h(s)$ stabilizes W for each $s \in \mathbb{S}$. Well, $h(s)$ will act by characters on the eigenspaces $W_{\mathbb{C}}^{p,q} \subseteq W_{\mathbb{C}}$, so $h(s)$ does indeed stabilize W. ■

Corollary 23. Fix $V \in \mathrm{HS}_{\mathbb{Q}}$. Then $\mathrm{MT}(V)$ is the group corresponding to the Tannakian subcategory $\langle V \rangle^{\otimes}$ of $\mathrm{HS}_{\mathbb{Q}}$.

Proof. ∎

Proposition 24. The Mumford–Tate group of an abelian variety with CM is a torus.

Define the Hodge group via $\mathbb{U}$.

2.5 The Rank of a CM Type

Proposition 24 explains that the Mumford–Tate group of an abelian variety with CM is a torus, so it is a natural question to ask about the rank of this torus. In this subsection, we will discuss a little about what is known about this rank. Our exposition largely follows [Lan11, Section 6.1].

Throughout this subsection, A is an absolutely simple abelian variety defined over a number field with CM type (K, Φ). We let (K^*, Φ^*) denote the reflex field and reflex CM type and pick up the following definition.

Definition 25 (rank)**.** Fix a CM type (K, Φ). Then the *rank* $\mathrm{rank}(K, \Phi)$ of (K, Φ) is the $\mathbb{Q}$-dimension of the image of the map $\mathrm{T}_\Phi \colon K \to K^*$ given by

$$\mathrm{T}_\Phi(\alpha) \coloneqq \sum_{\varphi \in \Phi} \varphi(\alpha).$$

Remark 26. Notably, the rank does not change upon passing to a Galois closure L of $K/\mathbb{Q}$ because T_Φ will simply become $\mathrm{T}_\Phi \circ \mathrm{T}_{L/K}$, and field traces of number fields are surjective. In the event where $K/\mathbb{Q}$ is Galois with $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$, we note that the existence of a normal basis implies that

$$\mathrm{rank}(K, \Phi) = \dim_{\mathbb{Q}} \Phi\mathbb{Q}[G],$$

where we view Φ as an element of $\mathbb{Z}[G]$ given by the sum of its elements. Similarly, one can go down to $\mathrm{rank}_{\mathbb{Z}} \Phi\mathbb{Z}[G]$ and even multiply by Φ on either side.

Remark 27. Notably, because the discussion in Remark 26 is largely independent of L (except for requiring L/K to be Galois), we see that

$$\mathrm{rank}(K, \Phi) = \mathrm{rank}(L, \Phi_L) = \mathrm{rank}(K_0, \Phi_0)$$

where (L, Φ_L) is the extension of (K, Φ) to L, and (K_0, Φ_0) is the primitive CM type extending to (K, Φ).

Remark 28. Using Remark 26, we note that $\mathrm{rank}(K, \Phi) = \mathrm{rank}(K^*, \Phi^*)$ because, upon passing all ranks and types to a Galois closure, sending $\sigma \mapsto \sigma^{-1}$ will map $\Phi\mathbb{Q}[G]$ to $\mathbb{Q}[G]\Phi^*$, showing that the $\mathbb{Q}$-dimensions of these spaces are equal.

The importance of this definition is as follows.

Proposition 29. Fix an abelian variety A defined over a number field with CM type (K, Φ). Then

$$\dim \mathrm{MT}(A) = \mathrm{rank}(K, \Phi).$$

Proof. We follow the argument of [Yan94, Proposition 1.1].

