DETERMINING MONODROMY GROUPS OF ABELIAN VARIETIES

DAVID ZYWINA

ABSTRACT. Associated to an abelian variety over a number field are several interesting and related groups: the motivic Galois group, the Mumford–Tate group, ℓ-adic monodromy groups, and the Sato–Tate group. Assuming the Mumford–Tate conjecture, we show that from two well chosen Frobenius polynomials of our abelian variety, we can recover the identity component of these groups (or at least an inner form), up to isomorphism, along with their natural representations. We also obtain a practical probabilistic algorithm to compute these groups by considering more and more Frobenius polynomials; the groups are connected and reductive and thus can be expressed in terms of root datum. These groups are conjecturally linked with algebraic cycles and in particular we obtain a probabilistic algorithm to compute the dimension of the Hodge classes of our abelian variety for any fixed degree.

1. INTRODUCTION

Throughout we fix a nonzero abelian variety A of dimension g defined over a number field K. Fix an embedding $K \subseteq \mathbb{C}$. Let $\bar{K}$ be the algebraic closure of K in $\mathbb{C}$ and define $\mathrm{Gal}_K := \mathrm{Gal}(\bar{K}/K)$. Define the homology group $V_A := H_1(A(\mathbb{C}), \mathbb{Q})$, where $A(\mathbb{C})$ is viewed with the usual analytic topology.

We now describe several of the algebraic groups we are interested in computing. We denote by G_A the **motivic Galois group** of A with respect to the category of motives in the sense of André [And96]; the article [CFC19] gives a nice overview of the relevant groups and their connections. We can view G_A as an algebraic subgroup of GL_{V_A} since each $H^i(A(\mathbb{C}), \mathbb{Q})$ is naturally isomorphic to the i-th exterior power of the dual of V_A; for a definition of GL_{V_A} see §1.10. The **Mumford–Tate group** $\mathrm{MT}_A \subseteq \mathrm{GL}_{V_A}$ of A, which is defined in §4.1 using the Hodge decomposition of $H_1(A(\mathbb{C}), \mathbb{C})$, agrees with the identity component G_A° of G_A, cf. [CFC19, p. 4].

Now take any rational prime ℓ. Let $V_\ell(A)$ be the ℓ-adic Tate module; it is a $2g$-dimensional $\mathbb{Q}_\ell$-vector space with an action of Gal_K which is discussed in §3.1. We express this Galois action in terms of a continuous representation

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

The **ℓ-adic monodromy group** of A is the Zariski closure $G_{A,\ell}$ of the image of $\rho_{A,\ell}$ in $\mathrm{GL}_{V_\ell(A)}$; it is an algebraic group defined over $\mathbb{Q}_\ell$. Using the comparison isomorphism $V_\ell(A) = V_A \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, we can view $G_{A,\ell}$ as a subgroup of $(\mathrm{GL}_{V_A})_{\mathbb{Q}_\ell}$. Moreover, we always have an inclusion $G_{A,\ell} \subseteq (G_A)_{\mathbb{Q}_\ell}$ from Artin's comparison theorem, cf. [CFC19, p. 2]. The **Mumford–Tate conjecture** for A says that in fact $G_{A,\ell} = (G_A)_{\mathbb{Q}_\ell}$; the original Mumford–Tate conjecture (Conjecture 4.3) only predicts that $G_{A,\ell}^\circ$ and $(G_A)_{\mathbb{Q}_\ell}^\circ = (\mathrm{MT}_A)_{\mathbb{Q}_\ell}$ agree, but these two formulations are equivalent by the main theorem of [CFC19].

Take any nonzero prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ for which A has good reduction. If $\mathfrak{p} \nmid \ell$, then $\rho_{A,\ell}$ is unramified at $\mathfrak{p}$ and we have

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

---

where $P_{A,\mathfrak{p}}(x)$ is the **Frobenius polynomial** of A at $\mathfrak{p}$. The polynomial $P_{A,\mathfrak{p}}(x)$ is monic of degree $2g$ with integer coefficients and does not depend on ℓ. In practice, these polynomials are computable when A is given explicitly.

There is a stronger conjectural version of this Frobenius compatibility. Fix any prime ℓ satisfying $\mathfrak{p} \nmid \ell$ and choose any embedding $\iota \colon \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$. Then by using ι, we may identify $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \in G_A(\overline{\mathbb{Q}}_\ell)$ with an element of $G_A(\mathbb{C})$. It is conjectured that the conjugacy class of $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ in $G_A(\mathbb{C})$ does not depend on the initial choice of prime ℓ or embedding ι. We will make use of a weaker version of this conjecture, cf. Conjecture 4.5.

Let $K_A^{\mathrm{conn}} \subseteq \overline{K}$ be the minimal extension of K for which the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}(\overline{K}/K_A^{\mathrm{conn}}))$ is $G_{A,\ell}^\circ$. The extension K_A^{conn}/K does not depend on ℓ and its degree can be bounded in terms of g, cf. Proposition 3.2. The reader is encouraged to focus on the case where $K_A^{\mathrm{conn}} = K$ since this assumption does not change the strength of the theorems and the group G_A is then connected as well, cf. [CFC19, p. 4].

The group $G_A^\circ = \mathrm{MT}_A$ is reductive. So in particular, the base extension of G_A° to $\overline{\mathbb{Q}}$ will be completely determined by its **root datum**. For some background on reductive groups and root data, see §2. Fix a maximal torus T of G_A° that is defined over $\mathbb{Q}$. The root datum $\Psi(G_A^\circ, T)$ of G_A° with respect to T consists of the group $X(T)$ of characters $T_{\overline{\mathbb{Q}}} \to (\mathbb{G}_m)_{\overline{\mathbb{Q}}}$, a finite set of **roots**, along with the group of cocharacters and coroots that satisfy certain conditions. The action of $\mathrm{Gal}_{\mathbb{Q}}$ on $X(T)$ induces an action on $\Psi(G_A^\circ, T)$. Suppressing the choice of torus T, we obtain an abstract root datum $\Psi(G_A^\circ)$, that is uniquely determined up to an automorphism from its Weyl group, with a homomorphism

$$\mu_{G_A^\circ} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(G_A^\circ))$$

arising from the Galois action. The representation V_A of G_A° also gives rise to a set of weights in $X(T)$ with multiplicities.

Our main result says that the root datum of G_A° and the homomorphism $\mu_{G_A^\circ}$ can be recovered from the Frobenius polynomials $P_{A,\mathfrak{p}}(x)$ of two "random" primes $\mathfrak{p}$ that split completely in K_A^{conn}.

Theorem 1.1. *Assume that Conjectures 4.3 and 4.5 hold for A. Then for almost all prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_K$ that split completely in K_A^{conn}, the polynomials $P_{A,\mathfrak{q}}(x)$ and $P_{A,\mathfrak{p}}(x)$ determine the following:*

- *the root datum $\Psi(G_A^\circ)$ up to isomorphism,*
- *the homomorphism $\mu_{G_A^\circ} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(G_A^\circ))$,*
- *the set of weights of the representation $G_A^\circ \subseteq \mathrm{GL}_{V_A}$ and their multiplicities.*

By "almost all", we mean that the above holds with $\mathfrak{q} \notin S$ and $\mathfrak{p} \notin S'$, where S and S' are sets of prime ideals of $\mathcal{O}_K$ of density 0 with the second set S' depending on $\mathfrak{q}$.

Remark 1.2.

(i) The root datum $\Psi(G_A^\circ)$ and the homomorphism $\mu_{G_A^\circ}$ do not determine the group G_A°, but they do characterize G_A^0 up to an inner form. In the proof, it will be convenient to work with the *quasi-split inner form* of G_A°.

(ii) Mark Kisin and Rong Zhou have recently announced a proof of Conjecture 4.5 for primes not dividing 2. Once their work is available, it will make Theorem 1.1 and our other results conditional only on the Mumford–Tate conjecture for A (Conjecture 4.3).

By considering the Frobenius polynomial $P_{A,\mathfrak{p}}(x)$ for two "random" primes $\mathfrak{p}$ that split completely in K_A^{conn}, we can also recover the ℓ-adic monodromy group $G_{A,\ell}^\circ$ and its representation $V_\ell(A)$, up to isomorphism, for all but finitely many ℓ.

Corollary 1.3. *Assume that Conjectures 4.3 and 4.5 hold for A. Let S be the (finite) set of primes ℓ for which $(G_A^\circ)_{\mathbb{Q}_\ell}$ is not quasi-split. Then for almost all prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_K$ that*

split completely in $\mathsf{K}_A^{\mathrm{conn}}$, *the polynomials* $\mathsf{P}_{A,\mathfrak{q}}(x)$ *and* $\mathsf{P}_{A,\mathfrak{p}}(x)$ *determine the group* $\mathsf{G}_{A,\ell}^{\circ}$ *and the representation* $\mathsf{V}_{\ell}(A)$ *of* $\mathsf{G}_{A,\ell}^{\circ}$ *up to isomorphism for all* $\ell \notin \mathsf{S}$.

Proof. From Theorem 1.1, we may assume that we know the root datum $\Psi(\mathsf{G}_A^{\circ})$, the homomorphism $\mu_{\mathsf{G}_A^{\circ}}$, and the weights of $\mathsf{G}_A^{\circ} \subseteq \mathrm{GL}_{\mathsf{V}_A}$ with multiplicities. Take any prime $\ell \notin \mathsf{S}$ and set $\mathsf{G} := (\mathsf{G}_A^{\circ})_{\overline{\mathbb{Q}}_\ell} = \mathsf{G}_{A,\ell}^{\circ}$, where the equality uses the Mumford–Tate conjecture assumption.

By choosing an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, we obtain the root datum $\Psi(\mathsf{G})$ and the associated homomorphism $\mu_{\mathsf{G}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathrm{Out}(\Psi(\mathsf{G}))$. Since G is quasi-split, this information determines the algebraic group $\mathsf{G} = \mathsf{G}_{A,\ell}^{\circ}$ up to isomorphism, cf. §2.9. Since we know the weights of the representation $(\mathsf{G}_A^{\circ})_{\mathbb{Q}_\ell} = \mathsf{G}_{A,\ell}^{\circ}$ on $\mathsf{V}_A \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathsf{V}_{\ell}(A)$ with multiplicities, we also have enough information to determine the representation $\mathsf{V}_{\ell}(A)$ of $\mathsf{G}_{A,\ell}^{\circ}$ up to isomorphism. Finally, the set S is finite, cf. Theorem 6.7 of [PR94]. $\qquad\square$

In §1.6, we will observe that given the polynomials $\mathsf{P}_{A,\mathfrak{p}}(x)$ and $\mathsf{P}_{A,\mathfrak{q}}(x)$ for appropriate prime ideals $\mathfrak{q}$ and $\mathfrak{p}$, the root datum with Galois action and weights as in Theorem 1.1 can be explicitly computed.

By choosing prime ideals "randomly", this will give a probabilistic algorithm to compute the information from Theorem 1.1; we can view it as a Monte Carlo algorithm where the probability that an incorrect result is returned decays exponentially in the number of primes considered.

In order to prove Theorem 1.1, it is easy to reduce to the case where $\mathsf{K}_A^{\mathrm{conn}} = \mathsf{K}$ (by replacing A by its base extension by $\mathsf{K}_A^{\mathrm{conn}}$). We do not want to impose this condition since our algorithm does not require knowledge of the field $\mathsf{K}_A^{\mathrm{conn}}$.

1.1. **Galois groups of Frobenius polynomials.** We now describe the Galois group of the Frobenius polynomial for almost all $\mathfrak{p}$ that split completely in $\mathsf{K}_A^{\mathrm{conn}}$; this will be a key ingredient in our proof of Theorem 1.1 and is of independent interest. Let $\mathcal{W}_{A,\mathfrak{p}} \subseteq \overline{\mathbb{Q}}$ be the set of roots of $\mathsf{P}_{A,\mathfrak{p}}(x)$.

Let us first define the groups that will generically occur as Galois groups. Let $W(\mathsf{G}_A^{\circ})$ be the Weyl group of G_A°. Let $\Gamma(\mathsf{G}_A^{\circ}) \subseteq \mathrm{Aut}(\Psi(\mathsf{G}_A^{\circ}))$ be the group containing $W(\mathsf{G}_A^{\circ})$ whose image in $\mathrm{Out}(\Psi(\mathsf{G}_A^{\circ})) = \mathrm{Aut}(\Psi(\mathsf{G}_A^{\circ}))/W(\mathsf{G}_A^{\circ})$ agrees with the image of $\mu_{\mathsf{G}_A^{\circ}}$. Let k be the fixed field in $\overline{\mathbb{Q}}$ of the kernel of $\mu_{\mathsf{G}_A^{\circ}}$.

Theorem 1.4. *Assume that Conjectures 4.3 and 4.5 hold for A. Fix a number field $\mathsf{k} \subseteq \mathsf{L} \subseteq \overline{\mathbb{Q}}$. There is a set S of prime ideals of $\mathcal{O}_{\mathsf{K}}$ with density 0 such that for all nonzero prime ideals $\mathfrak{p} \notin \mathsf{S}$ of $\mathcal{O}_{\mathsf{K}}$ that split completely in $\mathsf{K}_A^{\mathrm{conn}}$, we have*

$$\mathrm{Gal}(\mathsf{L}(\mathcal{W}_{A,\mathfrak{p}})/\mathsf{L}) \cong W(\mathsf{G}_A^{\circ}) \quad and \quad \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q}) \cong \Gamma(\mathsf{G}_A^{\circ}).$$

Remark 1.5. A variant of Theorem 1.4 has been proved by the author in the special case where A is geometrically simple but without assuming Conjecture 4.5, cf. Theorem 1.5 of [Zyw14]. Conjecture 4.5 makes it much easier to identify $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q})$ with a subgroup of $\Gamma(\mathsf{G}_A^{\circ})$.

1.2. **Sato–Tate groups.** The motivic Galois group G_A comes with a character to $(\mathbb{G}_m)_{\mathbb{Q}}$ arising from the weight structure on the category of motives; its kernel we denote by G_A^1. The neutral component of G_A^1 agrees with the Hodge group Hg_A of A which is defined in §4.1

We define the Sato–Tate group of A to be a maximal compact subgroup ST_A of $\mathsf{G}_A^1(\mathbb{C})$ with respect to the analytic topology; it is a compact Lie group that is unique up to conjugation in $\mathsf{G}_A^1(\mathbb{C})$. The identity component ST_A° of ST_A is a maximal compact subgroup of $\mathrm{Hg}_A(\mathbb{C})$.

By considering the Frobenius polynomial of two "random" primes ideals that split completely in $\mathsf{K}_A^{\mathrm{conn}}$, we can also recover ST_A°; it will be a straightforward consequence of Theorem 1.1.

Theorem 1.6. *Assume that Conjectures 4.3 and 4.5 hold for A. Then for almost all prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_{\mathsf{K}}$ that split completely in $\mathsf{K}_A^{\mathrm{conn}}$, the polynomials $\mathsf{P}_{A,\mathfrak{q}}(x)$ and $\mathsf{P}_{A,\mathfrak{p}}(x)$ determine the root datum of Hg_A along with the weights and multiplicities of the action of Hg_A on V_A. In particular,*

such polynomials determine the Lie group ST_A° *and the representation* $V_A \otimes_{\mathbb{Q}} \mathbb{C}$ *of* ST_A° *up to isomorphism.*

For context, we now recall the Sato–Tate conjecture, cf. §13 of [Ser94]. Fix a rational prime ℓ and an embedding $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. Take any nonzero prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which A has good reduction. Using the embedding ι, we may view $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ as a (semisimple) element of $G_A(\mathbb{C})$ and $g_{\mathfrak{p},\ell} := \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})/\sqrt{\mathrm{N}(\mathfrak{p})}$ as an element of $G_A^1(\mathbb{C})$. From Weil, we know that the complex roots of $P_{A,\mathfrak{p}}(x)$ all have absolute value $\sqrt{\mathrm{N}(\mathfrak{p})}$ and hence the eigenvalues of $g_{\mathfrak{p},\ell}$ all have absolute value 1. So there is an element $\vartheta_\mathfrak{p} \in \mathrm{ST}_A$, unique up to conjugacy in ST_A, such that $g_{\mathfrak{p},\ell}$ and $\vartheta_\mathfrak{p}$ are conjugate in $G_A^1(\mathbb{C})$.

Conjecture 1.7 (Sato–Tate). *The elements* $\{\vartheta_\mathfrak{p}\}_\mathfrak{p}$ *are equidistributed in the conjugacy classes of* ST_A *with respect to the Haar measure. Equivalently, for any continuous central function* $f\colon \mathrm{ST}_A \to \mathbb{C}$, *we have*

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

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

Remark 1.8.

    (i) As noted earlier, it is conjectured that the conjugacy class of $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ in $G_A(\mathbb{C})$ does not depend on the choice of ℓ and ι. This conjecture would imply that the conjugacy class of $\vartheta_\mathfrak{p}$ in ST_A does not depend on the choice of ℓ and ι.

    (ii) Fix a prime ℓ and an embedding $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. A common alternate definition of the Sato–Tate group is a maximal compact subgroup of $G_{A,\ell}(\mathbb{C})$, where we have used our embedding ι. The Mumford–Tate conjecture would imply that this definition agrees with ours (and is independent of the choice of ℓ and ι). Moreover, one can show that Conjecture 1.7 as stated implies the Mumford–Tate conjecture for A.

For integrals of the form $\int_{\mathrm{ST}_A^\circ} f \, d\mu$ with a central continuous $f\colon \mathrm{ST}_A^\circ \to \mathbb{C}$, Weyl's integration formula reduces it to an integral over a maximal torus of ST_A°. In §1.3, we gives some simple examples of such integrals that are computable when one knows the root datum of Hg_A and the weights of its action on V_A (which is information of Hg_A that can be computed using the algorithm of §1.6).

Remark 1.9. There has been a lot of recent progress computing Sato–Tate groups ST_A. In [FKRS12], Fité, Kedlaya, Rotger and Sutherland have classified all the possible Sato–Tate groups that arise for abelian surfaces. Fité, Kedlaya and Sutherland have also proved a classification for abelian threefolds, cf. [FKS19]. In particular, they find that there are 433 possible Sato–Tate groups of abelian threefolds up to conjugacy in $\mathrm{USp}(6)$; of these 14 are connected. While our algorithm will only give the identity component of ST_A, it has the benefit that it does not require a classification and hence can be used in higher dimensions where a classification is infeasible.

There has also been much working on computing Sato–Tate groups of various Jacobians with complex multiplication, for example see [FS14], [FS16], [FLGS18], [EG20]; these are particularly interesting because the group $\mathrm{ST}_A / \mathrm{ST}_A^\circ$ can be relatively large.

1.3. **Dimension of Hodge classes.** For an integer $n \geqslant 0$, the n-th cohomology group $H^n(A(\mathbb{C}), \mathbb{Q})$ has a Hodge structure of weight n which gives a decomposition

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

The cohomology class $\mathrm{cl}(Z) \in H^{2p}(A(\mathbb{C}), \mathbb{C})$ of an algebraic subvariety Z of $A_{\mathbb{C}}$ of codimension p lies in the $\mathbb{Q}$-vector space

$$\mathcal{H}^p(A) := H^{2p}(A(\mathbb{C}), \mathbb{Q}) \cap H^{p,p}(A)$$

of Hodge classes. The renowned Hodge conjecture for A predicts that for each integer $0 \leqslant p \leqslant g$, the cohomology classes $\mathrm{cl}(Z)$ of algebraic subvarieties of $A_{\mathbb{C}}$ with codimension p span the $\mathbb{Q}$-vector space $\mathcal{H}^p(A)$.

We are particularly interested in computing the dimension of the vector spaces $\mathcal{H}^p(A)$ since the Hodge conjecture will sometimes predict the existence of exceptional algebraic cycles. The following lemma shows that $\dim_{\mathbb{Q}} \mathcal{H}^p(A)$ is determined by the action of Hg_A on V_A. By using the techniques of §1.6, we can then make predictions for $\dim_{\mathbb{Q}} \mathcal{H}^p(A)$ by considering just a few Frobenius polynomials.

For integers $n \geqslant 0$ and $0 \leqslant k \leqslant 2g$, the representation V_A of GL_{V_A} gives rise to another representation $(\bigwedge^k V_A)^{\otimes n}$. We define $M_{k,n}$ to be the dimension of the subspace of $(\bigwedge^k V_A)^{\otimes n}$ fixed by Hg_A.

Lemma 1.10. *For each integer $0 \leqslant p \leqslant g$, we have $\dim_{\mathbb{Q}} \mathcal{H}^p(A) = M_{2p,1}$.*

Proof. There is a natural isomorphism of Hodge structures $V_0 := H^{2p}(A(\mathbb{C}), \mathbb{Q}) = \mathrm{Hom}(\bigwedge^{2p} V_A, \mathbb{Q})$. We have $\mathcal{H}^p(A) = V_0^{\mathrm{Hg}_A}$ by Theorem 17.3.3 of [BL04], so the dimension of $\mathcal{H}^p(A)$ is equal to $\dim_{\mathbb{Q}} V_0^{\mathrm{Hg}_A} = \dim_{\mathbb{Q}} (\bigwedge^{2p} V_A)^{\mathrm{Hg}_A} = M_{2p,1}$. $\qquad\square$

For $B \in \mathrm{GL}_{V_A}(\mathbb{C})$, denote its characteristic polynomial by $\sum_{k=0}^{2g} (-1)^k a_k(B) x^k$. The trace of the action of B on $(\bigwedge^k V_A)^{\otimes n}$ is $a_k(B)^n$. Since ST_A° is a maximal compact subgroup of $\mathrm{Hg}_A(\mathbb{C})$, $M_{k,n}$ is also the dimension of the subspace of $(\bigwedge^k V_A)^{\otimes n} \otimes_{\mathbb{Q}} \mathbb{C}$ fixed by ST_A°. Therefore,

$$M_{k,n} = \int_{\mathrm{ST}_A^\circ} a_k^n \, d\mu,$$

where μ is the Haar measure on ST_A° satisfying $\mu(\mathrm{ST}_A^\circ) = 1$.

We now explain how to compute the values $M_{k,n}$ which by Lemma 1.10 allows us to compute the dimension of Hodge classes. We suppose that the root datum $\Psi(\mathrm{Hg}_A)$ of Hg_A is known; it comes with a character group X, a finite set of roots $R \subseteq X$, and there is a Weyl group W that acts faithfully on X. Further suppose we also know the weights $\alpha_1, \cdots, \alpha_{2g} \in X$ of the representation V_A of Hg_A stated with multiplicity.

We can identify X with $X(T)$ for a maximal torus T of Hg_A. Let T_0 be the maximal compact subgroup of $T(\mathbb{C})$. Weyl's integration formula implies that

$$M_{k,n} = \frac{1}{|W|} \int_{T_0} a_k(t)^n \prod_{\alpha \in R} (1 - \alpha(t)) \, dt,$$

where dt is the Haar measure on T_0 normalized to have volume 1. Fix a basis $\beta_1, \ldots, \beta_m$ of the free abelian group X. For $\alpha \in X$, we have $\alpha = \prod_{i=1}^m \beta_i^{e_i(\alpha)}$ for unique $e_i(\alpha) \in \mathbb{Z}$. So there is an isomorphism of Lie groups $T_0 \to U(1)^m$, $t \mapsto (\beta_1(t), \ldots, \beta_m(t))$, where $U(1)$ is the unit circle in $\mathbb{C}^\times$. We have $a_k(t) = \sum_{J \subseteq \{1, \ldots, 2g\}, |J|=k} \prod_{j \in J} \alpha_j(t)$ and hence

$$M_{k,n} = \frac{1}{|W|} \int_{U(1)^m} \left(\sum_{J \subseteq \{1, \ldots, 2g\}, |J|=k} \prod_{j \in J} \prod_{i=1}^m t_i^{e_i(\alpha_j)} \right)^n \cdot \prod_{\alpha \in R} \left(1 - \prod_{i=1}^m t_i^{e_i(\alpha)} \right) dt_1 \cdots dt_m,$$

where dt_i is the Haar measure on $U(1)$ with volume 1. Such integrals are readily computable by expanding out and using that for an integer $b \in \mathbb{Z}$, the integral $\int_{U(1)} t_i^b \, dt_i$ is 1 if $b = 0$ and is 0 otherwise.

Remark 1.11. By Proposition 1 of [CFS19], $M_{1,2}$ is the rank of the group $\operatorname{End}(A_{\overline{K}})$. By Proposition 2 of [CFS19], $M_{2,1}$ is the rank of the Néron–Severi group $\operatorname{NS}(A_{\overline{K}})$.

1.4. **Endomorphism ring.** In this section, we describe how to compute some partial information for the ring $\operatorname{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$. We have an isomorphism

$$\operatorname{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_1 \times \cdots \times B_s,$$

where B_i is a central simple algebra over a number field L_i. For each $1 \leqslant i \leqslant s$, let m_i be the positive integer satisfying $\dim_{L_i} B_i = m_i^2$.

Theorem 1.12. *Assume that Conjectures 4.3 and 4.5 hold for A. Then for almost all prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_K$ that split completely in K_A^{conn}, the polynomials $P_{A,\mathfrak{q}}(x)$ and $P_{A,\mathfrak{p}}(x)$ determine the pairs $(L_1, m_1), \ldots, (L_s, m_s)$ up to reordering and replacing the L_i by isomorphic number fields.*

We now explain how the pairs (L_i, m_i) can be obtained from the root datum $\Psi(G_A^\circ)$ with its Galois action and the weights. We may assume that our root datum is $\Psi(G_A^\circ, T)$ for some maximal torus T of G_A°. Let $\Omega \subseteq X(T)$ be the weights of the representation V_A. Let $\Gamma := \Gamma(G_A^\circ, T)$ be the subgroup of $\operatorname{Aut}(\Psi(G_A^\circ, T)) \subseteq \operatorname{Aut}(X(T))$ containing the Weyl group $W := W(G_A^\circ, T)$ and whose image in $\operatorname{Out}(\Psi(G_A^\circ)) = \operatorname{Aut}(\Psi(G_A^\circ, T))/W$ agrees with the image of $\mu_{G_A^\circ}$. Let k be the fixed field in $\overline{\mathbb{Q}}$ of the kernel of $\mu_{G_A^\circ}$; we have a natural isomorphism $\operatorname{Gal}(k/\mathbb{Q}) = \Gamma/W$.

Let $\Omega_1, \ldots, \Omega_{s'}$ be the Γ-orbits of Ω. For each $1 \leqslant i \leqslant s'$, choose a W-orbit $\mathcal{O}_i \subseteq \Omega_i$. Let H_i be the group of $\sigma \in \Gamma$ for which $\sigma(\mathcal{O}_i) = \mathcal{O}_i$. Using the isomorphism $\Gamma/W = \operatorname{Gal}(k/\mathbb{Q})$, let L_i' be the subfield of k fixed by H_i/W. Let m_i' be the multiplicity of any weight in $\mathcal{O}_i$; this is well-defined since the W-action preserves multiplicities.

Theorem 1.12 is an immediate consequence of Theorem 1.1 and the following proposition which we will prove in §10.

Proposition 1.13. *We have $s' = s$ and after reordering the Γ-orbits of Ω, we have $m_i' = m_i$ and $L_i' \cong L_i$ for all $1 \leqslant i \leqslant s$.*

Remark 1.14.
  (i) When A is isogenous over $\overline{K}$ to a power of a simple abelian variety, Theorem 1.12 is also a consequence of a theorem of Costa, Lombardo and Voight [CLV19] which uses a weaker version of Theorem 1.4.
  (ii) In general, one cannot recover the structure of $\operatorname{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ from the Frobenius polynomials of two "random" prime ideals that split completely in K_A^{conn}. Since this ring is isomorphic to the subring of $\operatorname{End}(V_A)$ that commutes with the MT_A-action, this also means that we cannot always recover $\operatorname{MT}_A = G_A^\circ$, up to isomorphism, with the setup of Theorem 1.1.

  For example, consider an abelian variety A/K satisfying $K_A^{\mathrm{conn}} = K$ that is either the square of a non-CM elliptic curve or is a QM surface (i.e., its endomorphism ring is an indefinite quaternion algebra). For all primes ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ away from a set of density 0, one can show that $P_{A,\mathfrak{p}}(x) = Q_{\mathfrak{p}}(x)^2$ for an irreducible quadratic $Q_{\mathfrak{p}}(x) \in \mathbb{Z}[x]$. Moreover, the splitting fields of $Q_{\mathfrak{q}}(x)$ and $Q_{\mathfrak{p}}(x)$ will be linearly disjoint over $\mathbb{Q}$ for almost all $\mathfrak{q}$ and $\mathfrak{p}$. So from a few Frobenius polynomials, we are unable to determine the structure of $\operatorname{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$, but we can say that it is a central simple algebra over $\mathbb{Q}$ and $\dim_{\mathbb{Q}}(\operatorname{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}) = 2^2$.

1.5. **Overview of the proof of Theorem 1.1.** We now give an overview of the constructions underlying Theorem 1.1. Throughout, we assume that Conjectures 4.3 and 4.5 for A hold.

Let G be a quasi-split inner form of $G_A^\circ = \operatorname{MT}_A$, cf. §2.9. In particular, there is an isomorphism $f \colon G_{\overline{\mathbb{Q}}} \xrightarrow{\sim} (G_A^\circ)_{\overline{\mathbb{Q}}}$ such that $f^{-1} \circ \sigma(f)$ is an inner automorphism of $G_{\overline{\mathbb{Q}}}$ for all $\sigma \in \operatorname{Gal}_{\mathbb{Q}}$. Let r be the rank of the reductive group G_A° and hence also the rank of G. Since we are assuming the Mumford–Tate conjecture for A, the rank of each $G_{A,\ell}^\circ$ is also r.

For each nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ for which A has good reduction, let $\Phi_{A,\mathfrak{p}}$ be the subgroup of $\overline{\mathbb{Q}}^\times$ generated by the set of roots $\mathcal{W}_{A,\mathfrak{p}} \subseteq \overline{\mathbb{Q}}$ of $P_{A,\mathfrak{p}}(x)$. There is an action of $\mathrm{Gal}_\mathbb{Q}$ on the set $\mathcal{W}_{A,\mathfrak{p}}$, and hence also on the group $\Phi_{A,\mathfrak{p}}$, since $P_{A,\mathfrak{p}}(x)$ has rational coefficients. If $\Phi_{A,\mathfrak{p}}$ is torsion-free, then it is a free abelian group of rank at most r and $\mathfrak{p}$ splits completely in K_A^{conn}, cf. Lemma 3.3(i). By Lemma 3.3(ii), there is a set S of prime ideals of density 0 such that if $\mathfrak{p} \notin S$ splits completely in K_A^{conn}, then A has good reduction at $\mathfrak{p}$ and $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r.

Consider a nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ for which A has good reduction and $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r. Associated to $\mathfrak{p}$ is a Frobenius torus $T_\mathfrak{p}$ of G. More precisely, Theorem 5.1 implies that there is a maximal torus $T_\mathfrak{p}$ of G and an element $t_\mathfrak{p} \in T_\mathfrak{p}(\mathbb{Q})$ such that $f(t_\mathfrak{p}) \in \mathrm{GL}_{V_A}(\overline{\mathbb{Q}})$ has characteristic polynomial $P_{A,\mathfrak{p}}(x)$ and such that the homomorphism $X(T_\mathfrak{p}) \to \overline{\mathbb{Q}}^\times$, $\alpha \mapsto \alpha(t_\mathfrak{p})$ induces an isomorphism

$$(1.1) \qquad\qquad\qquad\qquad X(T_\mathfrak{p}) \xrightarrow{\sim} \Phi_{A,\mathfrak{p}}.$$

The isomorphism (1.1) respects the $\mathrm{Gal}_\mathbb{Q}$-actions.

Let $L \subseteq \overline{\mathbb{Q}}$ be any number field for which G_L is split. The group $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L)$ acts faithfully on $\Phi_{A,\mathfrak{p}}$. The Weyl group $W(G, T_\mathfrak{p})$ of G with respect to $T_\mathfrak{p}$ also acts faithfully on $X(T_\mathfrak{p})$. Via the isomorphism (1.1), we can identify $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L)$ with a subgroup of $W(G, T_\mathfrak{p})$, cf. §6. In particular, we have $[L(\mathcal{W}_{A,\mathfrak{p}}) : L] \leqslant |W(G)| = |W(G_A^\circ)|$.

Now fix a nonzero prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ for which A has good reduction and $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank r (it suffices to take $\mathfrak{q} \notin S$ that splits completely in K_A^{conn}). Define $L := \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$. The group G_L is split since we have a maximal torus $T_\mathfrak{q}$ of G that splits over L. We have $L \supseteq k$ where k is the field from §1.1. By Theorem 1.4, there is a set $S' \supseteq S$ of prime ideals of density 0 such that if $\mathfrak{p} \notin S'$ splits completely in K_A^{conn}, then A has good reduction at $\mathfrak{p}$ and the following conditions hold:

- $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r,
- $[L(\mathcal{W}_{A,\mathfrak{p}}) : L] = |W(G_A^\circ)|$.

Take any $\mathfrak{p}$ satisfying the above conditions. Using the isomorphism (1.1) as an identification, we have an inclusion $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) \subseteq W(G, T_\mathfrak{p})$. Therefore, $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) = W(G, T_\mathfrak{p})$ since the two groups both have cardinality $|W(G_A^\circ)|$.

With our choice of $\mathfrak{q}$ and $\mathfrak{p}$ as above, we now explain that Theorem 1.1 holds with these primes. We shall use the isomorphism (1.1) as an identification $X(T_\mathfrak{p}) = \Phi_{A,\mathfrak{p}}$. Under this identification, the set of weights $\Omega \subseteq X(T_\mathfrak{p})$ of the representation

$$\rho\colon G_{\overline{\mathbb{Q}}} \xrightarrow{f} (G_A^\circ)_{\overline{\mathbb{Q}}} \subseteq \mathrm{GL}_{V_A \otimes_\mathbb{Q} \overline{\mathbb{Q}}}$$

with respect to $T_\mathfrak{p}$ agrees with the set of roots $\mathcal{W}_{A,\mathfrak{p}}$ of $P_{A,\mathfrak{p}}(x)$. Moreover, the multiplicity of a weight $\alpha \in \Omega$ agrees with the multiplicity of α viewed as a root of $P_{A,\mathfrak{p}}(x)$. The Galois group $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L)$ acts faithfully on the set $\mathcal{W}_{A,\mathfrak{p}}$ and hence also on the group $\Phi_{A,\mathfrak{p}}$. With respect to our identification $X(T_\mathfrak{p}) = \Phi_{A,\mathfrak{p}}$, we have $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) = W(G, T_\mathfrak{p})$.

So from the polynomials $P_{A,\mathfrak{p}}(x)$ and $P_{A,\mathfrak{q}}(x)$, we have found a group of characters $X(T_\mathfrak{p})$ with $T_\mathfrak{p}$ a maximal torus of G, the $\mathrm{Gal}_\mathbb{Q}$-action on $X(T_\mathfrak{p})$, the set of weights $\Omega \subseteq X(T_\mathfrak{p})$ of ρ with multiplicities, and the group $W(G, T_\mathfrak{p})$ acting faithfully on $X(T_\mathfrak{p})$. From this information, we explain in §7 how to compute the set of roots $R(G, T_\mathfrak{p}) \subseteq X(T_\mathfrak{p})$ of G with respect to $T_\mathfrak{p}$. In this root computation, we make use of the fact that the each irreducible representation of $(G_A^\circ)_{\overline{\mathbb{Q}}}$ in $V_A \otimes_\mathbb{Q} \overline{\mathbb{Q}}$ is *minuscule*, cf. Proposition 4.8. Finally, we will observe that the root datum $\Psi(G, T_\mathfrak{p})$ is directly determined by $X(T_\mathfrak{p})$, $R(G, T_\mathfrak{p})$ and the action of $W(G, T_\mathfrak{p})$ on $X(T_\mathfrak{p})$. Since G is an inner form of G_A°, this gives us the desired quantities of Theorem 1.1.

For the Hodge group Hg_A, the character group can be taken to be $\Phi_{A,\mathfrak{p}}/\langle N(\mathfrak{p})\rangle$ and the roots and weights are the image of those of G_A°, see §8.6 for details.

1.6. **Algorithms.** We take it as given that for a nonzero prime ideal $\mathfrak{p}$ for which A has good reduction, the polynomial $P_{A,\mathfrak{p}}(x)$ can be computed; one can also ignore a finite number of troublesome primes. This should certainly be possible if A is given explicitly. The (reverse) of the polynomial $P_{A,\mathfrak{p}}(x)$ will occur as a factor in a zeta function and there are many techniques and strategies for computing zeta functions. Given a polynomial $P_{A,\mathfrak{p}}(x)$, the structure of the group $\Phi_{A,\mathfrak{p}}$ is computable, cf. §3.4.

We now assume that Conjectures 4.3 and 4.5 for A hold. Let r be the rank of G_A°. As noted in the overview in §1.5, there are nonzero prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_K$ such that A has good reduction and the following conditions hold:

(a) $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank r,
(b) $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r and $[L(\mathcal{W}_{A,\mathfrak{p}}) : L] = |W(G_A^\circ)|$, where $L := \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$.

Moreover, the set of $\mathfrak{q}$ satisfying (a) has positive density. For a fixed $\mathfrak{q}$, the set of $\mathfrak{p}$ satisfying (b) also has positive density (in fact, these densities can be bounded below by a positive constant that depends only on the dimension of A).

Assume that we know the Frobenius polynomials of two prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ as above. Let $\pi_1,\ldots,\pi_n$ be the distinct elements of $\mathcal{W}_{A,\mathfrak{p}}$ (working in some splitting field of $P_{A,\mathfrak{p}}(x)$). Let $\varphi\colon \mathbb{Z}^n \to \Phi_{A,\mathfrak{p}}$ be the surjective homomorphism satisfying $\varphi(e_i) = \pi_i$, where $e_1,\ldots,e_n$ is the standard basis of $\mathbb{Z}^n$. In §3.4, we explain how to compute to compute $\ker\varphi$ and hence $X := \mathbb{Z}^n/\ker\varphi$ gives the structure of $\Phi_{A,\mathfrak{p}}$. The Galois action on the roots $\pi_1,\ldots,\pi_n$ of $P_{A,\mathfrak{p}}(x)$ gives an injective homomorphism $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q}) \hookrightarrow S_n$. This gives an action of $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q})$ on $\mathbb{Z}^n/\ker\varphi$ that agrees with the action on $\Phi_{A,\mathfrak{p}}$ via the isomorphism induced by φ. Looking over the overview in §1.5 and using our isomorphism $X \xrightarrow{\sim} \Phi_{A,\mathfrak{p}}$, one can compute the set of weights $\Omega \subseteq X$ with multiplicities and the Weyl group $W := \mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L)$ with its action on X (with $L = \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$). As noted in the overview, the set of roots in X of G_A° can also be found using the algorithm from §7. We can thus find the root datum of G_A° and the action of $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q})$ on X gives the homomorphism $\mu_{G_A^\circ}$. As an aside, we note that we do not need to know the field K_A^{conn} for these computations.

So everything in Theorem 1.1 is computable, under Conjectures 4.3 and 4.5, assuming we can find prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ satisfying (a) and (b), respectively. Moreover, in such a situation one should be able to make the computational *unconditional*. Indeed, the existence of a prime $\mathfrak{q}$ satisfying (a) implies the Mumford–Tate conjecture for A, cf. Theorem 4.3 of [LP95] and Lemma 3.3. Conjecture 4.5 is not required if one can choose $\mathfrak{q}$ and $\mathfrak{p}$ so that A has ordinary reduction at these primes, cf. [Noo95]; this is doable in practice.

If we knew the integers r and $w := |W(G_A^\circ)|$, then we could just check primes $\mathfrak{q}$ and $\mathfrak{p}$ until we found a pair that satisfies (a) and (b), and we would have a deterministic algorithm to compute the information stated in Theorem 1.1.

However, r and w may not be known a priori. By looking at several good prime ideals $\mathfrak{p}$, say with norm up to some bound, we can make predictions for the value r and w. Let r' be maximal rank of a torsion-free group $\Phi_{A,\mathfrak{p}}$ that we encounter. We have $r' \leqslant r$, cf. Lemma 3.3(i). Fix a prime ideal $\mathfrak{q}$ for which $\Phi_{A,\mathfrak{q}}$ is free abelian of rank r'. Define $L := \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$ and let w' be the maximal value of the degree $[L(\mathcal{W}_{A,\mathfrak{p}}) : L]$ that is encountered amongst all good prime ideals $\mathfrak{p}$ for which $\Phi_{A,\mathfrak{p}}$ is free of rank r'. If $r' = r$, then $w' \leqslant w$, cf. §6.

Given r' and w', we can apply the above algorithm to obtain a prediction for the information of Theorem 1.1 (or we might have incompatible input for the root computations which, under the Mumford–Tate conjecture, says that $r' \neq r$ or $w' \neq w$). Assuming Conjectures 4.3 and 4.5, we will

obtain correct results by considering sufficiently many primes.

When trying to implement the above algorithm, besides possible finding the Frobenius polynomial, the biggest computational bottleneck is computing the splitting fields of the Frobenius polynomials $P_{A,\mathfrak{p}}(x)$ over $\mathbb{Q}$. In §9, we explain how without computing such splitting fields we can still compute the root datum $\Psi(G_A^\circ)$ up to isomorphism, the *image* of the homomorphism $\mu_{G_A^\circ}\colon \operatorname{Gal}_\mathbb{Q} \to \operatorname{Out}(\Psi(G_A^\circ))$, and the set of weights of the representation $G_A^\circ \subseteq \operatorname{GL}_{V_A}$ and their multiplicities.

An implementation of this algorithm in `Magma` [BCP97] can be found at:

<div align="center">

https://github.com/davidzywina/monodromy

</div>

Remark 1.15. The sets of density 0 in our proof of Theorem 1.1 arise from several applications of the Chebotarev density theorem. Making these sets computable is tricky because Chebotarev's theorem is applied to Galois extensions arising from the representations $\rho_{A,\ell}$ whose image is difficult to give explicitly (if we knew its image easily, we would easily obtain $G_{A,\ell}^\circ$).

At least under the Generalized Riemann Hypothesis (GRH) for number fields, it is possible to say something about the $\mathfrak{q}$ with smallest norm satisfying (a). Let r_0 be the common rank of the reductive groups $G_{A,\ell}$, cf. Lemma 3.3(iii); it equals r assuming the Mumford–Tate conjecture. In §7 of [Zyw19], it is show assuming GRH that there is a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ satisfying

$$N(\mathfrak{q}) \leqslant C(\max\{[K:\mathbb{Q}], h(A), \log D\})^f$$

for which A has good reduction and $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank r_0, where C and f are positive constants that depend only on g, $h(A)$ is the (logarithmic absolute and semistable) Faltings height of A, and D is the product of rational primes that ramify in K or are divisible by a prime ideal of $\mathcal{O}_K$ for which A has bad reduction. The constants C and f are computable but not worked out in [Zyw19]; they are likely too large to be of practical use.

1.7. **A CM example.** Let A be the Jacobian of the smooth projective curve C over $\mathbb{Q}$ defined by the equation $y^2 = x^9 - 1$; it is an abelian variety over $\mathbb{Q}$ of dimension 4.

Computing $\Phi_{A,\mathfrak{p}}$ for a few small primes, say $5 \leqslant p \leqslant 100$, we observe that $\Phi_{A,\mathfrak{p}}$ has torsion when $p \not\equiv 1 \pmod 9$ and is free of rank 4 when $p \equiv 1 \pmod 9$. For those primes satisfying $p \equiv 1 \pmod 9$, we also observe that $\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}}) = \mathbb{Q}(\zeta_9)$, where ζ_9 is a primitive 9-th root of unity in $\overline{\mathbb{Q}}$.

Assuming these properties for the groups $\Phi_{A,\mathfrak{p}}$ are typical, we now make a prediction for the group G_A° (while implicitly assuming that Conjectures 4.3 and 4.5 hold for A); we will prove these predictions afterwards. Using that conditions (a) and (b) should hold for a positive density set of primes, we expect that the rank of G_A° is 4 and $W(G_A^\circ) = 1$. In particular, we expect G_A° to be a torus of rank 4.

Consider any good prime $\mathfrak{p}$ for which $\Phi_{A,\mathfrak{p}}$ is free of rank 4. We then obtain a Frobenius maximal torus $T_\mathfrak{p}$ of G_A° which equals G_A° (note that G_A° is quasi-split since it is a torus). There is an element $t_\mathfrak{p} \in T_\mathfrak{p}(\mathbb{Q}) = G_A^\circ(\mathbb{Q})$ such that we have an isomorphism

$$(1.2) \qquad\qquad X(G_A^\circ) = X(T_\mathfrak{p}) \xrightarrow{\sim} \Phi_{A,\mathfrak{p}}, \quad \alpha \mapsto \alpha(t_\mathfrak{p})$$

for which the weights $\Omega \subseteq X(G_A^\circ)$ of the representation V_A of G_A° correspond with the roots $\mathcal{W}_{A,\mathfrak{p}} \subseteq \Phi_{A,\mathfrak{p}}$ of $P_{A,\mathfrak{p}}(x)$. We expect there to be $a, b, c \in \overline{\mathbb{Q}}$ such that the roots of $P_{A,\mathfrak{p}}(x)$ are:

$$(1.3) \qquad\qquad a, \quad b, \quad c, \quad p/a, \quad p/b, \quad p/c, \quad abc/p, \quad p^2/(abc)$$

and they are all distinct; this can be computed for any suitable prime (say $p = 19$) and then will hold in general by our isomorphism (1.2). We can also describe the action of $\Gamma := \operatorname{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ on the roots (1.3). We can choose a, b and c so that $\operatorname{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}(\sqrt{-3}))$ permutes these three roots transitively. This then describes the action of Γ on these roots since complex conjugation takes a root α to p/α.

We now have our description of the group G_A° and its representation up to isomorphism. Since G_A° is a torus, it is determined up to isomorphism, by the group $X(G_A^\circ)$ and the $\mathrm{Gal}_\mathbb{Q}$-action. So we can take $X := X(G_A^\circ)$ to be the free (multiplicative) abelian group on symbols a, b, c and p. We let $\Gamma := \mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ act on the group X by letting it fix p, letting $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}(\sqrt{-3}))$ act transitively on $\{a, b, c\}$, and letting complex conjugation map any $\alpha \in \{a, b, c\}$ to p/α. The representation V_A of G_A° is then determined, up to isomorphism, by letting (1.3) be the weights in X (each with multiplicity 1).

Following §1.3, one can then show that $\dim_\mathbb{Q} \mathcal{H}^2(A) = M_{4,1} = 8$. Indeed, Shioda has proved that $\dim_\mathbb{Q} \mathcal{H}^2(A) = 8$, cf. Example 6.1 of [Shi81] (moreover, $\mathcal{H}^2(A)$ is not generated by the intersection of pairs of divisors of A).