1. To set up our discussion, we set some notation. Given a number field F, we set $T_F \coloneqq \operatorname{Res}_{F/\mathbb{Q}} \mathbb{G}_m$ and $X_F \coloneqq X^*(T_F)$; note that X_F is the free abelian group generated by the set $\Gamma_F \coloneqq \operatorname{Hom}(F, \mathbb{C})$. For example, the reflex norm $\mathrm{N}_{\Phi^*} \colon (K^*)^\times \to K^\times$ (note $K^{**} \subseteq K$) can actually be viewed as a map $\mathrm{N}_{\Phi^*} \colon T_{K^*} \to T_K$ of $\mathbb{Q}$-tori and hence induces a map $\mathrm{T}_{\Phi^*} \colon X_K \to X_{K^*}$ on character groups defined by

$$\mathrm{T}_{\Phi^*}(x) \coloneqq \sum_{\tau \in \Phi^*} x\tau = x\Phi^*.$$

   To properly understand the product τx (and ones similar to it in the following argument), one should extend all embeddings to $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but the above construction of T_{Φ^*} explains why the definition is independent of these choices of liftings.

2. With this notation in place, we take a moment to describe $\mathrm{MT}(A)$ in terms of these tori. By the proof of Proposition 24, we see that the Hodge structure $h \colon \mathbb{S} \to \mathrm{GL}\left(H^1_B(A; \mathbb{Q})\right)$ factors through T_K. In fact, by definition of the CM type (K, Φ), we see that

$$H^{10} \cong \bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi,$$

   so the Hodge structure h is given by the torus map $X^*(h) \colon X_K \to X^*(\mathbb{S})$ defined by

$$\varphi \mapsto \begin{cases} z^{-1} & \text{if } \varphi \in \Phi, \\ \overline{z}^{-1} & \text{if } \varphi \notin \Phi, \end{cases}$$

   where $z, \overline{z} \colon X^*(\mathbb{S})$ are the two characters of Lemma 18. (Namely, the map $X^*(h)$ is intended to provide an $\mathbb{S}$-action on $H^1_B(A; \mathbb{Q})$ from which the Hodge structure $H^{01} \oplus H^{10}$ upon base-changing to $\mathbb{C}$. But we already understand the decomposition via the eigenspaces of Γ_K!) Now, identifying $X^*(\mathbb{U})$ with $\mathbb{Z}$ via $z^{-1} \mapsto 1$, we see that $\mathrm{Hg}(A)$ is the smallest algebraic $\mathbb{Q}$-group containing the image of the torus map $\mathbb{U} \to T_K$ defined on characters by

$$\varphi \mapsto \begin{cases} +1 & \text{if } \varphi \in \Phi, \\ -1 & \text{if } \varphi \notin \Phi. \end{cases}$$

3. The main claim is that $x \in X_K$ is trivial on $\mathrm{Hg}(A)$ if and only if $\mathrm{T}_{\Phi^*}(x)$ is an integral multiple of

$$\theta \coloneqq \sum_{\tau \in \Gamma_{K^*}} \tau.$$

   To see how this claim completes the proof, we note that it implies that we may carry out the computation

$$\begin{aligned} \dim \mathrm{MT}(A) &= 1 + \dim \mathrm{Hg}(A) \\ &= 1 + \operatorname{rank}_{\mathbb{Z}} X^*(\mathrm{Hg}(A)) \\ &= 1 + \operatorname{rank}_{\mathbb{Z}} X_K - \operatorname{rank}_{\mathbb{Z}} \{x \in X_K : x|_{\mathrm{Hg}(A)} = 1\} \\ &= 1 + \operatorname{rank}_{\mathbb{Z}} X_K - \operatorname{rank}_{\mathbb{Z}} \mathrm{T}_{\Phi^*}^{-1}(\mathbb{Z}\theta) \\ &= \operatorname{rank}_{\mathbb{Z}} X_K - \operatorname{rank}_{\mathbb{Z}} \ker \mathrm{T}_{\Phi^*} \\ &= \operatorname{rank}_{\mathbb{Z}} \operatorname{im} \mathrm{T}_{\Phi^*} \\ &= \operatorname{rank}_{\mathbb{Z}} \mathbb{Z}[\Gamma_{K^*}]\Phi^*, \end{aligned}$$

   which is what we wanted upon comparing with Remarks 26 and 28.