We now prove the above predictions. First observe that the abelian variety A has complex multiplication. Moreover, we have an isomorphism of rings $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}[\zeta_9]$, where ζ_9 corresponds with the automorphism of $A_{\overline{\mathbb{Q}}}$ arising from the automorphism $(x, y) \mapsto (\zeta_9 x, y)$ of $C_{\overline{\mathbb{Q}}}$. The field of definition of the endomorphisms of $A_{\overline{\mathbb{Q}}}$ is $\mathbb{Q}(\zeta_9)$, so $\mathbb{Q}(\zeta_9) \subseteq K_A^{\mathrm{conn}}$. This explains the condition $p \equiv 1 \pmod{9}$ above; we need this to hold for p to split completely in K_A^{conn}. In fact, one can show that $K_A^{\mathrm{conn}} = \mathbb{Q}(\zeta_9)$.

The group G_A° is a torus; we can identify it with a subgroup of the torus $\mathrm{Res}_{L/\mathbb{Q}}(\mathbb{G}_m)$, where $L := \mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_\mathbb{Z} \mathbb{Q}$, since the actions of G_A° and L commute and V_A is a 1-dimension L-vector space. In particular, $W(G_A^\circ) = 1$. The Mumford–Tate conjecture holds for all CM abelian varieties and in particular for A, cf. [Poh68, Yu15]. Conjecture 4.5 also holds for all CM abelian varieties and in particular A; this follows for example from the idelic description of the Galois representations as given in §7 of [ST68].

Since $W(G_A^\circ) = 1$ and the Conjectures 4.3 and 4.5 hold for A, to verify our predictions for G_A° it suffices to prove that $r = 4$. Suppose on the contrary that $r \neq 4$. We have $r \geqslant 5$ since we have observed that there are primes p for which $\Phi_{A,p}$ has rank 4. Since the the Mumford–Tate conjecture for A holds, there is a good prime p such that $\Phi_{A,p}$ is a free abelian group of rank $r \geqslant 5$. There are $a, b, c, d \in \overline{\mathbb{Q}}$ such the roots of $P_{A,p}(x)$ are:

$$(1.4) \qquad a, \quad b, \quad c, \quad d, \quad p/a, \quad p/b, \quad p/c, \quad p/d.$$

We deduce that $r = 5$ and that $\Phi_{A,p}$ has basis $\{a, b, c, d, p\}$. Arguing as above, though now unconditionally, we have an isomorphism (1.2) and the weights are given by (1.4). Following §1.3, one can compute that $\dim_\mathbb{Q} \mathcal{H}^2(A) = M_{4,1} = 6$. However, this contradicts the result of Shioda mentioned above. Therefore, $r = 4$ as claimed.

Remark 1.16. As noted by Shioda in Example 6.1 of [Shi81], A is isogenous to $B \times E$, where B is a simple abelian variety of dimension 3 and E is an elliptic curve. So $P_{A,p}(x) = P_{B,p}(x) \cdot P_{E,p}(x)$ for all good primes p. When $\Phi_{A,p}$ is free of rank 4, we can choose the roots (1.3) of $P_{A,p}(x)$ so that abc/p and $p^2/(abc)$ are the distinct roots of $P_{E,p}(x)$.

1.8. **Another example.** Let C be the smooth projective curve over $\mathbb{Q}$ with affine model

$$(1.5) \qquad y^2 = x(x^{20} + 7x^{18} - 7x^2 - 1).$$

Let A be the Jacobian of C; it is an abelian variety over $\mathbb{Q}$ of dimension 10.

We have computed the group $\Phi_{A,p}$ for all odd primes $p \leqslant 200$ for which the right hand side of (1.5) is separable modulo p. For such primes p, the group $\Phi_{A,p}$ is torsion-free if and only if p is an element of $\mathcal{P} := \{17, 41, 73, 89, 97, 113, 137, 193\}$. Moreover, $\Phi_{A,p}$ has rank 6 for all $p \in \mathcal{P}$.

A computation shows that the Galois group $\Gamma := \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,p})/\mathbb{Q})$ has order $2^5 \cdot 5!$ for all $p \in \mathcal{P}$. For any prime $p \in \mathcal{P}$, we have $P_{A,p}(x) = Q_p(x)^2$ for a polynomial $Q_p(x) \in \mathbb{Q}[x]$ whose discriminant is in $-2 \cdot (\mathbb{Q}^\times)^2$. In particular, $\mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\mathcal{W}_{A,p})$. Moreover, for any distinct $p, q \in \mathcal{P}$, one can verify

that $\mathbb{Q}(\mathcal{W}_{A,q}) \cap \mathbb{Q}(\mathcal{W}_{A,p}) = \mathbb{Q}(\sqrt{-2})$. Thus for any distinct $p, q \in \mathcal{P}$, we have $[L(\mathcal{W}_{A,p}) : L] = 2^4 \cdot 5!$ where $L = \mathbb{Q}(\mathcal{W}_{A,q})$.

By considering only the primes $p \leqslant 200$ and the conditions (a) and (b) of §1.6, we predict that the rank of G_A° is 6 and $|W(G_A^\circ)| = 2^4 \cdot 5!$. We now assume that $\operatorname{rank} G_A^\circ \leqslant 6$ and $|W(G_A^\circ)| \leqslant 2^4 \cdot 5!$. Under these assumptions, we shall compute the root datum of G_A°. Fix distinct primes q and p in $\mathcal{P}$.

Using Lemma 3.3(i) and Proposition 4.4, we have inequalities: $6 = \operatorname{rank} \Phi_{A,p} \leqslant \operatorname{rank} G_{A,\ell}^\circ \leqslant \operatorname{rank} G_A^\circ$. By our assumed bound on the rank of G_A°, the groups G_A° and $G_{A,\ell}^\circ$ both have rank 6. Theorem 4.3 of [LP95] implies that the Mumford–Tate conjecture for A holds. Conjecture 4.5 will holds for the primes p and q by Proposition 4.7(ii) (by considering the middle coefficient of the Frobenius polynomials, we find that A has ordinary reduction at p and q). So excluding our initial assumptions, the following computations will be unconditional.

Since $P_{A,p}(x) = Q_p(x)^2$ with $Q_p(x) \in \mathbb{Q}[x]$ separable of degree 10, there are $\alpha_1, \ldots, \alpha_5 \in \overline{\mathbb{Q}}$ such that the distinct roots of $P_{A,p}(x)$ are $\alpha_1, \ldots, \alpha_5, p/\alpha_1, \ldots, p/\alpha_5$. Since $\Phi_{A,p}$ has rank 6, it has basis $\alpha_1, \ldots, \alpha_5, p$. Let

$$\varphi \colon \Phi_{A,p} \hookrightarrow \mathbb{Q}^6$$

be the injective homomorphism satisfying $\varphi(\alpha_i) = e_i + 1/2 \cdot e_6$ for $1 \leqslant i \leqslant 5$ and $\varphi(p) = e_6$, where $e_1, \ldots, e_6$ is the standard basis of $\mathbb{Q}^6$. Define the set

$$\Omega := \varphi(\mathcal{W}_{A,p}) = \left\{ \pm e_i + \tfrac{1}{2} \cdot e_6 : 1 \leqslant i \leqslant 5 \right\}.$$

Let $X \subseteq \mathbb{Q}^6$ be the image of φ; equivalently, the subgroup of $\mathbb{Q}^6$ generated by Ω. The map φ defines an isomorphism $\Phi_{A,p} \xrightarrow{\sim} X$.

The Galois group $\Gamma := \operatorname{Gal}(\mathbb{Q}(\mathcal{W}_{A,p})/\mathbb{Q})$ has order $2^5 \cdot 5!$. The group Γ is as large as possible when we take into account that it induces an action on the set of pairs $\{\alpha_1, p/\alpha_1\}, \ldots, \{\alpha_5, p/\alpha_5\}$. Via the isomorphism $\varphi \colon \Phi_{A,p} \xrightarrow{\sim} X$ we obtain a faithful action of Γ on X and hence also on $X \otimes_\mathbb{Z} \mathbb{Q} = \mathbb{Q}^6$. In terms of the action on $\mathbb{Q}^6$, we can identify Γ with the group of signed permutation matrices in $\operatorname{GL}_6(\mathbb{Q})$ that fix e_6. Define the field $L := \mathbb{Q}(\mathcal{W}_{A,q})$ and the group $W := \operatorname{Gal}(L(\mathcal{W}_{A,p})/L)$. The group acts W acts faithfully on $\Phi_{A,p}$. Since $\mathbb{Q}(\mathcal{W}_{A,q}) \cap \mathbb{Q}(\mathcal{W}_{A,p}) = \mathbb{Q}(\sqrt{-2})$, restriction to $\mathbb{Q}(\mathcal{W}_{A,p})$ allows to identify W with the subgroup $\operatorname{Gal}(\mathbb{Q}(\mathcal{W}_{A,p})/\mathbb{Q}(\sqrt{-2})) \subseteq \Gamma$. Via its action on $\mathbb{Q}^6$, we can also view W as the subgroup of Γ that acts on $\pm e_1, \ldots, \pm e_5$ via signed permutations that only change an even number of signs.

Let G be the quasi-split inner form of G_A°. Using our assumptions and the overview of §1.5, we deduce that there is an maximal torus T_p of G for which we have an isomorphism

$$(1.6) \qquad\qquad X(T_p) = \Phi_{A,p} \xrightarrow{\varphi}{\sim} X$$

of groups with compatible actions of $\Gamma = \operatorname{Gal}(\mathbb{Q}(\mathcal{W}_{A,p})/\mathbb{Q})$. Moreover, the groups $W(G, T_p)$ that acts faithfully on $X(T_p)$ can be identified with W via the isomorphism (1.6). The set $\Omega \subseteq X$ corresponds to the usual set of weights in $X(T_p)$; each weight has multiplicity 2 since $Q_p(x)$ is separable. Let R be the subset of X corresponding to the set $R(G, T_p)$ of roots under the isomorphism (1.6).

We now compute R. The group W acts transitively on Ω. Define the set

$$C_\Omega := \{\alpha - \beta : \alpha, \beta \in \Omega, \ \alpha \neq \beta\};$$

it is the union of the two W-orbits $\{\pm e_i \pm e_j : 1 \leqslant i < j \leqslant 5\}$ and $\{\pm 2 e_i : 1 \leqslant i \leqslant 5\}$. Applying Algorithm 7.1 and Proposition 7.2, we find that the root system R is irreducible and is a subset of C_Ω. By Propositions 7.3 and 7.5, we find that R is of Lie type D_5 and that

$$R = \{\pm e_i \pm e_j : 1 \leqslant i < j \leqslant 5\}.$$

To finish computing the quantities of Theorem 1.1, we observe that the set of roots $R \subseteq X$ and the action of the Weyl group W on X determines the desired root datum, cf. Lemma 2.2. The

homomorphism $\mu_{G_A^\circ}$ arises from the natural isomorphism $\mathrm{Gal}(\mathbb{Q}(\sqrt{-2})/\mathbb{Q}) = \Gamma/W$.

Finally, Lemma 1.17 makes the above computations unconditional. For the proof, we need to know the structure of the ring $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$; this is not something that can be determined by considering only Frobenius polynomials (though following §1.4, we can predict that it is a semisimple central algebra over $\mathbb{Q}$ of degree 2).

Lemma 1.17. *The group G_A° has rank 6 and $W(G_A^\circ)$ has cardinality $2^4 \cdot 5!$.*

Proof. Let α and β be the automorphisms of $C_{\overline{\mathbb{Q}}}$ given by $(x,y) \mapsto (-1/x, y/x^{11})$ and $(x,y) \mapsto (-x, i \cdot y)$, respectively. Let $\overline{\alpha}$ and $\overline{\beta}$ be the automorphisms of the Jacobian $A_{\overline{\mathbb{Q}}}$ induced by α and β, respectively. We have $\alpha^2 = \iota$, $\beta^2 = \iota$ and $\alpha \circ \beta = \iota \circ \beta \circ \alpha$, where ι is the hyperelliptic involution. Since ι induces multiplication by -1 on $A_{\overline{\mathbb{Q}}}$, we find that the $\mathbb{Q}$-subalgebra D of $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ generated by $\overline{\alpha}$ and $\overline{\beta}$ is a quaternion algebra over $\mathbb{Q}$ for which $D \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to the real quaternions.

We claim that $D = \mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Assuming the claim, we now prove the lemma. Let Hg_A be the Hodge group of A, cf. §4.1. By Corollary 5.26 of [BGK10], we have $(\mathrm{Hg}_A)_{\mathbb{C}} \cong \mathrm{SO}(10)$; moreover, the group Hg_A is as large as possible when you take into account a polarization and the endomorphisms of A. Therefore, Hg_A has rank 5 and its Weyl group is isomorphic to the group $W(D_5)$ which has order $2^4 5!$. The lemma is now immediate since $G_A^\circ = \mathbb{G}_m \cdot \mathrm{Hg}_A \supsetneq \mathrm{Hg}_A$.

Since $D \subseteq \mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$, to prove the above claim it suffices to show that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ has dimension 4 over $\mathbb{Q}$. Fix a number field $K \subseteq \overline{\mathbb{Q}}$ so that A_K is isogenous to $\prod_{i=1}^s A_i$, where the A_i/K are powers of simple abelian varieties that are pairwise nonisogenous. By increasing K, we may further assume that $\mathrm{End}(A_K) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$, that $K_A^{\mathrm{conn}} = K$, and that $K_{A_i}^{\mathrm{conn}} = K$ for all $1 \leqslant i \leqslant s$. We have

$$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_1 \times \cdots \times B_s,$$

where $B_i := \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$. Each B_i is a central simple algebra over its center L_i. Let m_i be the degree of B_i, i.e., the positive integer for which $m_i^2 = \dim_{L_i} B_i$. The ring $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is noncommutative since it contains D. So we may assume that $m_1 \geqslant 2$ after possibly renumbering the A_i.

Take any prime $p \in \mathcal{P}$. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal dividing p and let d be the degree of $\mathbb{F}_{\mathfrak{p}}$ over $\mathbb{F}_p$. We have a surjective map

$$\mathcal{W}_{A,p} \to \mathcal{W}_{A_K,\mathfrak{p}}, \quad \pi \mapsto \pi^d;$$

it is a bijection since $\Phi_{A,p}$ is torsion-free. This bijection respects the $\mathrm{Gal}_{\mathbb{Q}}$-actions and $P_{A,p}(x)$ is the square of an irreducible polynomial, so $P_{A_K,\mathfrak{p}}(x) = Q(x)^2$ for an irreducible $Q(x) \in \mathbb{Q}[x]$. Since $P_{A_K,\mathfrak{p}}(x) = \prod_{i=1}^s P_{A_i,\mathfrak{p}}(x)$, the polynomial $P_{A_1,\mathfrak{p}}(x)$ is either $Q(x)$ or $Q(x)^2$. However, Lemma 6.1 of [Zyw14] implies that $P_{A_i,\mathfrak{p}}(x)$ is an m_i-th power (moreover, it shows that all the weights of $G_{A_i}^\circ$ acting on V_{A_i} have multiplicity m_i). Since $m_1 \geqslant 2$, we deduce that $P_{A_1,\mathfrak{p}}(x) = Q(x)^2 = P_{A_K,\mathfrak{p}}(x)$. Therefore, $s = 1$ and $m_1 = 2$. So $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_1$ and $\dim_{L_1} B_1 = 2^2$. To complete the lemma, it thus suffices to prove that $L_1 = \mathbb{Q}$.

Take any prime $q \in \mathcal{P} - \{p\}$. By Corollary 7.4.4 of [CMSV19], L_1 is isomorphic to a subfield of $\mathbb{Q}(\pi)$ for any $\pi \in \mathcal{W}_{A,p}$. Similarly, L_1 is isomorphic to a subfield of $\mathbb{Q}(\pi)$ for any $\pi \in \mathcal{W}_{A,q}$. Since $\mathbb{Q}(\mathcal{W}_{A,p}) \cap \mathbb{Q}(\mathcal{W}_{A,q}) = \mathbb{Q}(\sqrt{-2})$, the field L_1 is isomorphic to $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-2})$. From our earlier description of the Galois groups $W = \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,p})/\mathbb{Q}(\sqrt{-2}))$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,p})/\mathbb{Q})$, we find that $\sqrt{-2} \notin \mathbb{Q}(\pi)$ for all $\pi \in \mathcal{W}_{A,p}$. Therefore, $L_1 = \mathbb{Q}$. $\square$

Remark 1.18. Our set $\mathcal{P}$ is precisely the set of primes $p \leqslant 200$ that are congruent to 1 modulo 8. This suggests that K_A^{conn} is $\mathbb{Q}(\zeta_8)$.

1.9. **Structure of paper.** In §2, we recall what we need concerning reductive groups and root data. In §3, we review ℓ-adic monodromy groups. In §3.3, we describe some properties of the groups $\Phi_{A,\mathfrak{p}}$ and in §3.4 we explain how they can be computed. In §4, we recall the Mumford–Tate and Hodge groups of A and state the conjectures our theorems are conditional on.

In §5, we explain how to certain prime ideals $\mathfrak{p}$, we can construct a maximal torus $T_{\mathfrak{p}}$ of a quasi-split inner form of G_A°. Theorem 1.4 is proved in §6; much of the proof is dedicated to reducing to a setting considered by the author in an earlier paper. In §7, we explain how to compute roots of certain reductive groups over a field of characteristic 0 given a maximal torus, weights of a faithful representation, and the Weyl group.

In §8, we prove Theorems 1.1 and 1.6. We make some additional computational remarks in §9. Finally, Proposition 1.13 is proved in §10.

1.10. **Notation.** For a number field K, we denote by $\mathcal{O}_K$ the ring of integers of K. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we define its residue field $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$. Throughout, ℓ will always denote a rational prime. When talking about prime ideals of a number field K, density will always refer to *natural density*.

For a scheme X over a commutative ring R and a commutative R-algebra S, we denote by X_S the base extension of X by $\operatorname{Spec} S$.

Let V be a free module of finite rank over a field F. Denote by GL_V the F-scheme such that $GL_V(R) = \operatorname{Aut}_R(V \otimes_F R)$ for any commutative F-algebra R with the obvious functoriality. For an algebraic group G over a field F, we denote by G° the neutral component of G, i.e., the connected component of the identity of G. Note that G° is an algebraic subgroup of G.

2. Reductive groups

In this section, we recall what we need about reductive groups. For background on reductive groups see [Spr79]. Let k be a field of characteristic 0 and define $\operatorname{Gal}_k := \operatorname{Gal}(\bar{k}/k)$, where $\bar{k}$ is a fixed algebraic closure of k.

Let G be a connected and reductive group over k. Fix a maximal torus T of G.

2.1. **Character groups.** We define X(T) to be the group of homomorphisms $T_{\bar{k}} \to (\mathbb{G}_m)_{\bar{k}}$; it is a free abelian group whose rank is the dimension of T. There is a natural action of Gal_k on X(T) since T is defined over k. The group X(T) with its Gal_k-action determine the torus T up to isomorphism.

2.2. **Weyl group.** Let $N_G(T)$ be the normalizer of T in G. The torus T is its own centralizer in G. The (absolute) Weyl group of G with respect to T is the group

$$W(G,T) := N_G(T)(\bar{k})/T(\bar{k});$$

it is finite. Since G and T are defined over k, there is a natural action of Gal_k on W(G,T).

The Weyl group W(G,T) acts on the abelian group X(T); for $w \in W(G,T)$ and $\alpha \in X(T)$, we have

$$(w \cdot \alpha)(t) = \alpha(n^{-1}tn),$$

where $n \in N_G(T)(\bar{k})$ is a representative of w. The action of W(G,T) on X(T) is faithful and hence we can identify if with a subgroup of $\operatorname{Aut}(X(T))$.

Take any other maximal torus T′ of G. There is an element $g \in G(\bar{k})$ satisfying $gT_{\bar{k}}g^{-1} = T'_{\bar{k}}$. The homomorphism $N_G(T)_{\bar{k}} \to N_G(T')_{\bar{k}}$, $n \mapsto gng^{-1}$ is an isomorphism which induces an isomorphism $W(G,T) \xrightarrow{\sim} W(G,T')$. A different choice of g will alter this isomorphism by composing with an inner automorphism. So by using these isomorphisms, we can define a group W(G) for which there is an isomorphism to each W(G,T) that is distinguished up to composition with an inner automorphism.

2.3. Weights. Let $\rho\colon G \to GL_V$ be a representation, where V is a finite dimensional vector space over k. For each character $\alpha \in X(T)$, let V_α be the set of $v \in V \otimes_k \bar{k}$ satisfying $\rho(t)v = \alpha(t)v$ for all $t \in T(\bar{k})$. Each V_α is a $\bar{k}$-vector space and we have a direct sum

$$V \otimes_k \bar{k} = \bigoplus_{\alpha \in X(T)} V_\alpha.$$

A **weight** of ρ relative to T is an $\alpha \in X(T)$ for which $V_\alpha \neq 0$. We will denote the set of weights of ρ by Ω_ρ or Ω_V. Since G, T and ρ are defined over k, we find that Ω_V is stable under the Gal_k-action on $X(T)$. The set of weights Ω_V is also stable under the action of the Weyl group $W(G, T)$. The **multiplicity** of a weight α is the dimension of V_α over $\bar{k}$.

A **root** of G relative to T is a nontrivial weight of the adjoint representation of G. Denote the set of such roots by $R(G, T)$; it is stable under the actions of Gal_k and $W(G, T)$.

2.4. Root datum.

Definition 2.1. *A* **root datum** *is a 4-tuple* $(X, R, X^\vee, R^\vee)$ *where*

- *X and $X^\vee$ are free abelian groups of finite rank with a perfect pairing $\langle\,,\,\rangle\colon X \times X^\vee \to \mathbb{Z}$,*
- *R and $R^\vee$ are finite subsets of X and $X^\vee$, respectively, with a bijection $R \to R^\vee$, $\alpha \mapsto \alpha^\vee$,*

such that the following conditions hold for all $\alpha \in R$:

(a) $\langle \alpha, \alpha^\vee \rangle = 2$,
(b) $s_\alpha(R) = R$, *where s_α is the automorphism of X defined by $s_\alpha(x) = x - \langle x, \alpha^\vee \rangle\,\alpha$,*
(c) $s_\alpha^\vee(R^\vee) = R^\vee$, *where $s_\alpha^\vee$ is the automorphism of $X^\vee$ defined by $s_\alpha^\vee(y) = y - \langle \alpha, y \rangle\,\alpha^\vee$.*

We say that a root datum $(X, R, X^\vee, R^\vee)$ is **reduced** if for each $\alpha \in R$, the only elements of R that are linearly dependent with α in $X \otimes_\mathbb{Z} \mathbb{Q}$ are $\pm\alpha$.

An **isomorphism** between root data $(X, R, X^\vee, R^\vee)$ and $(X', R', X'^\vee, R'^\vee)$ is an isomorphism $\varphi\colon X \xrightarrow{\sim} X'$ of groups that gives a bijection from R to R' and whose dual $X'^\vee \to X^\vee$, with respect to the perfect pairings, gives a bijection from $R'^\vee$ to $R^\vee$.

Fix a root datum $\Psi = (X, R, X^\vee, R^\vee)$. Let $\mathrm{Aut}(\Psi)$ be the group of automorphisms of Ψ; it is a subgroup of $\mathrm{Aut}(X)$. The **Weyl group** of Ψ is the subgroup $W(\Psi)$ of $\mathrm{Aut}(X)$ generated by the set of s_α with $\alpha \in R$. The Weyl group $W(\Psi)$ is a finite and normal subgroup of $\mathrm{Aut}(\Psi)$. The **outer automorphism group** of Ψ is $\mathrm{Out}(\Psi) := \mathrm{Aut}(\Psi)/W(\Psi)$.

Lemma 2.2. *The root datum $\Psi = (X, R, X^\vee, R^\vee)$ is determined, up to isomorphism, by the following:*

(a) the group X and the set of roots R,
(b) the group $W(\Psi)$ and its action on X.