4. It remains to show the main claim. To begin, note that $x = \sum_{\sigma \in \Gamma_K} n_\sigma \sigma$ is trivial on $\mathrm{Hg}(A)$ if and only if gx is trivial on $\operatorname{im} h|_{\mathbb{U}}$ for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. (Without the extra g, we would be trivial on the smallest $\overline{\mathbb{Q}}$-subgroup of T_K containing $\operatorname{im} h|_{\mathbb{U}}$, so we add in the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action to allow for our Galois descent to $\mathrm{Hg}(A)$.) Continuing, xg is trivial on $\operatorname{im} h|_{\mathbb{U}}$ if and only if $xg \circ h|_{\mathbb{U}}$ is trivial, which is equivalent to $X^*(h|_{\mathbb{U}})(gx)$ being trivial, which we can compute is equivalent to

$$\sum_{g\sigma \in \Phi} n_\sigma = \sum_{g\sigma \notin \Phi} n_\sigma.$$

Of course, we note that these sums being equal is equivalent to either of them being equal to $\frac{1}{2}\sum_\sigma n_\sigma$. On the other hand, setting $x = \sum_{\sigma \in \Gamma_K} n_\sigma \sigma$ allows us to compute $\mathrm{T}_{\Phi^*}(x)$ as

$$\mathrm{T}_{\Phi^*}(x) = \sum_{\substack{\tau \in \Phi^* \\ \sigma \in \Gamma_K}} n_\sigma \sigma\tau.$$

Now, we see that $\mathrm{T}_{\Phi^*}(x)$ is a multiple of θ if and only if the sum

$$\sum_{\substack{\tau \in \Phi^* \\ \sigma \in \Gamma_K \\ \sigma\tau = \mu}} n_\sigma$$

does not depend on $\mu \in \Gamma_{K^*}$.[2] However, we see

$$\sum_{\substack{\tau \in \Phi^* \\ \sigma \in \Gamma_K \\ \sigma\tau = \mu}} n_\sigma = \sum_{\substack{\tau \in \Phi^* \\ \sigma \in \Gamma_K \\ \mu^{-1}\sigma = \tau^{-1}}} n_\sigma = \sum_{\mu^{-1}\sigma \in \Phi} n_\sigma$$

having value of independent of μ means that the sum for μ^{-1} and $\iota\mu^{-1}$ have the same value, which we noted above is equivalent for this sum to equal $\frac{1}{2}\sum_\sigma n_\sigma$. A comparison with our discussion at the end of the previous paragraph completes the proof. ∎

The point is that we have achieved a combinatorial description of $\dim \mathrm{MT}(A)$. For example, if we are able to show that $\mathrm{rank}(K, \Phi) = \dim A + 1$, then we are able to conclude that $\mathrm{MT}(A)$ must be equal to the maximal torus inside $\mathrm{GSp}_{2\dim A}(\mathbb{Q})$.

Here are some quick bounds on the rank; for example, for large degrees, we expect the rank to be relatively large.

Proposition 30. Fix a CM type (K, Φ) which is an extension of the primitive CM type (K_0, Φ_0). Then

$$1 + \log_2[K_0 : \mathbb{Q}] \leq \mathrm{rank}(K, \Phi) \leq \frac{1}{2}[K_0 : \mathbb{Q}] + 1.$$

Proof. We follow [Lan11, Theorem 1.2]; we show the inequalities separately.

- For the right inequality, we may as well take $K = K_0$ by Remark 27. Letting K_0^+ be the totally real subfield of K_0, the main point is that

$$\mathrm{T}_{K/K^+} \circ \mathrm{T}_\Phi = \mathrm{T}_{K/\mathbb{Q}}$$

because (K, Φ) is a CM type. Thus, $\dim_{\mathbb{Q}} \mathrm{T}_{K/K^+}(T_\Phi(K)) = 1$, but $\mathrm{T}_{K/K^+} \colon K \to K^+$ is surjective with kernel of dimension $\frac{1}{2}[K : \mathbb{Q}]$, so the result follows.

[2] The equality $\sigma\tau = \mu$ is understood to be an equality of embeddings on K^*, despite our aforementioned convention that all these elements in fact live in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If one is concerned with rigor, feel free to pass all automorphisms up to a fixed Galois closure L of K over $\mathbb{Q}$ and replace all sums with sums over all possible extensions to automorphisms $L \to L$.