Proof. We may assume that X, R, and $W(\Psi)$ are known, where $W(\Psi)$ is given by its faithful action on X. We may further assume that $X^\vee = \mathrm{Hom}_\mathbb{Z}(X, \mathbb{Z})$ with its perfect pairing $X \times X^\vee \to \mathbb{Z}$, $(\alpha, \beta) \mapsto \beta(\alpha)$. So to prove the lemma, we need only explain how to find the coroot $\alpha^\vee \in X^\vee$ for each $\alpha \in R$.

Take any $\alpha \in R$. Note that $s_\alpha(\alpha) = -\alpha$ and that $\{x \in X : s_\alpha(x) = x\}$ is a free $\mathbb{Z}$-module of rank $r - 1$, where r is the rank of X. Now take any $s \in W(\Psi)$ for which $s(\alpha) = -\alpha$ and for which $\{x \in X : s(x) = x\}$ is a free $\mathbb{Z}$-module of rank $r - 1$.

We claim that $s = s_\alpha$. The group $W(\Psi)$ acts on the $\mathbb{R}$-vector space $V := X \otimes_\mathbb{Z} \mathbb{R}$. Since $W(\Psi)$ is finite, there is an inner product $(\,,\,)$ on V satisfying $(w \cdot v_1, w \cdot v_2) = (v_1, v_2)$ for all $v_1, v_2 \in V$ and $w \in W(\Psi)$. By the conditions on s, we have $V = V_{-1} \oplus V_1$ and $V_{-1} = \mathbb{R}\alpha$, where V_λ is the eigenspace of s with eigenvalue λ. Since the inner product is invariant under s, we find that V_{-1} and V_1 are orthogonal. Since $V_{-1} = \mathbb{R}\alpha$ and V_1 is the orthogonal complement of V_{-1} in V, we deduce that the action of $s \in W(\Psi)$ on V depends only on α; this proves the claim.

From the claim, we can thus determine $s_\alpha \in W(\Psi)$ for any $\alpha \in R$. Since $\langle x, \alpha^\vee \rangle\alpha = x - s_\alpha(x)$ for all $x \in X$ and the pairing is perfect, we can then find $\alpha^\vee$. $\qquad\square$

14

2.5. **Root datum of** G. To our reductive group G and maximal torus T, we have a reduced root datum
$$\Psi(\mathsf{G},\mathsf{T}) := \big(X(\mathsf{T}), R(\mathsf{G},\mathsf{T}), X^\vee(\mathsf{T}), R^\vee(\mathsf{G},\mathsf{T})\big).$$

We have already defined $X(\mathsf{T})$ and $R(\mathsf{G},\mathsf{T})$. We define $X^\vee(\mathsf{T})$ to be the group of cocharacters $(\mathbb{G}_m)_{\bar{k}} \to \mathsf{T}_{\bar{k}}$. Composition defines a perfect pairing $X(\mathsf{T}) \times X^\vee(\mathsf{T}) \to \operatorname{End}((\mathbb{G}_m)_{\bar{k}}) = \mathbb{Z}$, where the last isomorphism uses that endomorphisms of $(\mathbb{G}_m)_{\bar{k}}$ are all obtained by raising to an integer power. The Weyl group $W(\Psi(\mathsf{G},\mathsf{T}))$ acts faithfully on $X(\mathsf{T})$ and we can identify it with $W(\mathsf{G},\mathsf{T})$. We will not define the set of coroots $R^\vee(\mathsf{G},\mathsf{T})$ since it is not needed in our application (we will construct our root datum in terms of Lemma 2.2).

2.6. **Outer automorphism groups.** The root datum $\Psi(\mathsf{G},\mathsf{T})$ depends only on G and T base changed to $\bar{k}$. To ease notation, we will assume that k is algebraically closed throughout §2.6.

Let G' be another connected reductive group defined over k with a fixed maximal torus T'. If there is an isomorphism $f\colon \mathsf{G} \to \mathsf{G}'$ satisfying $f(\mathsf{T}) = \mathsf{T}'$, then $X(\mathsf{T}) \to X(\mathsf{T}')$, $\alpha \mapsto \alpha \circ f^{-1}|_{\mathsf{T}'}$ is an isomorphism of groups that gives an isomorphism
$$f_*\colon \Psi(\mathsf{G},\mathsf{T}) \xrightarrow{\sim} \Psi(\mathsf{G}',\mathsf{T}')$$
of root data. The following fundamental result says that every isomorphism between $\Psi(\mathsf{G},\mathsf{T})$ and $\Psi(\mathsf{G}',\mathsf{T}')$ arises from such an f. For each $g \in \mathsf{G}(k)$, let $\operatorname{inn}(g)$ be the automorphism of G obtained by conjugation by g.

Theorem 2.3. *If $\varphi\colon \Psi(\mathsf{G},\mathsf{T}) \xrightarrow{\sim} \Psi(\mathsf{G}',\mathsf{T}')$ is an isomorphism of root data, then there is an isomorphism $f\colon \mathsf{G} \xrightarrow{\sim} \mathsf{G}'$ satisfying $f(\mathsf{T}) = \mathsf{T}'$ and $\varphi = f_*$. The isomorphism f is unique up to composing with $\operatorname{inn}(t)$ for some $t \in \mathsf{T}(k)$.*

2.6.1. *Same group and torus.* Consider the special case where $\mathsf{G} = \mathsf{G}'$ and $\mathsf{T} = \mathsf{T}'$. Let $\operatorname{Aut}(\mathsf{G},\mathsf{T})$ be the subgroup of $\operatorname{Aut}(\mathsf{G})$ consisting of all automorphisms f that satisfy $f(\mathsf{T}) = \mathsf{T}$. The map

(2.1) $$\operatorname{Aut}(\mathsf{G},\mathsf{T}) \to \operatorname{Aut}(\Psi(\mathsf{G},\mathsf{T})), \quad f \mapsto f_*$$

is a group homomorphism. By Theorem 2.3, the homomorphism (2.1) is surjective with kernel $\operatorname{inn}(\mathsf{T}(k))$. Let $\operatorname{Inn}(\mathsf{G},\mathsf{T})$ be the group of inner automorphisms f of G that satisfy $f(\mathsf{T}) = \mathsf{T}$. We have $\operatorname{Inn}(\mathsf{G},\mathsf{T}) = \operatorname{inn}(N_{\mathsf{G}}(\mathsf{T})(k))$, so the image of $\operatorname{Inn}(\mathsf{G},\mathsf{T})$ under (2.1) is $W(\mathsf{G},\mathsf{T})$. In particular, (2.1) induces an isomorphism
$$\operatorname{Aut}(\mathsf{G},\mathsf{T})/\operatorname{Inn}(\mathsf{G},\mathsf{T}) \xrightarrow{\sim} \operatorname{Out}(\Psi(\mathsf{G},\mathsf{T})).$$

Remark 2.4. Since all maximal tori of G are conjugate, the natural homomorphism $\operatorname{Aut}(\mathsf{G},\mathsf{T})/\operatorname{Inn}(\mathsf{G},\mathsf{T}) \to \operatorname{Out}(\mathsf{G}) := \operatorname{Aut}(\mathsf{G})/\operatorname{Inn}(\mathsf{G})$ is an isomorphism, where $\operatorname{Inn}(\mathsf{G})$ is the group of inner automorphism of G.

2.6.2. *Same group.* Suppose that $\mathsf{G} = \mathsf{G}'$ but the tori T and T' need not agree. Since k is algebraically closed, there is an inner automorphism f of G satisfying $f(\mathsf{T}) = \mathsf{T}'$ which induces an isomorphism $f_*\colon \Psi(\mathsf{G},\mathsf{T}) \xrightarrow{\sim} \Psi(\mathsf{G},\mathsf{T}')$. Our choice of f is not unique and can vary by composing with some $f' \in \operatorname{Inn}(\mathsf{G},\mathsf{T})$. We have $(f \circ f')_* = f_* \circ f'_*$ and from §2.6.1 we know that f'_* lies in $W(\mathsf{G},\mathsf{T})$. So our isomorphism $\Psi(\mathsf{G},\mathsf{T}) \xrightarrow{\sim} \Psi(\mathsf{G},\mathsf{T}')$ is unique up to composition with an element of the Weyl group. Using these isomorphisms, we will often suppress the torus and denote the root datum by $\Psi(\mathsf{G})$ (note that it is only uniquely determined up to an automorphism in $W(\mathsf{G},\mathsf{T})$).

With our fixed f as above, we have an isomorphism

(2.2) $$\operatorname{Aut}(\Psi(\mathsf{G},\mathsf{T})) \to \operatorname{Aut}(\Psi(\mathsf{G},\mathsf{T}')), \quad \varphi \mapsto f_* \circ \varphi \circ f_*^{-1}.$$

A different choice of f, would alter this isomorphism by conjugation by $W(\mathsf{G},\mathsf{T}')$. We thus have a canonical isomorphism $\operatorname{Out}(\Psi(\mathsf{G},\mathsf{T})) \xrightarrow{\sim} \operatorname{Out}(\Psi(\mathsf{G},\mathsf{T}'))$. Using these isomorphisms, we can suppress the torus and denote the group simply by $\operatorname{Out}(\Psi(\mathsf{G}))$.

2.6.3. *General case.* Consider again the general case where G and G' need not be equal. For an isomorphism $g\colon \Psi(G, T) \xrightarrow{\sim} \Psi(G', T')$, the group isomorphism $\mathrm{Aut}(\Psi(G, T)) \to \mathrm{Aut}(\Psi(G', T'))$, $\varphi \mapsto g \circ \varphi \circ g^{-1}$ induces an isomorphism

$$(2.3) \qquad\qquad [g]\colon \mathrm{Out}(\Psi(G)) \xrightarrow{\sim} \mathrm{Out}(\Psi(G')).$$

A different choice of g will alter (2.3) by composition with an inner automorphism of the group $\mathrm{Out}(\Psi(G'))$.

2.7. Galois action. Since T is defined over k, there is a natural action of Gal_k on $X(T)$ and $X^\vee(T)$ that respects the perfect pairing $X(T) \times X^\vee(T) \to \mathbb{Z}$. Since G and T are defined over k, we find that the sets $R(G, T)$ and $R^\vee(G, T)$ are stable under these Galois actions. The Galois action on $X(T)$ thus gives rise to a homomorphism

$$\varphi_{G,T}\colon \mathrm{Gal}_k \to \mathrm{Aut}(\Psi(G, T)).$$

By composing $\varphi_{G,T}$ with the quotient map $\mathrm{Aut}(\Psi(G, T)) \to \mathrm{Out}(\Psi(G))$, we obtain a homomorphism

$$\mu_G\colon \mathrm{Gal}_k \to \mathrm{Out}(\Psi(G))$$

that does not depend on the initial choice of T.

Let $\Gamma(G, T)$ be the subgroup of $\mathrm{Aut}(\Psi(G, T))$ that is the inverse image of $\mu_G(\mathrm{Gal}_k)$ under the homomorphism $\mathrm{Aut}(\Psi(G, T)) \to \mathrm{Out}(\Psi(G))$. Note that

$$\varphi_{G,T}(\mathrm{Gal}_k) \subseteq \Gamma(G, T).$$

From the isomorphism (2.2), we can suppress the torus and denote the common group by $\Gamma(G)$; note that it is only uniquely determined up to conjugation by $W(G)$.

2.8. Inner forms. Let G' be a connected reductive group defined over k with a fixed maximal torus T'. We say that G' is a form of G if they become isomorphic algebraic groups when base extended to $\bar{k}$. Note that G' is a form of G if and only if the root data $\Psi(G', T')$ and $\Psi(G, T)$ are isomorphic. We say that G' is an inner form of G there is an isomorphism $f\colon G_{\bar{k}} \to G'_{\bar{k}}$ such that $f^{-1} \circ \sigma(f)$ is an inner automorphism of $G_{\bar{k}}$ for all $\sigma \in \mathrm{Gal}_k$.

We shall say that the homomorphisms μ_G and $\mu_{G'}$ from §2.7 agree if there is an isomorphism $g\colon \Psi(G, T) \xrightarrow{\sim} \Psi(G', T')$ of root data such that $[g] \circ \mu_G = \mu_{G'}$ with $[g]$ as defined in §2.6.3.

Proposition 2.5. *Let G' be a connected and reductive group defined over k that is a form of G. Then G' is an inner form of G if and only if μ_G and $\mu_{G'}$ agree. In particular, the class of inner forms of G is determined by the abstract root datum $\Psi(G)$ and the homomorphism $\mu_G\colon \mathrm{Gal}_k \to \mathrm{Out}(\Psi(G))$.*

Proof. First take any isomorphism $f\colon G_{\bar{k}} \to G'_{\bar{k}}$ satisfying $f(T_{\bar{k}}) = T'_{\bar{k}}$. Take any $\sigma \in \mathrm{Gal}_k$. Since our reductive groups and tori are all defined over k, we have an isomorphism $\sigma(f)\colon G_{\bar{k}} \xrightarrow{\sim} G'_{\bar{k}}$ that satisfies $\sigma(f)(T_{\bar{k}}) = T'_{\bar{k}}$. For any character $\alpha \in X(T)$, we have

$$(\sigma(\alpha \circ f^{-1})) \circ f|_{T_{\bar{k}}} = \sigma(\alpha) \circ (\sigma(f)^{-1} \circ f)|_{T_{\bar{k}}} = \sigma(\alpha) \circ (f^{-1} \circ \sigma(f))^{-1}|_{T_{\bar{k}}}.$$

Therefore,

$$(2.4) \qquad\qquad f_*^{-1} \circ \varphi_{G',T'}(\sigma) \circ f_* = \xi_\sigma \circ \varphi_{G,T}(\sigma)$$

where $\xi_\sigma := (f^{-1} \circ \sigma(f))_* \in \mathrm{Aut}(\Psi(G, T))$.

First suppose that G' is an inner form of G and hence f may be chosen so that $f^{-1} \circ \sigma(f)$ is an inner automorphism of $G_{\bar{k}}$ for all $\sigma \in \mathrm{Gal}_k$. We have $f^{-1} \circ \sigma(f) \in \mathrm{Inn}(G_{\bar{k}}, T_{\bar{k}})$ and hence $\xi_\sigma \in W(G, T)$, cf. §2.6.1. From (2.4) and $\xi_\sigma \in W(G, T)$, we deduce that $\mu_{G'}(\sigma) = [f_*] \circ \mu_G(\sigma)$. Therefore, μ_G and $\mu_{G'}$ agree.

16

Now suppose that μ_G and $\mu_{G'}$ agree. There is an isomorphism $g\colon \Psi(G,T) \xrightarrow{\sim} \Psi(G',T')$ of root data such that $[g] \circ \mu_G = \mu_{G'}$. By Theorem 2.3, there is an isomorphism $f\colon G_{\bar{k}} \xrightarrow{\sim} G'_{\bar{k}}$ satisfying $f(T_{\bar{k}}) = T'_{\bar{k}}$ and $g = f_*$. Take any $\sigma \in \mathrm{Gal}_k$. From $[f_*] \circ \mu_G(\sigma) = \mu_{G'}(\sigma)$, we deduce that $f_* \circ \varphi_{G,T}(\sigma) \circ f_*^{-1} \circ \varphi_{G',T'}(\sigma)^{-1}$ lies in $W(G',T')$ and hence

$$f_*^{-1} \circ (f_* \circ \varphi_{G,T}(\sigma) \circ f_*^{-1} \circ \varphi_{G',T'}(\sigma)^{-1}) \circ f_* = \varphi_{G,T}(\sigma) \circ (f_*^{-1} \circ \varphi_{G',T'}(\sigma) \circ f_*)^{-1}$$

lies in $W(G,T)$. By (2.4), we find that $\xi_\sigma := (f^{-1} \circ \sigma(f))_*$ is an element of $W(G,T)$. From §2.6.1, we deduce that $f^{-1} \circ \sigma(f) \in \mathrm{Inn}(G_{\bar{k}}, T_{\bar{k}})$ for all $\sigma \in \mathrm{Gal}_k$. Therefore, G' is an inner form of G.

Finally, the last statement of the propostion is clear since the root datum of G determines the forms of G. $\qquad\square$

2.9. **Quasi-split groups.** Recall that a connected reductive group G defined over k is quasi-split if it has a Borel subgroup defined over k, i.e., there is an algebraic subgroup B of G for which $B_{\bar{k}}$ is a Borel subgroup of $G_{\bar{k}}$.

A connected reductive group G over k has an inner form G_0 that is quasi-split which is unique up to isomorphism, cf. [Mil17, Corollary 23.53]. We will refer to the group G_0 as *the* quasi-split inner form of G. Proposition 2.5 implies that G_0, up to isomorphism, is determined by the abstract root datum $\Psi(G)$ and the homomorphism $\mu_G\colon \mathrm{Gal}_k \to \mathrm{Out}(\Psi(G))$.

The quotient homomorphism $N_G(T)(\bar{k}) \to W(G,T)$ and the inclusion $N_G(T)(\bar{k}) \hookrightarrow G(\bar{k})$ induces maps $H^1(k, N_G(T)) \to H^1(k, W(G,T))$ and $H^1(k, N_G(T)) \to H^1(k, G)$, respectively, of Galois cohomology sets.

Proposition 2.6. *Suppose that G is quasi-split and that the maximal torus T contains a maximal split torus of G. Then for any $\xi \in H^1(k, W(G,T))$, there is a lift $\bar{\xi} \in H^1(k, N_G(T))$ of ξ which maps to the trivial class in $H^1(k, G)$.*

Proof. Let G' be the derived subgroup of G and define $T' := G' \cap T$. The group G' is semisimple and T' is a maximal torus of G' containing a maximal split torus of G'. The inclusion $N_{G'}(T') \subseteq N_G(T)$ induces an isomorphism $W(G',T') = W(G,T)$ that respects the Gal_k-actions. It thus suffices to prove the proposition with (G,T) replaced by (G',T'). The semisimple case of the proposition is Theorem 1.1 of [Rag04]. $\qquad\square$

2.10. **Semisimple conjugacy classes.** Let R be the affine coordinate ring of the connected reductive group G over k. The group G acts on R by composition with inner automorphisms. We define R^G to be the k-subalgebra of R consisting of those elements fixed by this G-action, i.e., the algebra of central functions on G. Define the k-variety

$$G^\sharp := \mathrm{Spec}(R^G)$$

and denote by $\mathrm{cl}_G\colon G \to G^\sharp$ the morphism induced by the inclusion $R^G \hookrightarrow R$ of k-algebras. The morphism cl_G is surjective.

Take any algebraically closed field L/k. For any $g \in G(L)$, we have $g = g_s g_u$ for unique commuting $g_s, g_u \in G(L)$ with g_s semisimple and g_u unipotent in G. For $g, h \in G(L)$, one can show that g_s and h_s are conjugate in $G(L)$ if and only if $\mathrm{cl}_G(g) = \mathrm{cl}_G(h)$. In particular, $G^\sharp(L)$ can be identified with the set of semisimple elements of $G(L)$ up to conjugacy.

2.11. **Minuscule representations.** Let $\rho\colon G \to \mathrm{GL}_U$ be an irreducible representation, where U is a finite dimensional k-vector space. The Weyl group $W(G,T)$ acts on the set of weights $\Omega_U \subseteq X(T)$ of the representation U relative to T.

We say that the representation ρ is minuscule if $W(G,T)$ acts transitively on Ω_U. The property of ρ being minuscule does not depend on the choice of T. (Note that some authors exclude the trivial irreducible representation in the definition of minuscule.)

3. ℓ-ADIC MONODROMY GROUPS

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

3.1. ℓ-adic monodromy groups.

Take any rational prime ℓ. For an integer $e \geqslant 1$, let $A[\ell^e]$ be the ℓ^e-torsion subgroup of $A(\overline{K})$; it is a free $\mathbb{Z}/\ell^e\mathbb{Z}$-module of rank $2g$. The ℓ-adic Tate module is $T_\ell(A) := \varprojlim_e A[\ell^e]$, where the inverse limit is with respect to multiplication by ℓ maps $A[\ell^{e+1}] \to A[\ell^e]$; it is a free $\mathbb{Z}_\ell$-module of rank $2g$. There is a natural action of Gal_K on the groups $A[\ell^e]$ and hence on the $\mathbb{Z}_\ell$-module $T_\ell(A)$. Define the $\mathbb{Q}_\ell$-vector space $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$; it has dimension $2g$. We have a Galois action on $V_\ell(A)$ that we can express in terms of a continuous representation

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

Definition 3.1. *The ℓ-adic monodromy group of A is the algebraic subgroup $G_{A,\ell}$ of $\mathrm{GL}_{V_\ell(A)}$ obtained by taking the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$.*

From the work of Faltings, cf. [Fal86], we know that the group $G_{A,\ell}^\circ$ is reductive. Define K_A^{conn} to be the subfield of $\overline{K}$ fixed by the kernel of the homomorphism

$$\mathrm{Gal}_K \xrightarrow{\rho_{A,\ell}} G_{A,\ell}(\mathbb{Q}_\ell) \to G_{A,\ell}(\mathbb{Q}_\ell)/G_{A,\ell}^\circ(\mathbb{Q}_\ell).$$

Equivalently, K_A^{conn} is the smallest extension of K in $\overline{K}$ that satisfies $\rho_{A,\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}}) \subseteq G_{A,\ell}^\circ(\mathbb{Q}_\ell)$.

Proposition 3.2.

    (i) The field K_A^{conn} depends only on A. In particular, it is independent of ℓ.

    (ii) The degree $[K_A^{\mathrm{conn}} : K]$ can be bounded in terms of g.

Proof. Part (i) was proved by Serre [Ser00, 133]; see also [LP97]. From (i), we find that K_A^{conn} is a subfield of $K(A[\ell^\infty])$ and hence $[K_A^{\mathrm{conn}} : K]$ divides $[K(A[\ell]) : K]\ell^{e_\ell}$ for some integer e_ℓ. Since $[K(A[\ell]) : K]$ divides $|\mathrm{GL}_{2g}(\mathbb{F}_\ell)|$, we deduce that $[K_A^{\mathrm{conn}} : K]$ divides $|\mathrm{GL}_{2g}(\mathbb{F}_\ell)|\ell^{e_\ell}$. Therefore, $[K_A^{\mathrm{conn}} : K]$ must divide $|\mathrm{GL}_{2g}(\mathbb{F}_2)| \cdot |\mathrm{GL}_{2g}(\mathbb{F}_3)|$ which completes the proof of (ii). $\square$

3.2. Compatibility.

Take any nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ for which A has good reduction. Denote by $A_\mathfrak{p}$ the abelian variety over $\mathbb{F}_\mathfrak{p}$ obtained by reducing A modulo $\mathfrak{p}$. There is a unique polynomial $P_{A,\mathfrak{p}}(x) \in \mathbb{Z}[x]$ such that $P_{A,\mathfrak{p}}(n)$ is the degree of the isogeny $n - \pi$ for each integer n, where π is the Frobenius endomorphism of $A_\mathfrak{p}/\mathbb{F}_\mathfrak{p}$. The polynomial $P_{A,\mathfrak{p}}(x)$ is monic of degree $2g$.

For each rational prime ℓ for which $\mathfrak{p} \nmid \ell$, the representation $\rho_{A,\ell}$ is unramified at $\mathfrak{p}$ and satisfies

$$\det(xI - \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})) = P_{A,\mathfrak{p}}(x).$$

Note that $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ is semisimple in $\mathrm{GL}_{V_\ell(A)}$ since π acts semisimply on the ℓ-adic Tate module of $A_\mathfrak{p}$. From Weil, we know that all of the roots of $P_{A,\mathfrak{p}}(x)$ in $\mathbb{C}$ have absolute value $N(\mathfrak{p})^{1/2}$.

3.3. The group $\Phi_{A,\mathfrak{p}}$.

Take any nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ for which A has good reduction. Let $\mathcal{W}_{A,\mathfrak{p}}$ be the set of roots of $P_{A,\mathfrak{p}}(x)$ in $\overline{\mathbb{Q}}$. We define $\Phi_{A,\mathfrak{p}}$ to be the subgroup of $\overline{\mathbb{Q}}^\times$ generated by $\mathcal{W}_{A,\mathfrak{p}}$. The abelian group $\Phi_{A,\mathfrak{p}}$ is finitely generated and has a natural $\mathrm{Gal}_\mathbb{Q}$-action since the coefficients of $P_{A,\mathfrak{p}}(x)$ are rational.

Let r be the rank of the reductive group $G_{A,\ell}^\circ$ for a fixed prime ℓ. By the following lemma, the integer r does not depend on the choice of ℓ.

Lemma 3.3.

    (i) If $\Phi_{A,\mathfrak{p}}$ is torsion-free, then $\mathfrak{p}$ splits completely in K_A^{conn} and $\Phi_{A,\mathfrak{p}}$ has rank at most r.

    (ii) There is a density 0 set S of prime ideals of $\mathcal{O}_K$ such that if $\mathfrak{p} \notin S$ splits completely in K_A^{conn}, then $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r.

    (iii) The integer r does not depend on the choice of ℓ.

Proof. Choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Take any nonzero prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which A has good reduction.

Let $T_{\mathfrak{p},\ell}$ be the Zariski closure in $G_{A,\ell}$ of the subgroup generated by the semisimple element $t_{\mathfrak{p},\ell} := \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$. Let $X(T_{\mathfrak{p},\ell})$ be the group of characters $(T_{\mathfrak{p},\ell})_{\overline{\mathbb{Q}}_\ell} \to (\mathbb{G}_m)_{\overline{\mathbb{Q}}_\ell}$. Since $T_{\mathfrak{p},\ell}$ is generated by $t_{\mathfrak{p},\ell}$, the homomorphism $f \colon X(T_{\mathfrak{p},\ell}) \to \overline{\mathbb{Q}}_\ell^\times$, $\alpha \mapsto \alpha(t_{\mathfrak{p},\ell})$ is injective. Let $\Omega_{\mathfrak{p},\ell} \subseteq X(T_{\mathfrak{p},\ell})$ be the set of weights of $T_{\mathfrak{p},\ell} \subseteq \mathrm{GL}_{V_\ell(A)}$ acting on $V_\ell(A)$; the set $\Omega_{\mathfrak{p},\ell}$ generates $X(T_{\mathfrak{p},\ell})$ since this action is faithful. The elements $\{\alpha(t_{\mathfrak{p},\ell}) : \alpha \in \Omega_{\mathfrak{p},\ell}\}$ are the roots of $P_{A,\mathfrak{p}}(x)$ in $\overline{\mathbb{Q}}_\ell$ and generate the image of f. Therefore, we have an isomorphism $f \colon X(T_{\mathfrak{p},\ell}) \to \Phi_{A,\mathfrak{p}}$, where we are using our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. In particular, the groups $X(T_{\mathfrak{p},\ell})$ and $\Phi_{A,\mathfrak{p}}$ are isomorphic.

Suppose that $\Phi_{A,\mathfrak{p}} \cong X(T_{\mathfrak{p},\ell})$ is torsion-free and hence $T_{\mathfrak{p},\ell}$ is a torus. We thus have $T_{\mathfrak{p},\ell} \subseteq G_{A,\ell}^\circ$ and hence $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in G_{A,\ell}^\circ(\mathbb{Q}_\ell)$. Therefore, $\mathfrak{p}$ splits completely in K_A^{conn}; note that $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in G_{A,\ell}^\circ(\mathbb{Q}_\ell)$ if and only if $\mathfrak{p}$ splits completely in K_A^{conn}. Since $T_{\mathfrak{p},\ell} \subseteq G_{A,\ell}^\circ$ is a torus and $G_{A,\ell}^\circ$ has rank r, we deduce that $T_{\mathfrak{p},\ell}$ has dimension at most r and hence $\Phi_{A,\mathfrak{p}} \cong X(T_{\mathfrak{p},\ell})$ has rank at most r. This proves (i) for all good primes $\mathfrak{p} \nmid \ell$. Part (i) for any excluded good primes $\mathfrak{p}|\ell$ will follow once we prove (iii) since we may choose a different initial prime ℓ.

By Theorem 1.2 of [LP97], there is a closed proper subvariety $Y \subseteq G_{A,\ell}$, that is stable under conjugation by $G_{A,\ell}$, such that if $\mathfrak{p} \nmid \ell$ is a prime ideal of $\mathcal{O}_K$ for which A has good reduction and $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in G_{A,\ell}^\circ(\mathbb{Q}_\ell) - Y(\mathbb{Q}_\ell)$, then $T_{\mathfrak{p},\ell}$ is a maximal torus of $G_{A,\ell}^\circ$. The Chebotarev density theorem then implies that there is a set S of prime ideals of $\mathcal{O}_K$ with density 0 such that if $\mathfrak{p} \notin S$ splits completely in K_A^{conn}, then $T_{\mathfrak{p},\ell}$ is a maximal torus of $G_{A,\ell}^\circ$. Since $X(T_{\mathfrak{p},\ell}) \cong \Phi_{A,\mathfrak{p}}$, there is a set S of prime ideals of $\mathcal{O}_K$ with density 0 such that if $\mathfrak{p} \notin S$ splits completely in K_A^{conn}, then $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r. This proves (ii). This also gives a characterization of the integer r that does not depend on ℓ and hence proves (iii). $\qquad\square$

Definition 3.4. *We define $\mathcal{S}_A$ to be the set of nonzero prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ for which A has good reduction and for which $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank r, where r is the common rank of the reductive groups $G_{A,\ell}^\circ$.*

Lemma 3.5.
  (i) The set $\mathcal{S}_A$ has density $1/[K_A^{\mathrm{conn}} : K]$.
  (ii) Take any prime ideal $\mathfrak{p} \in \mathcal{S}_A$ and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{K_A^{\mathrm{conn}}}$ that divides $\mathfrak{p}$. Then $\mathfrak{P} \in \mathcal{S}_{A'}$ and $P_{A',\mathfrak{P}}(x) = P_{A,\mathfrak{p}}(x)$ where A' is the base change of A to K_A^{conn}.

Proof. The set of prime ideals of $\mathcal{O}_K$ that split completely in K_A^{conn} has density $1/[K_A^{\mathrm{conn}} : K]$ by the Chebotarev density theorem. Part (i) thus follows from Lemma 3.3(i) and (ii).

We now prove (ii). The prime ideal $\mathfrak{p} \in \mathcal{S}_A$ splits completely in K_A^{conn} by Lemma 3.3(i). We thus have $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$ and hence the reduction of A and A' at the primes $\mathfrak{p}$ and $\mathfrak{P}$, respectively, agree. Therefore, $P_{A,\mathfrak{p}}(x) = P_{A',\mathfrak{P}}(x)$ and hence $\Phi_{A',\mathfrak{P}} = \Phi_{A,\mathfrak{p}} \cong \mathbb{Z}^r$. The reductive group $G_{A',\ell} = G_{A,\ell}^\circ$ has rank r and hence $\mathfrak{P} \in \mathcal{S}_{A'}$. $\qquad\square$

3.4. **Computing $\Phi_{A,\mathfrak{p}}$.** In this section, we describe how to compute the structure of the finitely generated abelian group $\Phi_{A,\mathfrak{p}}$ from $P_{A,\mathfrak{p}}(x)$; this is important to ensure that our results are algorithmic (also see Remark 3.7).

Let $\pi_1, \ldots, \pi_n$ be the distinct elements of $\mathcal{W}_{A,\mathfrak{p}}$. We have a surjective homomorphism

$$\varphi \colon \mathbb{Z}^n \to \Phi_{A,\mathfrak{p}}, \quad e \mapsto \prod_{i=1}^n \pi_i^{e_i}.$$

We first describe the $e \in \mathbb{Z}^n$ for which $\varphi(e)$ is a root of unity. Define the number field $L := \mathbb{Q}(\pi_1, \ldots, \pi_n)$. For each nonzero prime λ of $\mathcal{O}_L$, let $\nu_\lambda \colon L^\times \twoheadrightarrow \mathbb{Z}$ be the λ-adic valuation.

Lemma 3.6. *Take any $e \in \mathbb{Z}^n$. The following are equivalent:*

19

(a) $\varphi(e)$ *is a root of unity,*

(b) $\sum_{i=1}^{n} e_i v_\lambda(\pi_i) = 0$ *holds for all prime ideals* λ *of* $\mathcal{O}_L$ *dividing* $N(\mathfrak{p})$,

(c) $\sum_{i=1}^{n} e_i v_\lambda(\sigma^{-1}(\pi_i)) = 0$ *holds for a fixed prime ideal* λ *of* $\mathcal{O}_L$ *dividing* $N(\mathfrak{p})$ *and all* $\sigma \in$ $\mathrm{Gal}(L/\mathbb{Q})$.

Proof. For any prime ideal $\lambda | N(\mathfrak{p})$ of $\mathcal{O}_L$ and $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, one can check that $v_{\sigma(\lambda)}(\alpha) = v_\lambda(\sigma^{-1}(\alpha))$ holds for all $\alpha \in L$. The group $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the prime ideals of $\mathcal{O}_L$ that divide $N(\mathfrak{p})$ since $L/\mathbb{Q}$ is Galois, and hence (b) and (c) are equivalent.

For a fixed $e \in \mathbb{Z}^n$, define $\alpha := \varphi(e) = \prod_{i=1}^{n} \pi_i^{e_i} \in L^\times$. Observe that for a nonzero prime λ of $\mathcal{O}_L$, we have $v_\lambda(\alpha) = \sum_{i=1}^{n} e_i v_\lambda(\pi_i)$. If α is a root of unity, then we have $v_\lambda(\alpha) = 0$ for all λ. Therefore, (a) implies (b). We now assume that (b) holds, i.e., $v_\lambda(\alpha) = 0$ for all prime ideals $\lambda | N(\mathfrak{p})$ of $\mathcal{O}_L$. It suffices to prove that $\varphi(e)$ is a root of unity,

Take any nonzero prime ideal $\lambda \nmid N(\mathfrak{p})$ of $\mathcal{O}_L$. For each π_i, we have $\pi_i \bar{\pi}_i = N(\mathfrak{p})$, where $\bar{\pi}_i$ is the complex conjugate of π_i under any complex embedding. So $v_\lambda(\pi_i) + v_\lambda(\bar{\pi}_i) = 0$. Since π_i and $\bar{\pi}_i$ are algebraic integers, we have $v_\lambda(\pi_i) \geqslant 0$ and $v_\lambda(\bar{\pi}_i) \geqslant 0$, and hence $v_\lambda(\pi_i) = 0$. Therefore, $v_\lambda(\alpha) = 0$. Combining this with our assumption that (b) holds, we deduce that $v_\lambda(\alpha) = 0$ for all nonzero prime ideals λ of $\mathcal{O}_L$. This implies that $\alpha \in \mathcal{O}_L^\times$.

Take any embedding $\iota \colon L \hookrightarrow \mathbb{C}$. From Weil, we know that each $\iota(\pi_i)$ has absolute value $N(\mathfrak{p})^{1/2}$. Therefore, $|\iota(\alpha)| = N(\mathfrak{p})^{(e_1 + \cdots + e_n)/2}$ for any ι and hence $|N_{L/\mathbb{Q}}(\alpha)| = N(\mathfrak{p})^{[L:\mathbb{Q}](e_1 + \cdots + e_n)/2}$. We have $N_{L/\mathbb{Q}}(\alpha) = \pm 1$ since $\alpha \in \mathcal{O}_L^\times$, so $e_1 + \cdots + e_n = 0$. Therefore, α has absolute value 1 under any embedding into $\mathbb{C}$. Since α is a unit in $\mathcal{O}_L$ with absolute value 1 under any embedding into $\mathbb{C}$, we deduce that α is a root of unity. $\square$

Let $M_0 \subseteq \mathbb{Z}^n$ be the subgroup consisting of all $e \in \mathbb{Z}^n$ satisfying $\sum_{i=1}^{n} e_i v_\lambda(\pi_i) = 0$ for all prime ideals λ of $\mathcal{O}_L$ dividing $N(\mathfrak{p})$. By Lemma 3.6, we have $\varphi^{-1}(\mu_L) = M_0$, where μ_L is the (finite) subgroup of roots of unity in $L^\times$. Define the homomorphism

$$\psi := \varphi|_{M_0} \colon M_0 \to \mu_L, \quad e \mapsto \prod_{i=1}^{n} \pi_i^{e_i}.$$

Computing ψ on a basis of M_0, one can then explicitly compute $M := \ker(\psi) \subseteq \mathbb{Z}^n$. Observe that M is the kernel of φ. Therefore, φ induces an isomorphism

$$\bar{\varphi} \colon \mathbb{Z}^n / M \xrightarrow{\sim} \Phi_{A,\mathfrak{p}}.$$

Using Smith normal form, it is straightforward to compute the structure of $\mathbb{Z}^n / M$, and hence of $\Phi_{A,\mathfrak{p}}$ as a finitely generated abelian group; in particular, one can compute its rank and whether it has nontrivial torsion. The image of the standard basis elements in $\mathbb{Z}^n$ corresponds with the roots $\pi_1, \ldots, \pi_n$.

The action of $\mathrm{Gal}_\mathbb{Q}$ on $\Phi_{A,\mathfrak{p}}$ factors through $\mathrm{Gal}(L/\mathbb{Q})$; it is described by its action on the π_i. Using $\bar{\varphi}$, this gives an action of $\mathrm{Gal}(L/\mathbb{Q})$ on $\mathbb{Z}^n / M$.

Remark 3.7. We will revisit the computation of the groups $\Phi_{A,\mathfrak{p}}$ in §9.1, where for simplicity we restrict to primes $\mathfrak{p}$ for which A has good and ordinary reduction. We will be able to determine the structure of $\Phi_{A,\mathfrak{p}}$ as an abelian group without having to explicitly compute a splitting field $L/\mathbb{Q}$ of $P_{A,\mathfrak{p}}(x)$.

4. THE MUMFORD–TATE GROUP

Fix a nonzero abelian variety A defined over a number field K. Throughout we fix an embedding $\bar{K} \hookrightarrow \mathbb{C}$. In particular, using this embedding we can view K as a subfield of $\mathbb{C}$ and $A(\mathbb{C})$ as a complex manifold.

4.1. Mumford–Tate and Hodge groups.

The homology group

$$V_A := H_1(A(\mathbb{C}), \mathbb{Q}),$$

is a vector space of dimension $2 \dim A$ over $\mathbb{Q}$. It is endowed with a $\mathbb{Q}$-Hodge structure of type $\{(-1, 0), (0, -1)\}$ and hence we have a decomposition

$$V_A \otimes_{\mathbb{Q}} \mathbb{C} = H_1(A(\mathbb{C}), \mathbb{C}) = V_A^{-1,0} \oplus V_A^{0,-1}$$

satisfying $V_A^{0,-1} = \overline{V_A^{-1,0}}$. Let

$$\mu \colon \mathbb{G}_{m,\mathbb{C}} \to \mathrm{GL}_{V_A \otimes_{\mathbb{Q}} \mathbb{C}}$$

be the cocharacter for which $\mu(z)$ is the automorphism of $V_A \otimes_{\mathbb{Q}} \mathbb{C}$ that is multiplication by z on $V_A^{-1,0}$ and the identity on $V_A^{0,-1}$ for each $z \in \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C})$.

Definition 4.1. *The* **Mumford–Tate group** *of A is the smallest algebraic subgroup MT_A of GL_{V_A}, defined over $\mathbb{Q}$, which contains $\mu(\mathbb{C}^\times)$. The* **Hodge group** *of A is the smallest algebraic subgroup Hg_A of GL_{V_A}, defined over $\mathbb{Q}$, which contains $\mu(U(1))$, where $U(1) := \{z \in \mathbb{C}^\times : |z| = 1\}$.*

We have $\mathrm{MT}_A = \mathbb{G}_m \cdot \mathrm{Hg}_A$, where $\mathbb{G}_m$ is the group of homotheties in GL_{V_A}, cf. [BL04, Remark 17.3.1]. The groups MT_A and Hg_A are connected and reductive, cf. Proposition 17.3.6 and Remark 17.3.1 of [BL04].

The endomorphism ring $\mathrm{End}(A_{\overline{K}}) = \mathrm{End}(A_{\mathbb{C}})$ acts on V_A and preserves the Hodge decomposition. Therefore, $\mathrm{End}(A_{\overline{K}})$ commutes with μ and hence also MT_A. Moreover, the ring $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is naturally isomorphic to the commutant of MT_A in $\mathrm{End}_{\mathbb{Q}}(V_A)$ (or equivalently, the commutant of Hg_A in $\mathrm{End}_{\mathbb{Q}}(V_A)$), cf. [BL04, Proposition 17.3.4].

Choosing a polarization of A, we obtain a nondegenerate alternating pairing $E \colon V_A \times V_A \to \mathbb{Q}$. We have $\mathrm{Hg}_A \subseteq \mathrm{Sp}_{V_A, E}$, where $\mathrm{Sp}_{V_A, E} \subseteq \mathrm{GL}_{V_A}$ is the symplectic group with respect to the pairing E, cf. [BL04, Proposition 17.3.2]. Moreover, we have $\mathrm{MT}_A \subseteq \mathrm{GSp}_{V_A, E}$ and $\mathrm{MT}_A \cap \mathrm{Sp}_{V_A, E} = \mathrm{Hg}_A$.

Remark 4.2. As noted in §1, MT_A agrees with the identity component G_A°, where $\mathsf{G}_A \subseteq \mathrm{GL}_{V_A}$ is the motivic Galois groups of A with respect to the category of motives in the sense of André [And96].

4.2. The Mumford–Tate conjecture.

Take any prime ℓ. The **comparison isomorphism** $V_\ell(A) = V_A \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ induces an isomorphism $\mathrm{GL}_{V_\ell(A)} = \mathrm{GL}_{V_A, \mathbb{Q}_\ell}$ of algebraic groups over $\mathbb{Q}_\ell$. Note that these isomorphisms depends on our fixed embedding $\overline{K} \hookrightarrow \mathbb{C}$.

The following conjecture says that the connected $\mathbb{Q}_\ell$-algebraic groups $\mathsf{G}_{A,\ell}^\circ$ and $\mathrm{MT}_{A,\mathbb{Q}_\ell}$ are the same when we use the comparison isomorphism as an identification, cf. [Ser77, §3].

Conjecture 4.3 (Mumford–Tate conjecture)**.** *For each prime ℓ, we have $\mathsf{G}_{A,\ell}^\circ = \mathrm{MT}_{A,\mathbb{Q}_\ell}$.*

One inclusion of the Mumford–Tate conjecture is known unconditionally, see Deligne's proof in [DMOS82, I, Prop. 6.2].

Proposition 4.4. *For each prime ℓ, we have $\mathsf{G}_{A,\ell}^\circ \subseteq \mathrm{MT}_{A,\mathbb{Q}_\ell}$.*

The groups $\mathsf{G}_{A,\ell}^\circ$ are reductive and have common rank, cf. Lemma 3.3(iii). By Theorem 4.3 of [LP95], we have $\mathsf{G}_{A,\ell}^\circ = \mathrm{MT}_{A,\mathbb{Q}_\ell}$ if and only if the ranks of $\mathsf{G}_{A,\ell}^\circ$ and MT_A are equal. In particular, the Mumford–Tate conjecture for A holds for one prime ℓ if and only if it holds for all ℓ.

4.3. Frobenius compatibility.

Define the field $L := K_A^{\mathrm{conn}}$. For each prime ℓ, we have $\rho_{A,\ell}(\mathrm{Gal}_L) \subseteq \mathsf{G}_{A,\ell}^\circ(\mathbb{Q}_\ell)$. By Proposition 4.4, we have a well-defined Galois representation

$$\mathrm{Gal}_L \xrightarrow{\rho_{A,\ell}} \mathsf{G}_{A,\ell}^\circ(\mathbb{Q}_\ell) \subseteq \mathrm{MT}_A(\mathbb{Q}_\ell).$$

For a nonzero prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_L$ for which A has good reduction, we obtain a conjugacy class $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ in $\mathrm{MT}_A(\mathbb{Q}_\ell)$ and hence a well-defined element $F_{\mathfrak{p},\ell} := \mathrm{cl}_{\mathrm{MT}_A}(\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}))$ in $\mathrm{MT}_A^\sharp(\mathbb{Q}_\ell)$ with notation as in §2.10. Conjecturally, $F_{\mathfrak{p},\ell}$ is an element of $\mathrm{MT}_A^\sharp(\mathbb{Q})$ that is independent of ℓ.

Conjecture 4.5. *Let* $L := K_A^{conn}$ *and let* $\mathfrak{p}$ *be any nonzero prime ideal of* $\mathcal{O}_L$ *for which* A *has good reduction. Then there exists an element* $F_\mathfrak{p} \in MT_A^\sharp(\mathbb{Q})$ *such that* $F_{\mathfrak{p},\ell} = F_\mathfrak{p}$ *for all rational primes* ℓ *satisfying* $\mathfrak{p} \nmid \ell$.

Equivalently, for all primes ℓ *satisfying* $\mathfrak{p} \nmid \ell$ *and all embeddings* $\iota \colon \mathbb{Q}_\ell \to \mathbb{C}$, *the conjugacy class of* $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ *in* $MT_A(\mathbb{C})$, *using the embedding* ι, *does not dependent on the choice of* ℓ *or* ι.

Remark 4.6.

(i) Observe that the image of $F_{\mathfrak{p},\ell}$ under the natural map $MT_A^\sharp(\mathbb{Q}_\ell) \to GL_{V_A}^\sharp(\mathbb{Q}_\ell)$ lies in $GL_{V_A}^\sharp(\mathbb{Q})$ and is independent of ℓ; this is equivalent to the characteristic polynomial $P_{A,\mathfrak{p}}(x)$ of $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ having rational coefficients that do not depend on ℓ. So the above conjecture can be viewed as a strengthening of our earlier notion of compatibility.

(ii) A more general version of Conjecture 4.5 was alluded to in §1 that would work for any good prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ where the motivic Galois group of A takes the role of MT_A, cf. Conjectures 12.6 and 3.4 in [Ser94].

As noted in Remark 1.2, Kisin and Zhou have announced a proof of Conjecture 4.5 when $\mathfrak{p} \nmid 2$. In the meantime, the following partial results of Noot are useful.

Proposition 4.7 (Noot). *Let* $\mathfrak{p}$ *be a nonzero prime ideal of the ring of integers of* K_A^{conn} *for which* A *has good reduction.*

(i) *Suppose that the derived subgroup of* $(MT_A)_{\overline{\mathbb{Q}}}$ *has no direct factor isomorphic to* SO_{2n} *with* $n \geqslant 4$, *and that the quotient of two distinct roots of* $P_{A,\mathfrak{p}}(x)$ *is never a root of unity. Then* $F_{\mathfrak{p},\ell}$ *lies in* $MT^\sharp(\mathbb{Q})$ *and is independent of* ℓ.

(ii) *If* A *has ordinary reduction at* $\mathfrak{p}$, *then* $F_{\mathfrak{p},\ell}$ *is in* $MT_A^\sharp(\mathbb{Q})$ *and is independent of* ℓ. *Moreover, there is a semisimple* $t_\mathfrak{p} \in MT_A(\mathbb{Q})$ *that is conjugate to* $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ *in* $MT_A(\mathbb{Q}_\ell)$ *for all* ℓ *satisfying* $\mathfrak{p} \nmid \ell$.