- For the left inequality, we may as well assume that $K/\mathbb{Q}$ is Galois by Remarks 26 and 27. Set $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$, and let $H \subseteq G$ consist of those automorphisms σ such that $\Phi\sigma = \Phi$; note H is the subgroup fixing K^*. By taking the reflex field (which is legal by Remark 28), it suffiees to show that

$$\dim_{\mathbb{F}_2} \Phi\mathbb{F}_2[G] \overset{?}{\geq} 1 + \log_2[K^* : \mathbb{Q}],$$

for which we will actually show

$$\#\Phi\mathbb{F}_2[G] \overset{?}{\geq} 2[K^* : \mathbb{Q}].$$

For this, we need to exhibit at least $2[K_0 : \mathbb{Q}] = 2 \cdot \#(H\backslash G)$ elements in $\#\Phi\mathbb{F}_2[G]$, so we choose the elements

$$\{\Phi\sigma : \sigma \in H\backslash G\} \sqcup \{\Phi + \Phi\sigma : \sigma \in H\backslash G\}.$$

It is enough to show that these elements are distinct in $\mathbb{F}_2[G]$. For example, $\Phi\sigma \equiv \Phi\sigma'$ would imply $\Phi\sigma'\sigma^{-1} \equiv \Phi$ and hence $\sigma'\sigma^{-1} \in H$ and hence $\sigma = \sigma'$ by definition of H. Similarly, one sees that the elements $\Phi + \Phi\sigma$ are pairwise distinct. Lastly, we see that we can never have $\Phi\sigma \equiv \Phi + \Phi\sigma'$ because this would imply

$$\Phi + \Phi\iota \equiv \Phi + \Phi\iota + \underbrace{\Phi\sigma' + \Phi\sigma'\iota}_{=\Phi+\Phi\iota} \equiv 0,$$

where ι denotes complex conjugation; this is a contradiction. ■

Example 31. If A is an absolutely simple abelian variety with CM type (K, Φ) of dimension $g \in \{1, 2, 3\}$, then the bounds of Proposition 30 imply $\mathrm{rank}(K, \Phi) = g + 1$.

It turns out that one can upgrade the argument in the left inequality as follows.

Proposition 32. Let (K_0, Φ_0) be a primitive CM type such that $[K_0 : \mathbb{Q}] = 2p$ for an odd prime p. Then $\mathrm{rank}(K_0, \Phi_0) = p + 1$.

Proof. We follow [Rib83, Theorem 2]. Let K be a Galois closure of K_0 over $\mathbb{Q}$, and set $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$. We are interested in computing $\dim_{\mathbb{Q}} \mathbb{Q}[G]\Phi$, so we note Proposition 30 immediately upper-bounds this dimension by $p + 1$. For the lower bound, we proceed in steps.

1. The key is to view $\mathbb{Q}[G]\Phi$ as a G-module where G acts on the left by multiplication. In particular, we claim that this map

$$G \to \mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}[G]\Phi$$

is injective: some $g \in G$ fixes $\mathbb{Q}[G]\Phi$ if and only if $g\sigma\Phi = \sigma\Phi$ for all $\sigma \in G$. However, this is equivalent to $\sigma^{-1}g\sigma\Phi = \Phi$, which we see is equivalent to $\sigma^{-1}g\sigma$ fixing K_0 for all σ! In other words, we need g to fix all embeddings of K_0 into K, so because K is a Galois closure of K_0, this is equivalent to g being the identity.

2. This injectivity gets us most of the way: choose some $g \in G$ of order p (which exists because $[K_0 : \mathbb{Q}]$ must divide the order of G), so we view $\mathbb{Q}[G]\Phi$ as a $\langle g \rangle$-representation, which produces an eigenspace decomposition

$$\mathbb{Q}[G] \cong A \oplus B,$$

where g acts on A nontrivially, and g acts on B nontrivially. Because g acts on $\mathbb{Q}[G]\Phi$ nontrivially, A is nonzero, so $\dim_{\mathbb{Q}} A \geq p - 1$.

3. It remains to show that $\dim_{\mathbb{Q}} B \geq 2$. Of course $\theta \coloneqq \sum_{\sigma \in G} \sigma$ is fixed by G, so the primary difficulty of the remainder of the proof is finding another vector fixed by g. It will turn out that $\left(1 + g + \cdots + g^{p-1}\right)\Phi$ will do the trick, but this is not obvious. Undoing the arguments of Proposition 24, we note that

$$\frac{\mathbb{Q}[G]\Phi}{\mathbb{Q}[G]\Phi \cap \mathbb{Q}\theta} = \frac{\mathrm{im}(\Phi\colon \mathbb{Q}[G] \to \mathbb{Q}[G])}{\mathbb{Q}[G]\Phi \cap \mathbb{Q}\theta} \cong \frac{\mathbb{Q}[G]}{\{x \in \mathbb{Q}[G] : x\Phi \in \mathbb{Q}\theta\}}.$$

Now, the arguments of Proposition 24 tell us that we have a well-defined map on this quotient defined by $\mathbb{Q}[G] \to \mathbb{Q}$ where $\sigma \mapsto 1$ if $\sigma \in \Phi$ and $\sigma \mapsto -1$ otherwise. As such, $\left(1 + g + \cdots + g^{p-1}\right)\Phi \notin \mathbb{Q}\theta$ because $1+g+\cdots+g^{p-1}$ is nonzero in the quotient above because it is nonzero under the aforementioned map $\mathbb{Q}[G] \to \mathbb{Q}$. (Importantly, here we have used the fact that p is odd!) ■

As a last example, we work with abelian extensions.

Lemma 33. Let (K, Φ) be a CM type such that $K/\mathbb{Q}$ is an abelian extension with Galois group G. Then $\operatorname{rank}(K, \Phi)$ equals the number of characters $\chi\colon G \to \mathbb{C}^\times$ such that $\chi(\Phi) \neq 0$.

Proof. We will compute $\operatorname{rank}(K, \Phi)$ as $\dim_{\mathbb{C}} \mathbb{C}[G]\Phi$. One can diagonalize the G-action on $\mathbb{C}[G]$ into

$$\mathbb{C}[G] \cong \bigoplus_{\chi} \mathbb{C}_\chi,$$

where G acts on $\mathbb{C}_\chi$ by χ. Thus, $\mathbb{Q}[G]\Phi$ will equal the sum of the spaces $\mathbb{C}_\chi\Phi$, but $\mathbb{C}_\chi\Phi$ is nonzero if and only if $\chi(\Phi) \neq 0$. ■

Remark 34. Work in the setting of Lemma 33. Let $\iota \in G$ denote complex conjugation. If χ is a nontrivial character satisfying $\chi(\iota) = 1$, then we see that

$$0 = \sum_{g \in G} \chi(g) = \chi(\Phi + \iota\Phi) = 2\chi(\Phi),$$

so $\chi(\Phi) = 0$.

Example 35. Fix a prime p, and define the CM type Φ on $\mathbb{Q}(\zeta_p)$ by $\Phi = \left\{\zeta_p \mapsto \zeta_p^i : 1 \leq i \leq \frac{p-1}{2}\right\}$. We will show that $\operatorname{rank}(\mathbb{Q}(\zeta_p), \Phi) = p$ by following [Kub65, Section 4]. We use Lemma 33. In view of Remark 34, it is enough to check that $\chi(\Phi) \neq 0$ for each of the $\frac{p-1}{2}$ characters χ satisfying $\chi(\iota) = -1$. By identifying $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $(\mathbb{Z}/p\mathbb{Z})^\times$, this reduces to computing sums of the form $\sum_{i=1}^{(p-1)/2} \chi(i)$ for characters χ satisfying $\chi(-1) = -1$. We relegate these computations to Lemma 36 below.