Proof. We first prove (i). In the notation of [Noo09], we have $\mathrm{Conj}(MT_A) = MT_A^\sharp$ and $\mathrm{Conj}'(MT_A)$ equals $\mathrm{Conj}(MT_A)$ by our assumption on the derived subgroup of $(MT_A)_{\overline{\mathbb{Q}}}$. Part (i) follows from Theorem 1.8 of [Noo09]. Part (ii) follows from Theorem 2.2 of [Noo95]. $\qquad\square$

4.4. **Minuscule representations.** The following proposition gives some constraints on the representation $MT_A \hookrightarrow GL_{V_A}$. For the definition of minuscule, see §2.11.

Proposition 4.8.

(i) *Every irreducible representation* $U \subseteq V_A \otimes_\mathbb{Q} \overline{\mathbb{Q}}$ *of* $(MT_A)_{\overline{\mathbb{Q}}}$ *is minuscule.*

(ii) *Each irreducible component of the root system associated to* MT_A *is of classical type* A_n, B_n, C_n *or* D_n.

Proof. Fix a maximal torus T of MT_A and set $W := W(MT_A, T)$. Note that the algebraic group MT_A and its faithful representation V_A satisfy the assumptions of §3.2 of [Ser79].

Let $\Omega_{V_A} \subseteq X(T)$ be the set of weights of the representation V_A of MT_A. Let $\Omega_{V_A}^+ \subseteq \Omega_{V_A}$ be the set of highest weights of the irreducible representations $U \subseteq V_A \otimes_\mathbb{Q} \overline{\mathbb{Q}}$ of $(MT_A)_{\overline{\mathbb{Q}}}$ with respect to a fixed base of the root system $R \subseteq X(T) \otimes_\mathbb{Z} \mathbb{Q}$ of MT_A.

Take any irreducible representation $U \subseteq V_A \otimes_\mathbb{Q} \overline{\mathbb{Q}}$ of $(MT_A)_{\overline{\mathbb{Q}}}$. Let $\chi \in \Omega_{V_A}^+$ be the highest weight of U; it is the unique element in $\Omega_{V_A}^+ \cap \Omega_U$. We have $W \cdot \chi \subseteq \Omega_U$ since Ω_U is W-stable. Part (i) of the proposition is thus equivalent to showing that $\Omega_{V_A} = W \cdot \Omega_{V_A}^+$. This follows from Proposition 4 of [Ser79].

Part (ii) is a consequence of the corollary to Proposition 7 in [Ser79]. $\qquad\square$

5. Frobenius tori

Fix a nonzero abelian variety A defined over a number field K. Let G be the quasi-split inner form of the Mumford–Tate group MT_A. Consider a representation

$$\rho \colon G_{\overline{\mathbb{Q}}} \xrightarrow{\sim} (MT_A)_{\overline{\mathbb{Q}}} \subseteq GL_{V_A, \overline{\mathbb{Q}}},$$

where the isomorphism is one arising from G being an inner twist of MT_A. In particular, the representation ρ of $G_{\overline{\mathbb{Q}}}$ is well-defined up to isomorphism.

Let $\mathcal{S}_A$ be the set of prime ideals of $\mathcal{O}_K$ from Definition 3.4. For each prime ideal $\mathfrak{p} \in \mathcal{S}_A$, we now show that G has a maximal torus $T_{\mathfrak{p}}$ satisfying some interesting properties.

Theorem 5.1. *Assume that Conjectures 4.3 and 4.5 hold for A. Take any $\mathfrak{p} \in \mathcal{S}_A$ and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{K_A^{\mathrm{conn}}}$ that divides $\mathfrak{p}$. Then there is a semisimple $t_{\mathfrak{p}} \in G(\mathbb{Q})$ satisfying the following properties:*

(a) $\mathrm{cl}_{MT_A}(\rho(t_{\mathfrak{p}})) = F_{\mathfrak{P}}$, with $F_{\mathfrak{P}} \in MT_A^{\sharp}(\mathbb{Q})$ as in Conjecture 4.5,
(b) $t_{\mathfrak{p}}$ lies in a unique maximal torus $T_{\mathfrak{p}}$ of G,
(c) the map

$$(5.1) \qquad\qquad X(T_{\mathfrak{p}}) \to \Phi_{A,\mathfrak{p}}, \quad \alpha \mapsto \alpha(t_{\mathfrak{p}})$$

is a well-defined isomorphism of abelian groups that respects the $\mathrm{Gal}_{\mathbb{Q}}$-actions,
(d) under the isomorphism (5.1), the set $\Omega_{\mathfrak{p}} \subseteq X(T_{\mathfrak{p}})$ of weights of ρ with respect to $T_{\mathfrak{p}}$ corresponds with the set $\mathcal{W}_{A,\mathfrak{p}} \subseteq \Phi_{A,\mathfrak{p}}$ of roots of $P_{A,\mathfrak{p}}(x)$.

5.1. Proof of Theorem 5.1.

Let A' be the base change of A to K_A^{conn}. By Lemma 3.5(ii), we have $\mathfrak{P} \in \mathcal{S}_{A'}$ and $P_{A,\mathfrak{p}}(x) = P_{A',\mathfrak{P}}(x)$. In particular, $\mathcal{W}_{A,\mathfrak{p}} = \mathcal{W}_{A',\mathfrak{P}}$ and $\Phi_{A,\mathfrak{p}} = \Phi_{A',\mathfrak{P}}$. So to prove the theorem, there is no harm in replacing the pair $(A, \mathfrak{p})$ by $(A', \mathfrak{P})$. So without loss of generality, we may assume that $K_A^{\mathrm{conn}} = K$ and hence $\mathfrak{P} = \mathfrak{p}$.

Fix a maximal torus T of G that contains a maximal split torus of G. The torus T has rank r, where r is the common rank of the groups $G_{A,\ell}$ since we are assuming the Mumford–Tate conjecture. Let $\Omega \subseteq X(T)$ be the set of weights of ρ with respect to T.

Define the set

$$B_{\mathfrak{p}} := \{ t \in T(\overline{\mathbb{Q}}) : \mathrm{cl}_{MT_A}(\rho(t)) = F_{\mathfrak{p}} \}.$$

Conjugation induces an action of the Weyl group $W(G, T)$ on $B_{\mathfrak{p}}$.

Lemma 5.2.

(i) The action of $W(G, T)$ on $B_{\mathfrak{p}}$ is simply transitive.
(ii) Every $t_0 \in B_{\mathfrak{p}}$ generates $T_{\overline{\mathbb{Q}}}$ as an algebraic group.
(iii) For each $t_0 \in B_{\mathfrak{p}}$, the map

$$f \colon X(T) \to \Phi_{A,\mathfrak{p}}, \quad \alpha \mapsto \alpha(t_0)$$

is a well-defined group isomorphism that maps Ω to $\mathcal{W}_{A,\mathfrak{p}}$.

Proof. Take any $t_0 \in B_{\mathfrak{p}}$. We have $\mathrm{cl}_{MT_A}(\rho(t_0)) = F_{\mathfrak{p}}$, so the characteristic polynomial of $\rho(t_0)$ is $P_{A,\mathfrak{p}}(x)$. Therefore, $\mathcal{W}_{A,\mathfrak{p}}$ is equal to the set of $\alpha(t_0)$ with $\alpha \in \Omega$. The group $X(T)$ is generated by Ω since $\rho|_T \colon T \hookrightarrow GL_{V_A}$ is an embedding. Therefore, the image of $X(T) \to \overline{\mathbb{Q}}^{\times}$, $\alpha \mapsto \alpha(t_0)$ is generated by $\mathcal{W}_{A,\mathfrak{p}}$. We thus have a well-defined and surjective homomorphism

$$f \colon X(T) \to \Phi_{A,\mathfrak{p}}, \quad \alpha \mapsto \alpha(t_0)$$

that sends Ω to $\mathcal{W}_{A,\mathfrak{p}}$.

The group $X(T)$ is free abelian of rank r. The group $\Phi_{A,\mathfrak{p}}$ is also a free abelian of rank r since $\mathfrak{p}$ is in $\mathcal{S}_A$. Since f is a surjective homomorphism between two free abelian groups of rank r, it must be an isomorphism. This completes the proof of part (iii).

If t_0 did not generate the torus $T_{\overline{\mathbb{Q}}}$, then there would be a nontrivial character $\alpha \in X(T)$ for which $\alpha(t_0) = 1$. Part (ii) is thus an immediate consequence of (iii).

It remains to prove (i). Take any two $t_0, t_1 \in B_{\mathfrak{p}}$. We have $\rho(t_1) = h\rho(t_0)h^{-1}$ for some $h \in \mathrm{MT}_A(\overline{\mathbb{Q}})$ since t_0 and t_1 are semisimple and $\mathrm{cl}_{\mathrm{MT}_A}(\rho(t_0)) = F_{\mathfrak{p}} = \mathrm{cl}_{\mathrm{MT}_A}(\rho(t_1))$. We thus have $t_1 = gt_0g^{-1}$ for the unique $g \in G(\overline{\mathbb{Q}})$ that satisfies $\rho(g) = h$. Since t_1 and t_0 both generate $T_{\overline{\mathbb{Q}}}$ by (ii), we have $T_{\overline{\mathbb{Q}}} = g \cdot T_{\overline{\mathbb{Q}}} \cdot g^{-1}$. So g normalizes $T_{\overline{\mathbb{Q}}}$ and gives rise to an element of $W(G,T)$ that sends t_0 to t_1. The group $W(G,T)$ thus acts transitively on $B_{\mathfrak{p}}$ since t_0 and t_1 were arbitrary elements of $B_{\mathfrak{p}}$.

Finally, we show that $W(G,T)$ acts faithfully on $B_{\mathfrak{p}}$. Suppose that $w \cdot t_0 = t_0$ for some $w \in W(G,T)$ and $t_0 \in B_{\mathfrak{p}}$. By part (ii) this implies that w acts trivially on the torus $T_{\overline{\mathbb{Q}}}$. We thus have $w = 1$ since the group $W(G,T)$ acts faithfully on $T_{\overline{\mathbb{Q}}}$. $\qquad\square$

Lemma 5.3. *If there is an element $t_{\mathfrak{p}} \in G(\mathbb{Q})$ that is conjugate in $G(\overline{\mathbb{Q}})$ to some $t_0 \in B_{\mathfrak{p}}$, then $t_{\mathfrak{p}}$ satisfies all the properties of Theorem 5.1.*

Proof. Assume that there is a $t_{\mathfrak{p}} \in G(\mathbb{Q})$ which satisfies $t_{\mathfrak{p}} = gt_0g^{-1}$ for some $g \in G(\overline{\mathbb{Q}})$ and $t_0 \in B_{\mathfrak{p}}$.

Let $T_{\mathfrak{p}}$ be the algebraic subgroup of G generated by $t_{\mathfrak{p}}$. Using Lemma 5.2(ii), we find that $(T_{\mathfrak{p}})_{\overline{\mathbb{Q}}}$ is a maximal torus of $G_{\overline{\mathbb{Q}}}$; moreover, we have $(T_{\mathfrak{p}})_{\overline{\mathbb{Q}}} = g \cdot T_{\overline{\mathbb{Q}}} \cdot g^{-1}$. Therefore, $T_{\mathfrak{p}}$ is a maximal torus of G. In particular, $t_{\mathfrak{p}}$ is semisimple and $T_{\mathfrak{p}}$ is the unique maximal torus of G containing $t_{\mathfrak{p}}$; this proves that (b) in Theorem 5.1 holds for our $t_{\mathfrak{p}}$.

Using $(T_{\mathfrak{p}})_{\overline{\mathbb{Q}}} = g \cdot T_{\overline{\mathbb{Q}}} \cdot g^{-1}$, we have a group isomorphism $\varphi \colon X(T_{\mathfrak{p}}) \xrightarrow{\sim} X(T)$ satisfying $\varphi(\alpha)(t) = \alpha(gtg^{-1})$ for each $\alpha \in X(T_{\mathfrak{p}})$. Define $f_{\mathfrak{p}} \colon X(T_{\mathfrak{p}}) \xrightarrow{\sim} \Phi_{A,\mathfrak{p}}$ to be the isomorphism $f_{\mathfrak{p}} = f \circ \varphi$ where f is the isomorphism associated to t_0 from Lemma 5.2(iii). For each $\alpha \in X(T_{\mathfrak{p}})$, we have

$$f_{\mathfrak{p}}(\alpha) = f(\varphi(\alpha)) = (\varphi(\alpha))(t_0) = \alpha(gt_0g^{-1}) = \alpha(t_{\mathfrak{p}}).$$

For each $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have $\sigma(f_{\mathfrak{p}}(\alpha)) = \sigma(\alpha(t_{\mathfrak{p}})) = \sigma(\alpha)(t_{\mathfrak{p}}) = f_{\mathfrak{p}}(\sigma(\alpha))$, where we have used that $\sigma(t_{\mathfrak{p}}) = t_{\mathfrak{p}}$ since $t_{\mathfrak{p}} \in G(\mathbb{Q})$. This proves that (c) in Theorem 5.1 holds for our $t_{\mathfrak{p}}$.

Let $\Omega_{\mathfrak{p}} \subseteq X(T_{\mathfrak{p}})$ be the set of weights of ρ with respect to $T_{\mathfrak{p}}$. By Lemma 5.2(iii), we have $f(\Omega) = \mathcal{W}_{A,\mathfrak{p}}$. We have $\varphi(\Omega_{\mathfrak{p}}) = \Omega$ and thus $f_{\mathfrak{p}}(\Omega_{\mathfrak{p}}) = f(\varphi(\Omega_{\mathfrak{p}})) = f(\Omega) = \mathcal{W}_{A,\mathfrak{p}}$. Therefore, part (d) of Theorem 5.1 holds for our $t_{\mathfrak{p}}$.

We have $\rho(t_{\mathfrak{p}}) = \rho(g)\rho(t_0)\rho(g)^{-1}$ and hence $\mathrm{cl}_{\mathrm{MT}_A}(\rho(t_{\mathfrak{p}})) = \mathrm{cl}_{\mathrm{MT}_A}(\rho(t_0))$. Since $t_0 \in B_{\mathfrak{p}}$, we have $\mathrm{cl}_{\mathrm{MT}_A}(\rho(t_{\mathfrak{p}})) = F_{\mathfrak{p}}$. Therefore, part (a) of Theorem 5.1 holds for our $t_{\mathfrak{p}}$. $\qquad\square$

Fix an element $t_0 \in B_{\mathfrak{p}}$. There is a natural action of $\mathrm{Gal}_{\mathbb{Q}}$ on $B_{\mathfrak{p}}$ since T, ρ and $\mathrm{cl}_{\mathrm{MT}_A}$ are defined over $\mathbb{Q}$ and $F_{\mathfrak{p}} \in \mathrm{MT}_A^{\sharp}(\mathbb{Q})$. For any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, Lemma 5.2(i) implies that there is a unique $\xi_{\sigma} \in W(G,T)$ that satisfies $\sigma(t_0) = \xi_{\sigma}^{-1} \cdot t_0$. For $\sigma, \tau \in \mathrm{Gal}_{\mathbb{Q}}$, we have

$$(\sigma\tau)(t_0) = \sigma(\tau(t_0)) = \sigma(\xi_{\tau}^{-1} \cdot t_0) = \sigma(\xi_{\tau})^{-1} \cdot \sigma(t_0) = \sigma(\xi_{\tau})^{-1} \cdot (\xi_{\sigma}^{-1} \cdot t_0) = (\xi_{\sigma}\sigma(\xi_{\tau}))^{-1} \cdot t_0$$

ane hence $\xi_{\sigma\tau} = \xi_{\sigma}\sigma(\xi_{\tau})$. Therefore, the map

$$\xi \colon \mathrm{Gal}_{\mathbb{Q}} \to W(G,T), \quad \sigma \mapsto \xi_{\sigma}$$

is a 1-cocycle.

Lemma 5.4. *There is an element $g \in G(\overline{\mathbb{Q}})$ such that $g^{-1}\sigma(g)$ normalizes $T_{\overline{\mathbb{Q}}}$ and is a representative of ξ_{σ} in $W(G,T)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.*

Proof. Let $p_1 \colon H^1(\mathbb{Q}, N_G(T)) \to H^1(\mathbb{Q}, W(G,T))$ and $p_2 \colon H^1(\mathbb{Q}, N_G(T)) \to H^1(\mathbb{Q}, G)$ be the maps of Galois cohomology sets induced by the natural maps $N_G(T)(\overline{\mathbb{Q}}) \twoheadrightarrow W(G,T)$ and $N_G(T) \hookrightarrow G$. By Proposition 2.6, there is an $x \in H^1(\mathbb{Q}, N_G(T))$ such that $p_1(x) = [\xi]$ and $p_2(x)$ is the trivial class. Here we have used that G is quasi-split and that T contains a maximally split torus in G.

Since $p_2(x)$ is the trivial class, there is an element $g \in G(\overline{\mathbb{Q}})$ such that $x = [\zeta]$, where $\zeta \colon \mathrm{Gal}_{\mathbb{Q}} \to N_G(T)(\overline{\mathbb{Q}})$ is a 1-cocycle satisfying $\zeta_\sigma = g^{-1}\sigma(g)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. In particular, $g^{-1}\sigma(g) = \zeta_\sigma$ is in $N_G(T)(\overline{\mathbb{Q}})$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Let $[g^{-1}\sigma(g)]$ be the image of $g^{-1}\sigma(g)$ in $W(G, T)$. Since $[\xi] = p_1(x) = p_1([\zeta])$, there is an element $w \in W(G, T)$ such that

$$\xi_\sigma = w^{-1} \cdot [g^{-1}\sigma(g)] \cdot \sigma(w)$$

for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Let $\mathfrak{n} \in N_G(T)(\overline{\mathbb{Q}})$ be a representative of w. After replacing g by $g\mathfrak{n}^{-1}$, we may further assume that $w = 1$; the lemma is now immediate. $\qquad\square$

Take $g \in G(\overline{\mathbb{Q}})$ as in Lemma 5.4 and define $t_\mathfrak{p} := g t_0 g^{-1} \in G(\overline{\mathbb{Q}})$. For any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have

$$\sigma(t_0) = \xi_\sigma^{-1} \cdot t_0 = \sigma(g)^{-1} g t_0 g^{-1} \sigma(g)$$

and hence $\sigma(t_\mathfrak{p}) = \sigma(g t_0 g^{-1}) = \sigma(g)\sigma(t_0)\sigma(g)^{-1} = g t_0 g^{-1} = t_\mathfrak{p}$. Since $\sigma(t_\mathfrak{p}) = t_\mathfrak{p}$ holds for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have $t_\mathfrak{p} \in G(\mathbb{Q})$. Theorem 5.1 is now an immediate consequence of Lemma 5.3.

6. Galois groups of Frobenius polynomials

Fix a nonzero abelian variety A over a number field K for which $K_A^{\mathrm{conn}} = K$. Throughout §6, we shall assume that Conjectures 4.3 and 4.5 hold for the abelian variety A.

Let G be the quasi-split inner form of the Mumford–Tate group MT_A. Let $\mathcal{S}_A$ be the set of prime ideals of $\mathcal{O}_K$ from Definition 3.4; it has density 1 by Lemma 3.5(i). For each prime ideal $\mathfrak{p} \in \mathcal{S}_A$, we have a maximal torus $T_\mathfrak{p}$ of G as in Theorem 5.1 generated by a semisimple $t_\mathfrak{p} \in G(\mathbb{Q})$.

Fix a prime ideal $\mathfrak{p} \in \mathcal{S}_A$. With notation as in §2.7, the natural action of $\mathrm{Gal}_{\mathbb{Q}}$ on the group $X(T_\mathfrak{p})$ can be expressed in terms of a representation

$$\varphi_\mathfrak{p} := \varphi_{G, T_\mathfrak{p}} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(\Psi(G, T_\mathfrak{p})) \subseteq \mathrm{Aut}(X(T_\mathfrak{p}))$$

and we have an inclusion $\varphi_\mathfrak{p}(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \Gamma(G, T_\mathfrak{p})$.

Let k_G be the fixed field in $\overline{\mathbb{Q}}$ of the $\ker \mu_G$, where μ_G is defined in §2.7. The field k_G can also be described as the minimal extension of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ for which $\varphi_\mathfrak{p}(\mathrm{Gal}(\overline{\mathbb{Q}}/k_G)) \subseteq W(G, T_\mathfrak{p})$ holds for a fixed $\mathfrak{p} \in \mathcal{S}_A$; note that it does not depend on the choice of prime $\mathfrak{p}$. The splitting field of $T_\mathfrak{p}$ is $\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})$ and hence $k_G \subseteq \mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})$ for all $\mathfrak{p} \in \mathcal{S}_A$. We can similarly define a field k_{MT_A} associated to the Mumford–Tate group of A and it equals k_G by Proposition 2.5.

The following is the main result of this section; it describes the image of $\varphi_\mathfrak{p}$ for all $\mathfrak{p} \in \mathcal{S}_A$ away from a set of density 0.

Theorem 6.1. *Assume that Conjectures 4.3 and 4.5 hold for A. For a fixed number field $k_G \subseteq L \subseteq \overline{\mathbb{Q}}$, we have*

$$\varphi_\mathfrak{p}(\mathrm{Gal}_L) = W(G, T_\mathfrak{p}) \quad \text{and} \quad \varphi_\mathfrak{p}(\mathrm{Gal}_{\mathbb{Q}}) = \Gamma(G, T_\mathfrak{p})$$

for all $\mathfrak{p} \in \mathcal{S}_A$ away from a set of density 0.

The following corollary describes the Galois group of $P_{A,\mathfrak{p}}(x)$ for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

Corollary 6.2. *Assume that Conjectures 4.3 and 4.5 hold for A. For a fixed number field $k_{\mathrm{MT}_A} \subseteq L \subseteq \overline{\mathbb{Q}}$, we have*

$$\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) \cong W(\mathrm{MT}_A) \quad \text{and} \quad \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q}) \cong \Gamma(\mathrm{MT}_A)$$

for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ away from a set of density 0.

Proof. As already noted, we have $k_G = k_{\mathrm{MT}_A}$. For $\mathfrak{p} \in \mathcal{S}_A$, we have $\varphi_\mathfrak{p}(\mathrm{Gal}_L) \cong \mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L)$ and $\varphi_\mathfrak{p}(\mathrm{Gal}_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q})$ since $X(T_\mathfrak{p})$ and $\Phi_{A,\mathfrak{p}}$ are isomorphic $\mathrm{Gal}_{\mathbb{Q}}$-modules by Theorem 5.1 and the group $\Phi_{A,\mathfrak{p}}$ is generated by $\mathcal{W}_{A,\mathfrak{p}}$. Since G and MT_A are inner forms of each other, we have $W(G, T_\mathfrak{p}) \cong W(\mathrm{MT}_A)$ and $\Gamma(G, T_\mathfrak{p}) \cong \Gamma(\mathrm{MT}_A)$. The corollary is now a direct consequence of Theorem 6.1 and $\mathcal{S}_A$ having density 1. $\qquad\square$

6.1. **Proof of Theorem 1.4.** Recall that $G_A^\circ = MT_A$. In the special case where $K_A^{conn} = K$, the theorem is equivalent to Corollary 6.2. We now consider the general case.

Let A' be the base change of A to K_A^{conn}; it has the same Mumford–Tate group. Take any $\mathfrak{p} \in \mathcal{S}_A$ and any prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K_A^{conn}}$ dividing $\mathfrak{p}$. By Lemma 3.5(ii), we have $\mathfrak{P} \in \mathcal{S}_{A'}$ and $P_{A',\mathfrak{P}}(x) = P_{A,\mathfrak{p}}(x)$. In particular, $L(\mathcal{W}_{A,\mathfrak{p}}) = L(\mathcal{W}_{A',\mathfrak{P}})$. Therefore,

$$|\{\mathfrak{p} \in \mathcal{S}_A : N(\mathfrak{p}) \leqslant x, \, \mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) \not\cong W(MT_A)\}|$$
$$\leqslant |\{\mathfrak{p} \in \mathcal{S}_{A'} : N(\mathfrak{P}) \leqslant x, \, \mathrm{Gal}(L(\mathcal{W}_{A',\mathfrak{P}})/L) \not\cong W(MT_A)\}|$$
$$= o(x/\log x)$$

as $x \to \infty$, where we have used that A' satisfies the special case of the theorem already proved. Therefore for all $\mathfrak{p} \in \mathcal{S}_A$ away from a set of density 0, we have $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) \cong W(MT_A)$. The first part of theorem is immediate since $\mathcal{S}_A$ consists of all prime ideals of $\mathcal{O}_K$, away from a set of density 0, that split completely in K_A^{conn}. The proof of the second part of the theorem is identical.