Lemma 36. Fix a character $\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ satisfying $\chi(-1) = -1$. Then

$$\sum_{i=1}^{(p-1)/2} \chi(i) \neq 0.$$

Proof. We follow [Kub65, Lemma 4.3]. For brevity, define $g \coloneqq \frac{p-1}{2}$. The key input is to use the class number formula for cyclotomic fields. Indeed, by combining [Was12, Proposition 4.1, Theorem 4.2, Corollary 4.4], we see that

$$A \coloneqq \sum_{i=1}^{g} i\chi(i)$$

is nonzero. We will transform this nonvanishing result into the required one. We begin by defining the family

of sums

$$\begin{aligned}
A_< &\coloneqq \sum_{i=1}^{g} i\chi(i), \\
A_> &\coloneqq \sum_{i=g+1}^{p-1} i\chi(i), \\
A_0 &\coloneqq \sum_{i=1}^{g} 2i\chi(2i), \\
A_1 &\coloneqq \sum_{i=1}^{g} (2i-1)\chi(2i-1), \\
B_< &\coloneqq \sum_{i=1}^{g} \chi(i), \\
B_1 &\coloneqq \sum_{i=1}^{g} \chi(2i-1).
\end{aligned}$$

To continue, we describe some relations between these sums.

- One has $A = A_< + A_> = A_0 + A_1$.
- Because $\chi(-1) = -1$, we can see that $A_> = A_< - pB_<$ by sending $i \mapsto (p-i)$ in the sum. Combining with the previous point, we see that $A = 2A_< - pB_<$.
- On the other hand, considering B_1, we send $i \mapsto (p-i)$ to make the terms even and then factor out a factor of 2 to show that $B_1 = -\chi(2)B_<$.
- Similarly, considering A_1, we send $i \mapsto (p-i)$ to make the terms even and then factor our a factor of 2 to show that $A_1 = 2\chi(2)A_< - p\chi(2)B_<$. Summing, we see $A = A_1 + A_2 = 4\chi(2)A_< - p\chi(2)B_<$.

In total, we are able to see that

$$4\chi(2)A_< - p\chi(2)B_< = A = 2\chi(2)A_< - p\chi(2)B_<$$

is a nonzero value. However, $B_< = 0$ combined with the equality of the left and right sides would require $A_< = 0$ and then $A = 0$, which is a contradiction, as required. ■

2.6 A Nondegenerate Jacobian

In this subsection, fix an odd prime p, and we study the Jacobian J_p of the $\mathbb{Q}$-curve $C_p \colon y^2 = x^p - 1$. The goal of the present subsection is to establish some basic facts about J_p. In particular, we will show that J_p is absolutely simple of dimension $\frac{p-1}{2}$ and $\operatorname{rank} J_p = \frac{p+1}{2}$.

A computation with the Riemann–Hurwitz formula (for general hyperelliptic curves) explains that the genus g of C_p is $\frac{p-1}{2}$, so we see $\dim J_p = \frac{p-1}{2}$. Note that $\langle \zeta_p \rangle$ acts on C_p by $\zeta_p \cdot (x, y) \coloneqq (\zeta_p x, y)$, so J_p has an endomorphism of order p, so $\mathbb{Z}[\zeta_p] \subseteq \operatorname{End} J_p$, so J_p has complex multiplication by $\mathbb{Q}(\zeta_p)$. Let's compute the CM type of J_p.

> **Remark 37.** If we were to work with $C_m \colon y^2 = x^m - 1$ for a general positive integer m, it still turns out that $J_m \coloneqq \operatorname{Jac} C_m$ admits complex multiplication, but it is no longer enough for $\mathbb{Q}(\zeta_m) \subseteq \operatorname{End}^0 J_m$ because $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ is less than $2 \dim J_m = m - 1$ when m fails to be prime.

Lemma 38. The CM type of J_p is given by $(\mathbb{Q}(\zeta_p), \Phi)$, where

$$\Phi \coloneqq \left\{ \zeta_p \mapsto \zeta_p^i : 1 \le i \le \frac{p-1}{2} \right\}.$$

Proof. We need to diagonalize the action of $\langle \zeta_p \rangle$ on $H^{10}(J_p) = H^0(J_p, \Omega^1_{J_p})$. It is a property of the Jacobian that

$$H^0(J_p, \Omega^1_{J_p}) \cong H^0(C_p, \Omega^1_{C_p}),$$

so we may diagonalize the action of $\langle \zeta_p \rangle$ on the space of differentials on C_p. Well, one can check that $C_p \colon y^2 = x^p - 1$ has a basis of differentials given by $x^i \, dx/y$ where $i \in \{0, \dots, \frac{p-3}{2}\}$; importantly, one ought to check that these differentials do not have poles at the points at infinity, which can be done by passing to the corresponding affine chart via $(x, y) \mapsto \left(1/u, v/u^{(p+1)/2}\right)$. Anyway, we conclude by noting that

$$\zeta_p \cdot \frac{x^i \, dx}{y} = \zeta_p^{i+1} \frac{x^i \, dx}{y},$$

so the given Φ does in fact describe the diagonalization of our action on H^{10}. ∎

Thus, Example 35 explains that $\dim \mathrm{MT}(A) = \mathrm{rank}(\mathbb{Q}(\zeta_p), \Phi) = p$, which forces $\mathrm{MT}(A) = \mathrm{Res}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} \mathbb{G}_m$.

Lastly, we check that J_p is absolutely simple. It is enough to check that the CM type $(\mathbb{Q}(\zeta_p), \Phi)$ is primitive.

Lemma 39. The CM type $(\mathbb{Q}(\zeta_p), \Phi)$ is primitive.

Proof. The CM type is primitive if and only if $\sigma\Phi = \Phi$ implies $\sigma = \mathrm{id}$ for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Denoting the $\mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p)$ defined by $\zeta_p \mapsto \zeta_p^i$ by σ_i, we see that we would like to show that $\sigma_i \Phi = \Phi$ implies $i = 1$. In other words, for any $i \neq 1$, we would like to show that

$$\left\{ ai \pmod p : 1 \le a \le \frac{p-1}{2} \right\} \neq \left\{ a \pmod p : 1 \le a \le \frac{p-1}{2} \right\}.$$

For this, we follow [Goo24, Lemma 4.2]. For $i > \frac{p-1}{2}$, we see that i lives in the left-hand set but not in the right-hand set, so there is nothing to do. Otherwise, $i \le \frac{p-1}{2}$, so $\frac{g-1}{2i} \le \frac{g-1}{i} + 1$, so we can find an integer j in the interval $\left(\frac{g-1}{2i}, \frac{g-1}{i}\right]$. But then $\frac{p-1}{2} < ij \le p-1$, so ij is in the left-hand set but not in the right-hand set. ∎

3 Basic Cases

In this subsection, we work out some basic cases.

Proposition 40. Fix an abelian variety A over a number field K with CM by E. Then Conjecture 1 holds for A.

Proof. The main point is that we are able to lift $\mathrm{Frob}_{\mathfrak{p}}$ to become an endomorphism of A.

Let $\mathcal{A}$ be the Néron model of A over $\mathcal{O}_{K_{\mathfrak{p}}}$, and let $\kappa \coloneqq \mathcal{O}_K/\mathfrak{p}$ be the residue field. The Néron mapping property implies $\mathrm{End}_E(A)^\circ = \mathrm{End}_E^\circ(\mathcal{A})$, which then has a natural reduction map to $\mathrm{End}_E^\circ(\mathcal{A}_\kappa)$. An argument on the Tate module tells us that

$$\mathrm{End}_E^\circ(A) \to \mathrm{End}_E^\circ(\mathcal{A}_\kappa)$$

is injective, but we see that both sides are free E-modules of rank 1. Thus, this reduction map is an isomorphism, so $\mathrm{Frob}_{\mathfrak{p}}$ lifts from an endomorphism on $\mathcal{A}_\kappa$ to an endomorphism on A.