6.2. **Proof of Theorem 6.1.** Since $L \supseteq k_G$, we have $\varphi_\mathfrak{p}(\mathrm{Gal}_L) \subseteq W(G, T_\mathfrak{p})$. From the definition of $\Gamma(G, T_\mathfrak{p})$, the homomorphism $\mathrm{Gal}_\mathbb{Q} \xrightarrow{\varphi_\mathfrak{p}} \Gamma(G, T_\mathfrak{p}) \to \Gamma(G, T_\mathfrak{p})/W(G, T_\mathfrak{p})$ is surjective and hence to prove the theorem it suffices to show that $\varphi_\mathfrak{p}(\mathrm{Gal}_L) = W(G, T_\mathfrak{p})$ for all $\mathfrak{p} \in \mathcal{S}_A$ away from a set of density 0

After possibly replacing L by a finite extension, we may assume that the group G_L is split. Let Λ be the set of primes ℓ that split completely in L. Note that $G_{\mathbb{Q}_\ell}$ is split for all $\ell \in \Lambda$.

Fix a prime $\ell \in \Lambda$. By the Mumford–Tate conjecture, we have $G_{A,\ell} = (MT_A)_{\mathbb{Q}_\ell}$. Since G is the quasi-split inner form of MT_A, the group $G_{\mathbb{Q}_\ell}$ is the quasi-split inner form of $(MT_A)_{\mathbb{Q}_\ell}$. Since $G_{\mathbb{Q}_\ell}$ is split by our choice of ℓ, we deduce that $(MT_A)_{\mathbb{Q}_\ell}$ is split. By the Mumford–Tate conjecture, $G_{A,\ell}$ is also split. Fix a split maximal torus T of $G_{A,\ell}$.

Take any prime ideal $\mathfrak{p} \in \mathcal{S}_A'$ satisfying $\mathfrak{p} \nmid \ell$, where $\mathcal{S}_A'$ is the set of $\mathfrak{p} \in \mathcal{S}_A$ for which $N(\mathfrak{p})$ is prime. Choose an element $t_{\mathfrak{p},\ell} \in T(\overline{\mathbb{Q}}_\ell)$ that is conjugate to $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ in $G_{A,\ell}(\overline{\mathbb{Q}}_\ell)$. As in §5 of [Zyw14], we obtain a homomorphism

$$\psi_{\mathfrak{p},\ell} \colon \mathrm{Gal}_{\mathbb{Q}_\ell} \to W(G_{A,\ell}, T)$$

that is characterized by the property that $\sigma(t_{\mathfrak{p},\ell}) = \psi_{\mathfrak{p},\ell}(\sigma)^{-1}(t_{\mathfrak{p},\ell})$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$. Note that a different choice of $t_{\mathfrak{p},\ell} \in T(\overline{\mathbb{Q}}_\ell)$ would alter $\psi_{\mathfrak{p},\ell}$ by an inner automorphism. A different choice T' of split maximal torus of $G_{A,\ell}$, would give rise to the same homomorphism after first composing with an appropriate isomorphism $W(G_{A,\ell}, T) \xrightarrow{\sim} W(G_{A,\ell}, T')$.

We now relate $\psi_{\mathfrak{p},\ell}$ with our homomorphism $\varphi_\mathfrak{p}$. Choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$; it gives rise to an injective homomorphism $\mathrm{Gal}_{\mathbb{Q}_\ell} = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \mathrm{Gal}_\mathbb{Q}$. We have $\varphi_\mathfrak{p}(\mathrm{Gal}_{\mathbb{Q}_\ell}) \subseteq W(G, T_\mathfrak{p})$ since $\varphi_\mathfrak{p}(\mathrm{Gal}_L) \subseteq W(G, T_\mathfrak{p})$ and ℓ splits completely in L. Let

$$\varphi_{\mathfrak{p},\ell} \colon \mathrm{Gal}_{\mathbb{Q}_\ell} \to W(G)$$

be the homomorphism obtained by composing $\mathrm{Gal}_{\mathbb{Q}_\ell} \hookrightarrow \mathrm{Gal}_\mathbb{Q}$ with $\varphi_\mathfrak{p}$ and an isomorphism $W(G, T_\mathfrak{p}) \xrightarrow{\sim} W(G)$ as described in §2.2.

Lemma 6.3. *For each $\mathfrak{p} \in \mathcal{S}_A'$ satisfying $\mathfrak{p} \nmid \ell$, there is an isomorphism $\beta \colon W(G_{A,\ell}, T) \xrightarrow{\sim} W(G)$ satisfying $\varphi_{\mathfrak{p},\ell} = \beta \circ \psi_{\mathfrak{p},\ell}$. Moreover, one can take the isomorphism β so that, up to composition with an inner automorphism of $W(G)$, it does not depend on $\mathfrak{p}$.*

Proof. Let $\rho \colon G_{\overline{\mathbb{Q}}_\ell} \to (MT_A)_{\overline{\mathbb{Q}}_\ell}$ be an isomorphism arising from G being an inner twist of MT_A. With our fixed $t_\mathfrak{p} \in T_\mathfrak{p}(\mathbb{Q})$ as in Theorem 5.1, we have $\mathrm{cl}_{MT_A}(\rho(t_\mathfrak{p})) = F_\mathfrak{p}$. By Conjecture 4.5, $\rho(t_\mathfrak{p})$ is conjugate to $t_{\mathfrak{p},\ell}$ in $G_{A,\ell}(\overline{\mathbb{Q}}_\ell)$. So by composing ρ with an inner automorphism, we may assume

26

that $\rho(t_{\mathfrak{p}}) = t_{\mathfrak{p},\ell}$. Since the torus $T_{\mathfrak{p}}$ is generated by $t_{\mathfrak{p}}$, we find that ρ restricts to an isomorphism $(T_{\mathfrak{p}})_{\overline{\mathbb{Q}}_\ell} \to T_{\overline{\mathbb{Q}}_\ell}$. We thus have a group isomorphism

$$\rho^* \colon X(T) \xrightarrow{\sim} X(T_{\mathfrak{p}}), \quad \alpha \mapsto \alpha \circ \rho|_{(T_{\mathfrak{p}})_{\overline{\mathbb{Q}}_\ell}}.$$

Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$ and $\alpha \in X(T_{\mathfrak{p}})$. We have $(\varphi_{\mathfrak{p}}(\sigma)\alpha)(t_{\mathfrak{p}}) = \sigma(\alpha)(t_{\mathfrak{p}}) = \sigma(\alpha(t_{\mathfrak{p}}))$ since $t_{\mathfrak{p}} \in T_{\mathfrak{p}}(\mathbb{Q})$. We have $\alpha(t_{\mathfrak{p}}) = \alpha(\rho^{-1}(t_{\mathfrak{p},\ell})) = ((\rho^*)^{-1}(\alpha))(t_{\mathfrak{p},\ell})$. The character $(\rho^*)^{-1}(\alpha)$ in $X(T)$ is fixed by σ since T is a split torus defined over $\mathbb{Q}_\ell$. Therefore,

$$\begin{aligned}
(\varphi_{\mathfrak{p}}(\sigma)\alpha)(t_{\mathfrak{p}}) &= ((\rho^*)^{-1}(\alpha))(\sigma(t_{\mathfrak{p},\ell})) \\
&= ((\rho^*)^{-1}(\alpha))(\psi_{\mathfrak{p},\ell}(\sigma)^{-1} t_{\mathfrak{p},\ell})) \\
&= ((\rho^*)^{-1}(\alpha))(\psi_{\mathfrak{p},\ell}(\sigma)^{-1} \rho(t_{\mathfrak{p}})) \\
&= ((\rho^* \circ \psi_{\mathfrak{p},\ell}(\sigma) \circ (\rho^*)^{-1})(\alpha))(t_{\mathfrak{p}}).
\end{aligned}$$

Since $t_{\mathfrak{p}}$ generates $T_{\mathfrak{p}}$ and $\alpha \in X(T_{\mathfrak{p}})$ was arbitrary, we deduce that $\varphi_{\mathfrak{p}}(\sigma) = \rho^* \circ \psi_{\mathfrak{p},\ell}(\sigma) \circ (\rho^*)^{-1}$ holds for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$. The isomorphism $N_{G_{A,\ell}}(T)(\overline{\mathbb{Q}}_\ell) \to N_G(T_{\mathfrak{p}})(\overline{\mathbb{Q}}_\ell)$ given by $n \mapsto \rho^{-1}(n)$ induces an isomorphism $\beta \colon W(G_{A,\ell}, T) \to W(G, T_{\mathfrak{p}})$.

Take any $n \in N_{G_{A,\ell}}(T)(\overline{\mathbb{Q}}_\ell)$ and let $w := [n]$ be its image in $W(G_{A,\ell}, T)$. For any $\alpha \in X(T_{\mathfrak{p}})$ and $t \in T_{\mathfrak{p}}(\overline{\mathbb{Q}}_\ell)$, we have

$$((\rho^* \circ w \circ (\rho^*)^{-1})(\alpha))(t) = \alpha(\rho^{-1}(n^{-1}\rho(t)n)) = \alpha((\rho^{-1}(n))^{-1} t \, \rho^{-1}(n)) = (\beta(w)(\alpha))(t).$$

Since α and t were arbitrary, we deduce that $\rho^* \circ w \circ (\rho^*)^{-1} = \beta(w)$ for all $w \in W(G_{A,\ell}, T)$. In particular, we have $\varphi_{\mathfrak{p}}(\sigma) = \beta(\psi_{\mathfrak{p},\ell}(\sigma))$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$. The last statement in the lemma follows by noting that in the proof, we only changed ρ by composition with an inner automorphism. $\qquad\square$

Let $\bar{\rho}_{A,\ell} \colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{F}_\ell}(A[\ell])$ be the representation describing the Galois action on the ℓ-torsion points of A.

Lemma 6.4. *Take any subset C of $W(G)$ that is stable under conjugation. Take any prime $\ell \in \Lambda$. There is a subset U_ℓ of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation and satisfies the following properties:*

- *If $\mathfrak{p} \in S_A'$ satisfies $\mathfrak{p} \nmid \ell$ and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \subseteq U_\ell$, then $\varphi_{\mathfrak{p},\ell}$ is unramified and $\varphi_{\mathfrak{p},\ell}(\mathrm{Frob}_\ell) \subseteq C$.*
- *Let K' be a finite extension of K and let κ be a subset of Gal_K that consists of a union of cosets of $\mathrm{Gal}_{K'}$. Then we have*

$$\frac{|\bar{\rho}_{A,\ell}(\kappa) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\kappa)|} = \frac{|C|}{|W(G)|} + O(1/\ell)$$

where the implicit constant depends only on A and K'.

Proof. By excluding a finite number of ℓ, one can assume that the group scheme $\mathcal{G}_{A,\ell}$ of §5 of [Zyw14] is a split reductive group scheme (we can take $U_\ell = \emptyset$ and adjust the implicit constant appropriately to deal with these excluded primes). We may assume that our split torus T of $G_{A,\ell}$ is chosen to be the generic fiber of a split maximal torus of $\mathcal{G}_{A,\ell}$.

Take any subset C' of $W(G_{A,\ell}, T)$ that is stable under conjugation. Lemma 5.1 of [Zyw14] implies that Then there is a subset U_ℓ of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation and satisfies the following:

- *If $\mathfrak{p} \in S_A'$ satisfies $\mathfrak{p} \nmid \ell$ and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \subseteq U_\ell$, then $\psi_{\mathfrak{p},\ell}$ is unramified and $\psi_{\mathfrak{p},\ell}(\mathrm{Frob}_\ell) \subseteq C'$.*
- *Let K' be a finite extension of K and let κ be a subset of Gal_K that consists of a union of cosets of $\mathrm{Gal}_{K'}$. Then we have*

$$\frac{|\bar{\rho}_{A,\ell}(\kappa) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\kappa)|} = \frac{|C'|}{|W(G_{A,\ell}, T_0)|} + O(1/\ell),$$

27

where the implicit constant depends only on A and K'.

The lemma is now an immediate consequence of Lemma 6.3 by taking $C' := \beta^{-1}(C)$. $\qquad\square$

Serre proved that there is a finite Galois extension K'/K such that $(\prod_\ell \rho_{A,\ell})(\mathrm{Gal}_{K'})$ equals $\prod_\ell \rho_{A,\ell}(\mathrm{Gal}_{K'})$ where the products are over all primes ℓ, cf. [Ser00, #138]. The following is Proposition 2.12 of [Zyw14].

Lemma 6.5. *Let Λ_0 be a finite set of rational primes. For each prime $\ell \in \Lambda_0$, fix a subset U_ℓ of the group $\bar\rho_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation. Then the set of all nonzero primes ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ for which $\bar\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \subseteq U_\ell$ for all $\ell \in \Lambda_0$ has density*

$$\sum_C \frac{|C|}{|\mathrm{Gal}(K'/K)|} \cdot \prod_{\ell \in \Lambda_0} \frac{|\bar\rho_{A,\ell}(\Gamma_C) \cap U_\ell|}{|\bar\rho_{A,\ell}(\Gamma_C)|},$$

where C varies over the conjugacy classes of $\mathrm{Gal}(K'/K)$ and Γ_C is the set of $\sigma \in \mathrm{Gal}_K$ for which $\sigma|_{K'} \in C$.

For $\mathfrak{p} \in \mathcal{S}_A$, we know that $\varphi_\mathfrak{p}(\mathrm{Gal}_L) \subseteq W(G, T_\mathfrak{p})$. Let $\varphi'_\mathfrak{p} \colon \mathrm{Gal}_L \to W(G)$ be the homomorphism obtained by composing $\varphi_\mathfrak{p}$ with an isomorphism $W(G, T_\mathfrak{p}) \cong W(G)$ as in §2.2. It thus remains to show that $\varphi'_\mathfrak{p}(\mathrm{Gal}_L) = W(G)$ for all $\mathfrak{p} \in \mathcal{S}_A$ away from a set of density 0.

Take any conjugacy class C of $W(G)$. Define the set

$$\mathcal{B}_C = \{\mathfrak{p} \in \mathcal{S}'_A : \varphi'_\mathfrak{p}(\mathrm{Gal}_L) \cap C = \emptyset\}.$$

Fix an $x \geqslant 2$. Let $\Lambda(x)$ be the set of $\ell \in \Lambda$ satisfying $\ell \leqslant x$. For each $\ell \in \Lambda$, let U_ℓ be the subset of $\bar\rho_{A,\ell}(\mathrm{Gal}_K)$ as in Lemma 6.4.

Take any prime $\mathfrak{p} \in \mathcal{B}_C$ not dividing one of the finite number of primes in $\Lambda(x)$. Suppose that $\bar\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \subseteq U_\ell$ for some $\ell \in \Lambda(x)$. Then $\varphi_{\mathfrak{p},\ell}$ is unramified at ℓ and satisfies $\varphi_{\mathfrak{p},\ell}(\mathrm{Frob}_\ell) \subseteq C$ by our choice of U_ℓ. Since ℓ splits completely in L, we deduce that $\varphi'_\mathfrak{p}(\mathrm{Gal}_L)$ contains an element in the conjugacy class C. However, this is contradicts that $\mathfrak{p} \in \mathcal{B}_C$. Therefore, $\bar\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \not\subseteq U_\ell$ for all $\ell \in \Lambda(x)$ and all $\mathfrak{p} \in \mathcal{B}_C$ that do not divide any of the finitely many primes in $\Lambda(x)$.

Using Lemma 6.5, we deduce that the set $\mathcal{B}_C$ is contained in a set of primes that has density

$$\delta(x) := \sum_\kappa \frac{|\kappa|}{|\mathrm{Gal}(K'/K)|} \cdot \prod_{\ell \in \Lambda(x)} \frac{|\bar\rho_{A,\ell}(\Gamma_\kappa) \cap (\bar\rho_{A,\ell}(\mathrm{Gal}_K) - U_\ell)|}{|\bar\rho_{A,\ell}(\Gamma_\kappa)|}$$

$$= \sum_\kappa \frac{|\kappa|}{|\mathrm{Gal}(K'/K)|} \cdot \prod_{\ell \in \Lambda(x)} \left(1 - \frac{|\bar\rho_{A,\ell}(\Gamma_\kappa) \cap U_\ell|}{|\bar\rho_{A,\ell}(\Gamma_\kappa)|}\right),$$

where κ varies over the conjugacy classes of $\mathrm{Gal}(K'/K)$ and Γ_κ is the set of $\sigma \in \mathrm{Gal}_K$ for which $\sigma|_{K'} \in \kappa$.

We may assume that $|C|/|W(G)| < 1$ since otherwise $W(G) = 1$ and the theorem is immediate. Choose $\varepsilon > 0$ such that $1 - |C|/|W(G)| + \varepsilon < 1$. Then by using the cardinality estimates from Lemma 6.4, we have

$$\delta(x) = O\left((1 - |C|/|W(G)| + \varepsilon)^{|\Lambda(x)|}\right),$$

where the implicit constant depends on A, K', L and ε. Since $0 < 1 - |C|/|W(G)| + \varepsilon < 1$, we have $\delta(x) \to 0$ as $x \to +\infty$. Therefore, the set $\mathcal{B}_C$ has density 0.

Take any prime ideal $\mathfrak{p} \in \mathcal{S}'_A - (\cup_C \mathcal{B}_C)$, where the union is over the set of conjugacy classes C of $W(G)$. By our choice of $\mathfrak{p}$, $\varphi'_\mathfrak{p}(\mathrm{Gal}_L)$ is a subgroup of $W(G)$ that satisfies $\varphi'_\mathfrak{p}(\mathrm{Gal}_L) \cap C \neq \emptyset$ for all conjugacy classes C of $W(G)$. By Jordan's lemma [Ser03, Theorem 4'], we deduce that $\varphi'_\mathfrak{p}(\mathrm{Gal}_L) = W(G)$. It thus suffices to show that $\mathcal{S}'_A - (\cup_C \mathcal{B}_C)$ has density 1. This is clear since the sets $\mathcal{B}_C$ have density 0, the set $\mathcal{S}_A$ has density 1, and the set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ with $N(\mathfrak{p})$ a prime has density 1.

Fix a field k of characteristic 0 and an algebraic closure $\bar{k}$. Let G be a connected reductive group defined over k. Let

$$\rho \colon G \to \mathrm{GL}_V$$

be a representation whose kernel is a subgroup of the center of G, where V is a finite dimensional k-vector space. Fix a maximal torus T of G. For every representation $U \subseteq V \otimes_k \bar{k}$ of $G_{\bar{k}}$, denote by $\Omega_U \subseteq X(T)$ the set of weights of $T_{\bar{k}}$ acting on U.

Assume further that every irreducible representation $U \subseteq V \otimes_k \bar{k}$ of $G_{\bar{k}}$ is minuscule, i.e., the Weyl group $W(G, T)$ acts transitively on Ω_U. We will later apply the results of this section to the representation from Proposition 4.8.

Let $R(G, T) \subseteq X(T)$ be the set of roots of G relative to T. The goal of this section is describe how one can compute $R(G, T)$ directly from the action of $W(G, T)$ on $X(T)$ and the set Ω_V.

For each $W(G, T)$-orbit $\Omega \subseteq \Omega_V$, define the subset

$$C_\Omega := \{\alpha\beta^{-1} : \alpha, \beta \in \Omega, \alpha \neq \beta\}.$$

of $X(T)$. The set C_Ω is stable under the action of $W(G, T)$ on $X(T)$. The following algorithm will produce a sequence of nonempty finite subsets $S_1, \ldots, S_s$ of $X(T)$; it will terminate since the finite sets U_i that arise have strictly decreasing cardinality.

Algorithm 7.1.

(1) *Set $i = 1$ and define $U_1 := \bigcup_\Omega C_\Omega$, where Ω runs over the $W(G, T)$-orbits in Ω_V. If $U_1 = \emptyset$, then we take $s = 0$ and terminate the algorithm.*

(2) *Choose a $W(G, T)$-orbit O of U_i that has minimal cardinality. Choose a $W(G, T)$-orbit $\Omega \subseteq \Omega_V$ for which $O \subseteq C_\Omega$.*

(3) *Define S_i to be the set of elements of C_Ω that lie in the span of O in $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

(4) *Let U_{i+1} be the set of elements of U_i that are not in the span of $S_1 \cup \cdots \cup S_i$ in $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

(5) *If $U_{i+1} \neq \emptyset$, then increase i by 1 and go back to step (2).*

The following shows that the sets S_i are related to the irreducible components of $R(G, T)$.

Proposition 7.2. *For each $1 \leqslant i \leqslant s$, there is a unique irreducible component R_i of the root system $R(G, T) \subseteq X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ with $R_i \subseteq S_i$. Moreover,*

$$R(G, T) = \bigcup_{1 \leqslant i \leqslant s} R_i$$

is a disjoint union that gives the decomposition of $R(G, T)$ into irreducible root systems.

We now explain how to compute the Lie type of the irreducible root systems R_i. Take any $1 \leqslant i \leqslant s$. Let W_i be the quotient of $W(G, T)$ that acts faithfully on S_i. Let r_i be the dimension of the span of S_i in $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 7.3. *Fix an $1 \leqslant i \leqslant s$. Set $r := r_i$ and $W := W_i$.*

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

(ii) *If $r \geqslant 3$, then R_i has type B_r if and only if $|W| = 2^r r!$ and S_i consists of at least three W-orbits.*

(iii) *If $r \geqslant 2$, then R_i has type C_r if and only if $|W| = 2^r r!$ and S_i consists of two W-orbits.*

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

(v) *If $r = 6$, then R_i has type E_6 if and only if $|W| = 51840$.*

(vi) *If $r = 7$, then R_i has type E_7 if and only if $|W| = 2903040$.*

(vii) *The root system R_i is not of any of the following types: G_2, F_4, E_8.*

Remark 7.4. Note that Proposition 7.3 determines the Lie type of each R_i. The conditions on r are imposed to avoid the ambiguity of the exceptional isomorphisms $A_1 = B_1 = C_1$, $B_2 = C_2$ and $A_3 = D_3$.

The following proposition shows how one can determine R_i as a subset of $\mathcal{S}_i$ by considering the action of $W(G, T)$ on $\mathcal{S}_i$ (with the type of R_i being computable by Proposition 7.3).

Proposition 7.5. *Fix an* $1 \leqslant i \leqslant s$. *Set* $r := r_i$, $W := W_i$ *and* $\mathcal{S} := \mathcal{S}_i$.

    (i) If $r \geqslant 1$ *and* R_i *is of type* A_r, *then* R_i *is the unique* W-*orbit of* $\mathcal{S}$ *of cardinality* $r(r + 1)$.
    (ii) If $r \geqslant 3$ *and* R_i *is of type* B_r, *then* R_i *is the union of the unique* W-*orbits of* $\mathcal{S}$ *of cardinality* $2r$ *and* $2r(r - 1)$.
    (iii) If $r \geqslant 2$ *and* R_i *is of type* C_r, *then* $R_i = \mathcal{S}$.
    (iv) If $r \geqslant 4$ *and* R_i *is of type* D_r, *then* R_i *is the unique* W-*orbit of* $\mathcal{S}$ *with cardinality* $2r(r - 1)$.
    (v) If R_i *is of type* E_6, *then* R_i *is the unique* W-*orbit of* $\mathcal{S}$ *with cardinality* 72.
    (vi) If R_i *is of type* E_7, *then* R_i *is the unique* W-*orbit of* $\mathcal{S}$ *with cardinality* 126.