We now note that the diagram

$$\begin{array}{ccc} H^1_B(A;\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell & \xrightarrow{H^1_B(F)} & H^1_B(A;\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \\ \downarrow & & \downarrow \\ H^1_{\text{ét}}(A;\mathbb{Q}_\ell) & \xrightarrow{\rho_\ell(\mathrm{Frob}_\mathfrak{p})} & H^1_{\text{ét}}(A;\mathbb{Q}_\ell) \end{array}$$

commutes by the functoriality of the applied comparison isomorphism (and the definition of F), so the result follows. Perhaps one should check that $H^1_B(F) \in G(A)$, but this follows because endomorphisms must preserve the Hodge structure, so F will send Hodge cycles to Hodge cycles (and thus send absolute Hodge cycles to absolute Hodge cycles). ■

Proposition 41. Fix an elliptic curve A over a number field. Then Conjecture 1 holds for A.

Proof. If A has complex multiplication, we are done by Proposition 40. This leaves us with two cases.

- Suppose $A_{\mathbb{C}}$ still has no complex multiplication. Then $\mathrm{MT}(A)$ is $\mathrm{GL}_{2,\mathbb{Q}}$, so the result follows from classical considerations.
- Suppose $A_{\mathbb{C}}$ is CM so that A has potential CM. For brevity, define $V \coloneqq H^1(A;\mathbb{Q})$. Note that A_L has CM for some quadratic extension L of K, so we produce a short exact sequence

  $$1 \to \mathrm{MT}(A) \to G(A) \to \mathrm{Gal}(L/K) \to 1.$$

  Note $\mathrm{MT}(A)$ is a torus, so $V_{\mathbb{C}}$ decomposes into two eigenspaces $V_{\mathbb{C}} = V^1_{\mathbb{C}} \oplus V^2_{\mathbb{C}}$; considering the rank of $\mathrm{MT}(A)$, we see that $\sigma \in \mathrm{MT}(A)$ if and only if $\sigma_{\mathbb{C}} \colon V_{\mathbb{C}} \to V_L$ sends $V^1_{\mathbb{C}}$ and $V^2_{\mathbb{C}}$ to themselves. Thus, choosing some $c \in G(A)$ to lift the generator of $\mathrm{Gal}(L/K)$, we see that c must normalize $\mathrm{MT}(A)$ while not actually living in $\mathrm{MT}(A)$, and the only way for this to happen is for $c_{\mathbb{C}}$ to swap $V^1_{\mathbb{C}}$ and $V^2_{\mathbb{C}}$ (possibly adding a scalar in the process to ensure that c is defined over $\mathbb{Q}$).

  This will be enough to complete the proof. Letting q be the cardinality of $\mathcal{O}_K/\mathfrak{p}$, we know that $\rho_\ell(\mathrm{Frob}_\mathfrak{p})$ is semisimple with characteristic polynomial $P_\mathfrak{p}(x) \in \mathbb{Q}[x]$ not depending on ℓ. The point is that the eigenvalues $\alpha_{1,\ell}$ and $\alpha_{2,\ell}$ of $\rho_\ell(\mathrm{Frob}_\mathfrak{p})$ on $V^1_{\mathbb{C}}$ and $V^2_{\mathbb{C}}$ may not be determined up to order, but the set of eigenvalues $\{\alpha_{1,\ell}, \alpha_{2,\ell}\}$ is independent of ℓ. Conjugation by c is able to swap the two eigenspaces, so we see that the conjugacy class of $\rho_\ell(\mathrm{Frob}_\mathfrak{p})$ is now independent of ℓ. ■

Remark 42. It may appear that one can upgrade this second proof to work for arbitrary abelian varieties with potential CM, but this is not the case. Indeed, the given proof only functions because $\mathrm{Gal}(L/K)$ acts simply transitively on the eigenspaces of $\mathrm{MT}(A)$ acting on $V_{\mathbb{C}}$. However, $G(A) \subseteq \mathrm{GSp}_{2\dim A}(\mathbb{Q})$, so one cannot hope for the normalizer of a torus to be large enough in general.