Using Propositions 7.2, 7.3 and 7.5, we find that the set of roots $R(G, T)$ can be computed from the set of weights $\Omega_V \subseteq X(T)$ and the action of $W(G, T)$ on $X(T)$.

7.1. **Proof of Propositions 7.2, 7.3 and 7.5.** Without loss of generality, we may assume that k is algebraically closed. In this proof, we will view $X(T)$ and all the other character groups that arise as additive groups. For example, C_Ω is now the set of $\alpha - \beta$ with distinct $\alpha, \beta \in \Omega$. Additive notation will make it notational easier to work with the $\mathbb{R}$-vector space $X(T)_{\mathbb{R}} := X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ and the $\mathbb{Q}$-vector space $X(T)_{\mathbb{Q}} := X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$.

In §7.1.1, we will prove the three propositions under additional assumptions. The general case will be considered in §7.1.2 where we will reduce to the special case considered in §7.1.1.

7.1.1. *Special case.* Throughout §7.1.1, we further suppose that G is semisimple and almost simple, and that the representation ρ is irreducible. By *almost simple*, we mean that the quotient of G by its (finite) center is a simple algebraic group.

To ease notation, set $W := W(G, T)$ and $X := X(T)$. Let r be the rank of G. Since G is almost simple, the root system $R := R(G, T)$ in $X_{\mathbb{R}} := X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ is irreducible.

Lemma 7.6. *The representation* $X_{\mathbb{R}}$ *of the group* W *is irreducible. The subspace of* $X_{\mathbb{R}}$ *fixed by* W *is* 0.

Proof. Take any subspace $\mathcal{V} \subseteq X_{\mathbb{R}}$ stable under the action of W. Let $(\,,\,)$ be an inner product on $X_{\mathbb{R}}$ that is invariant under the action of W. Let $\mathcal{V}^{\perp}$ be the orthogonal complement of $\mathcal{V}$ with respect to this inner product. For any root $\alpha \in R$, the reflection s_α of $X_{\mathbb{R}}$ defined by $s_\alpha(\nu) = \nu - (\nu, \alpha)/(\alpha, \alpha) \cdot \alpha$ lies in W.

Take any root $\alpha \in R$ not in $\mathcal{V}^{\perp}$; we have $(\nu, \alpha) \neq 0$ for some $\nu \in \mathcal{V}$. Therefore, $\alpha = (\alpha, \alpha)/(\nu, \alpha) \cdot (s_\alpha(\nu) - \nu)$ is an element of $\mathcal{V}$, where we have used that $\mathcal{V}$ is stable under the action of W.

Therefore, every root $\alpha \in R$ either lies in $\mathcal{V}$ or $\mathcal{V}^{\perp}$. That R is an irreducible root system in $X_{\mathbb{R}}$ implies that $\mathcal{V} = 0$ or $\mathcal{V} = X_{\mathbb{R}}$. This implies that $X_{\mathbb{R}}$ is an irreducible representation of W.

Finally, suppose $X_{\mathbb{R}}^W \neq 0$. Since $X_{\mathbb{R}}$ is an irreducible representation of W, we deduce that W acts trivially on $X_{\mathbb{R}}$ which contradicts that W acts faithfully on X. Therefore, $X_{\mathbb{R}}^W = 0$. $\square$

Lemma 7.7. *Algorithm* 7.1 *terminates with* $s = 1$. *We have*

$$\mathcal{S}_1 = C_{\Omega_V} = \{\alpha - \beta : \alpha, \beta \in \Omega_V, \alpha \neq \beta\}$$

and $\mathcal{S}_1$ *spans* $X_{\mathbb{R}}$.

Proof. Since V is irreducible, it must be a minuscule representation of G by our assumption on ρ. Therefore, W acts transitively on Ω_V. So in Algorithm 7.1, we have $\mathcal{U}_1 = C_{\Omega_V}$.

We have $|\Omega_V| > 1$ since ρ is irreducible and it image is a nontrivial semisimple group (by assumption the kernel of ρ is central). Since $|\Omega_V| > 1$, we find that $\mathcal{U}_1$ is nonempty. Choose any W-orbit $\mathcal{O}$ of $\mathcal{U}_1$ that has minimal cardinality. We have $\mathcal{O} \subseteq C_{\Omega_V}$ and Ω_V is a transitive W-set.

Let $\mathcal{V}$ be the span of $\mathcal{O}$ in $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$. The set $\mathcal{O}$, and hence also the vector space $\mathcal{V}$, is stable under the action of W. Since $\mathcal{O} \neq \{0\}$, we must have $\mathcal{V} = X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ by Lemma 7.6. So the set $\mathcal{S}_1$ of elements in C_{Ω_V} that lie in $\mathcal{V}$ is simply C_{Ω_V}. Since $\mathcal{O} \subseteq C_{\Omega_V}$, we find that $\mathcal{S}_1$ spans $\mathcal{V} \otimes_{\mathbb{Q}} \mathbb{R} = X_{\mathbb{R}}$.

Let $\mathcal{U}_2$ be the set of elements of $\mathcal{U}_1$ that are not in the span of $\mathcal{S}_1$ in $\mathcal{V}$; it is empty. The lemma follows by applying Algorithm 7.1 with the above computations. $\square$

Since $\mathcal{S}_1$ spans $X_{\mathbb{R}}$, the quotient W_1 of W that acts faithfully on $\mathcal{S}_1$ is simply W. The dimension r_1 of the span of $\mathcal{S}_1$ in $X_{\mathbb{R}}$ is equal to r. Therefore, $W_1 = W$ and $r_1 = r$. We set $\mathcal{S} := \mathcal{S}_1$.

Since $R \subseteq X_{\mathbb{R}}$ is an irreducible root system, it must be isomorphic to precisely one of the following:

(7.1) $\qquad A_r, \quad B_r \ (r \geqslant 3), \quad C_r \ (r \geqslant 2), \quad D_r \ (r \geqslant 4), \quad E_6, \quad E_7, \quad E_8, \quad F_4, \quad G_2;$

note that the constraints on r are added to avoid exceptional isomorphisms. See [Bou68] for a description of these irreducible root systems.

Once a choice of positive roots R^+ of $R \subseteq X_{\mathbb{R}}$ has been made, the irreducible representation ρ of G will have a highest weight $\varpi \in \Omega_V \subseteq X_{\mathbb{R}}$. The actual choice of positive roots does not matter for us since we are interested in the set of weights

$$\Omega_V = W \cdot \varpi;$$

recall W acts transitively on Ω_V since the representation V is irreducible and hence minuscule.

We can now assume that the root system R is one of (7.1) with explicit definitions as in [Bou68, Planche I–VI, p. 250–266]. Bourbaki chooses a set of positive roots R^+ and [Bou75, VIII, §7, no. 3] then gives all highest weights that could arise from a nontrivial irreducible minuscule representation. This data has been collected in Table 1 below.

For each irreducible root system, we give the highest weights of irreducible minuscule representations with notation as in [Bou68, Planche I–VI]; for the classical types, we will later express these weights in terms of roots. Note that the root systems G_2, F_4 and E_8 do not have minuscule weights. In Table 1, we also given the dimension of the corresponding representation and the order of the Weyl group.

root system	A_r	B_r	C_r	D_r	D_r	E_6	E_7
highest weight	$\varpi_s \ (1 \leqslant s \leqslant r)$	ϖ_r	ϖ_1	ϖ_1	ϖ_{r-1}, ϖ_r	ϖ_1, ϖ_6	ϖ_7
dimension	$\binom{r+1}{s}$	2^r	$2r$	$2r$	2^{r-1}	27	56
$|W|$	$(r+1)!$	$2^r r!$	$2^r r!$	$2^{r-1} r!$	$2^{r-1} r!$	51840	2903040

TABLE 1. Irreducible root systems and minuscule weights.

The proof of the propositions, in the special setting of §7.1.1, can now be reduced to verifying the cases from Table 1. For each of the root systems R and highest weight ϖ occurring in Table 1, we compute

$$\Omega := W \cdot \varpi,$$

where W is the Weyl group of R. Now define

$$\mathcal{S} := \{\alpha - \beta : \alpha, \beta \in \Omega, \ \alpha \neq \beta\}.$$

Case by case, we will check below that R can be determined from the action of W on $\mathcal{S}$ as stated in Proposition 7.5. Also we will verify that $\mathcal{S}$ has two W-orbits when $R = C_r \ (r \geqslant 2)$ and at least three

W-orbits when $R = B_r$ $(r \geqslant 3)$. This will complete the proof of Proposition 7.5 in the special case of §7.1.1. Since $s = 1$ and $R \subseteq \mathcal{S}$, this will also complete the proof of Proposition 7.2 in the setting of §7.1.1.

Finally, Proposition 7.3 in the setting of §7.1.1 is now immediate; note that r as given and $|W|$ will distinguish the cases except for B_r and C_r.

- **Case 1: $R = A_r$ $(r \geqslant 1)$.**

Let $\mathcal{V}$ be the subspace of $\mathbb{R}^{r+1}$ consisting of $x \in \mathbb{R}^{r+1}$ satisfying $\sum_{i=1}^{r+1} x_i = 0$. Let $e_1, \ldots, e_{r+1}$ be the standard basis of $\mathbb{R}^{r+1}$. Then

$$R = \{e_i - e_j : i \neq j\}$$

is a root system of type A_r in $\mathcal{V}$. The Weyl group W acts on $e_1, \ldots, e_{r+1}$ by all permutations.

We have $\varpi_s = (e_1 + \cdots + e_s) - \frac{s}{r+1}(e_1 + \cdots + e_{r+1})$ for an integer $1 \leqslant s \leqslant r$. Therefore,

$$\Omega := W\varpi_s = \left\{ \sum_{i \in I} e_i - \frac{s}{r+1}(e_1 + \cdots + e_{r+1}) : I \subseteq \{1, \ldots, r+1\}, |I| = s \right\}.$$

One can verify that the set $\mathcal{S}$ consists of

$$(7.2) \qquad \alpha = \sum_{i \in I} e_i - \sum_{j \in J} e_j$$

with I and J disjoint subsets of $\{1, \ldots, r+1\}$ of equal cardinality m, where $1 \leqslant m \leqslant r+1-s$. The W-orbit of $\alpha \in \mathcal{S}$ given by (7.2) depends only on m and has cardinality

$$\binom{r+1}{m}\binom{r+1-m}{m} = \frac{(r+1)!}{(r+1-m)!m!}\frac{(r+1-m)!}{(r+1-2m)!m!} = \binom{r+1}{2m}\binom{2m}{m}.$$

It is a straightforward exercise to verify that $\binom{r+1}{2m}\binom{2m}{m} \neq \binom{r+1}{2}\binom{2}{1} = r(r+1)$ for all $1 < m \leqslant r$; in fact, we have $\binom{r+1}{2m}\binom{2m}{m} > \binom{r+1}{2}\binom{2}{1}$ whenever $r \geqslant 6$. Therefore, R is the unique W-orbit in $\mathcal{S}$ of cardinality $r(r+1)$.

- **Case 2: $R = B_r$ $(r \geqslant 3)$.**

Let $e_1, \ldots, e_r$ be the standard basis of $\mathbb{R}^r$. Then

$$R = \{\pm e_i\} \cup \{\pm e_i \pm e_j : i < j\}$$

is a root system of type B_r in $\mathbb{R}^r$. The Weyl group W acts on $\pm e_1, \ldots, \pm e_r$ via signed permutations. Note that R is the union of two W-orbits with cardinality $2r$ and $2r(r-1)$.

We have $\varpi_r = \frac{1}{2}(e_1 + \cdots + e_r)$ and hence

$$\Omega := W\varpi_r = \left\{ \tfrac{1}{2}(\pm e_1 \pm \cdots \pm e_r) \right\}.$$

The set $\mathcal{S}$ consists of elements of the form $\alpha := \sum_{i \in I} \varepsilon_i e_i$, where I is a nonempty subset of $\{1, \ldots, r\}$ and $\varepsilon_i \in \{\pm 1\}$. Note that the W-orbit $W\alpha$ depends only on $m := |I| \geqslant 1$ and we have

$$|W\alpha| = \binom{r}{m} \cdot 2^m.$$

Using $1 \leqslant m \leqslant r$, it is a straightforward exercise to show that $m = 1$ and $m = 2$ give the unique W-orbits in $\mathcal{S}$ of cardinality $2r$ and $2r(r-1)$, respectively. Therefore, R is the union of the W-orbits with $m = 1$ and $m = 2$. Finally, observe that $\mathcal{S}$ consists of precisely r orbits of W; they are indexed by $1 \leqslant m \leqslant r$.

- **Case 3: $R = C_r$ $(r \geqslant 2)$.**

Let $e_1, \ldots, e_r$ be the standard basis of $\mathbb{R}^r$. Then

$$R = \{\pm e_i \pm e_j : i < j\} \cup \{\pm 2e_i\}$$

is a root system of type C_r in $\mathbb{R}^r$. The Weyl group W acts on $\pm e_1, \dots, \pm e_r$ via signed permutations. Note that R is the union of two W-orbits with cardinality $2r$ and $2r(r-1)$.

We have $\varpi_1 = e_1$ and hence
$$\Omega := W \cdot \varpi_1 = \{\pm e_1, \dots, \pm e_r\}.$$
In this case, one can check directly that $S = \{\alpha - \beta : \alpha, \beta \in \Omega, \ \alpha \neq \beta\}$ equals R. Observe that $S = R$ consists of two W-orbits.

- **Case 4: $R = D_r$ $(r \geqslant 4)$ and highest weight ϖ_1.**
  Let $e_1, \dots, e_r$ be the standard basis of $\mathbb{R}^r$. Then
  $$R = \{\pm e_i \pm e_j : i < j\}$$
  is a root system of type D_r in $\mathbb{R}^r$. The Weyl group W acts on $\pm e_1, \dots, \pm e_r$ via signed permutations that only change an even number of signs.

  We are considering the minuscule weight ϖ_1 in this case. We have $\varpi_1 = e_1$ and hence
  $$\Omega := W \cdot \varpi_1 = \{\pm e_1, \dots, \pm e_r\}.$$
  The set S is the union of two W-orbits $\{\pm e_i \pm e_j : i < j\}$ and $\{\pm 2e_i\}$ which have cardinality $2r(r-1)$ and $2r$, respectively. Therefore, R is the unique W-orbit in S of cardinality $2r(r-1)$.

- **Case 5: $R = D_r$ $(r \geqslant 4)$ and highest weight ϖ_{r-1} or ϖ_r.**
  Let $e_1, \dots, e_r$ be the standard basis of $\mathbb{R}^r$. Then
  $$R = \{\pm e_i \pm e_j : i < j\}$$
  is a root system of type D_r in $\mathbb{R}^r$. The Weyl group W acts on $\pm e_1, \dots, \pm e_r$ via signed permutations that only change an even number of signs.

  We are considering a minuscule weight $\varpi \in \{\varpi_{r-1}, \varpi_r\}$ in this case. We have
  $$\varpi = \frac{1}{2}(e_1 + \cdots + e_{r-1} + \varepsilon e_r),$$
  where $\varepsilon = -1$ if $\varpi = \varpi_{r-1}$ and $\varepsilon = 1$ if $\varpi = \varpi_r$. Therefore,
  $$\Omega := W\varpi = \left\{(\varepsilon_1 e_1 + \cdots + \varepsilon_r e_r)/2 : \varepsilon_i \in \{\pm 1\}, \ \prod_i \varepsilon_i = \varepsilon\right\}.$$
  One can check that S consists of elements of the form
  $$\alpha := \sum_{i \in I} \varepsilon_i e_i$$
  with $\varepsilon_i \in \{\pm 1\}$, where I is a nonempty subset of $\{1, \dots, r\}$ of *even* cardinality, and $\prod_{i=1}^r \varepsilon_i = \varepsilon$ if $I = \{1, \dots, r\}$.

  Note that the W-orbit $W\alpha$ depends only on the even integer $m := |I| \geqslant 1$. We have
  $$|W\alpha| = \binom{r}{m} 2^m$$
  if $m < r$ and $|W\alpha| = 2^{r-1}$ if $m = r$. Using that $1 \leqslant m \leqslant r$ is even, it is a straightforward exercise to show there is a unique W-orbit in S of cardinality $\binom{r}{2} 2^2 = 2r(r-1)$. This orbit is $\{\pm e_i \pm e_i : i < j\} = R$.

- **Case 6: $R = E_6$ or $R = E_7$.**
  This case is a direct and not particularly interesting computation. We have also used `Magma` [BCP97], which contains the information on the irreducible root systems from Bourbaki [Bou68], to verify this case.

  The following `Magma` code checks the E_7 case; it shows that S is the union of W-orbits of cardinality 56, 126 and 756, and that R is the W-orbit of cardinality 126.

```
RR:=RootSystem("E7");
R:=Roots(RR);
W:=ReflectionGroup(RR);
DynkinDiagram(RR); // same numbering as Bourbaki!

// minuscule highest weight from Bourbaki in terms of simple roots
pi:=Vector([2/2,3/2,4/2,6/2,5/2,4/2,3/2]);
Omega:=pi^W;
S:={a-b : a,b in Omega | a ne b};
while #S ne 0 do
        O:=Rep(S)^W;
        print #O, O eq R;
        S:=S diff O;
end while;
```

The two E_6 cases are computed in the same manner. Besides replacing "E7" with "E6" in the above code, one also uses one of the two vectors $(4/3, 3/3, 5/3, 6/3, 4/3, 2/3)$ and $(2/3, 3/3, 4/3, 6/3, 5/3, 4/3)$; they are the coordinates of ϖ_1 and ϖ_6 with respect to the simple roots as chosen in [Bou68, Planche V]. In both cases, we find that S is the union of two W-orbits of cardinality 72 and 270. The set R is the orbit with 72 elements.

Remark 7.8. Due to Proposition 4.8(ii), we know that the E_6 and E_7 cases will not occur in our application to Mumford–Tate groups of abelian varieties.

7.1.2. *General case.* We now consider the general case. The goal is to reduce to the special case of §7.1.1.

Let G_0 be the neutral component of the center of G; it is a torus. Let G^{der} be the derived subgroup of G; it is a semisimple group. Let $G_1, \ldots, G_m$ be the nontrivial normal subgroups of G^{der} that are connected and minimal with respect to inclusion; these groups are almost simple, i.e., the center $Z(G_i)$ of G_i is finite and the quotient $G_i/Z(G_i)$ is a simple algebraic group. The group G is an **almost direct product** of $G_0, \ldots, G_m$, i.e., the morphism

$$\varphi \colon G_0 \times G_1 \times \cdots \times G_m \to G$$

defined by multiplication is a surjective homomorphism whose kernel is finite and contained in the center, cf. [PR94, Proposition 2.4].

For each $0 \leqslant i \leqslant m$, define $T_i := G_i \cap T$; it is a maximal torus of G_i. Note that $T_0 \times \cdots \times T_m$ is a maximal torus of $G_0 \times \cdots \times G_m$ and $\varphi(T_0 \times \cdots \times T_m) = T$. We then have a homomorphism

$$X(T) \to X(T_0 \times \cdots \times T_m) = X(T_0) \oplus \cdots \oplus X(T_m), \quad \alpha \mapsto \alpha \circ \varphi.$$

Tensoring up to $\mathbb{Q}$ gives an isomorphism

$$X(T)_{\mathbb{Q}} = X(T_0)_{\mathbb{Q}} \oplus \cdots \oplus X(T_m)_{\mathbb{Q}},$$

where $X(T_i)_{\mathbb{Q}} := X(T_i) \otimes_{\mathbb{Z}} \mathbb{Q}$; we will use this isomorphism as an identification. We thus have a disjoint union

(7.3) $$R(G, T) = \bigcup_{i=1}^{m} R(G_i, T_i);$$

this is the decomposition of $R(G, T)$ into irreducible root systems.

For each $0 \leqslant i \leqslant m$, we have a natural map $W(G, T) \to W(G_i, T_i)$. This induces an isomorphism

$$W(G, T) = W(G_0, T_0) \times \cdots \times W(G_m, T_m)$$

that we will also use an identification. From the action of $W(G, T)$ on $X(T)_{\mathbb{Q}}$, we see that every $W(G, T)$-orbit $\mathcal{O} \subseteq X(T)_{\mathbb{Q}}$ is of the form

$$\mathcal{O}_0 \oplus \cdots \oplus \mathcal{O}_m := \{\alpha_0 + \cdots + \alpha_m : \alpha_i \in \mathcal{O}_i\}$$

for unique $W(G_i, T_i)$-orbits $\mathcal{O}_i$ in $X(T_i)_{\mathbb{Q}}$.

Lemma 7.9. *We have $s \leqslant m$. After reordering the groups $G_1, \ldots, G_m$, the following will hold for all $1 \leqslant i \leqslant s$:*

(a) *The set $\mathcal{S}_i$ spans the $\mathbb{Q}$-vector space $X(T_i)_{\mathbb{Q}}$.*

(b) *There is an irreducible and minuscule representation V_i of G_i such that $\mathcal{S}_i = \{\alpha - \beta : \alpha, \beta \in \Omega_{V_i}, \alpha \neq \beta\}$, where $\Omega_{V_i} \subseteq X(T_i)$ is the set of weights of T_i acting on V_i.*

Proof. Take any $1 \leqslant i \leqslant s$. Assume, after possibly reordering the groups $G_1, \ldots, G_m$, that $\mathcal{S}_j$ spans $X(T_j)_{\mathbb{Q}}$ for all $1 \leqslant j < i$. Note that this assumption is vacuous if $i = 1$.

We claim that the following hold:

- $i \leqslant m$,
- $\mathcal{S}_i$ spans $X(T_j)_{\mathbb{Q}}$ for some $i \leqslant j \leqslant m$,
- $\mathcal{S}_i = \{\alpha - \beta : \alpha, \beta \in \Omega_U, \alpha \neq \beta\}$ for some irreducible and minuscule representation U of G_j.

We could further assume that $j = i$ after swapping G_i and G_j.

Note that once the claim has been proved, the lemma will follow by induction on i.

We now prove the claim. In the construction of $\mathcal{S}_i$, we chose a $W(G, T)$-orbit $\mathcal{O} \subseteq \mathcal{U}_i$ of minimal cardinality and a $W(G, T)$-orbit $\Omega \subseteq \Omega_V$ for which $\mathcal{O} \subseteq C_\Omega$. The orbit Ω is equal to Ω_U for some irreducible representation $U \subseteq V$ of G; this makes use of our minuscule assumption on ρ.

Since U is an irreducible representation of G, there are irreducible representations U_j of G_j for all $0 \leqslant j \leqslant m$ such that the representation $U_0 \otimes \cdots \otimes U_m$ of $G_0 \times \cdots \times G_m$ is isomorphic to the representation U of $G_0 \times \cdots \times G_m$ obtained by composing φ with the representation of G.

We have

$$(7.4) \qquad\qquad \Omega = \Omega_U = \{\alpha_0 + \cdots + \alpha_m : \alpha_j \in \Omega_{U_j}\},$$

where $\Omega_{U_j} \subseteq X(T_j)$ is the set of weights of G_j acting on U_j with respect to T_j. The group $W(G, T)$ acts transitively on Ω_U since U is minuscule by our assumptions on ρ. Therefore, $W(G_j, T_j)$-acts transitively on Ω_{U_j} for each j, i.e., U_j is a minuscule representation of G_j.

From (7.4), we have

$$C_\Omega = \Big\{ \sum_{j=1}^m (\alpha_j - \beta_j) : \alpha_j, \beta_j \in \Omega_{U_j} \Big\} \setminus \{0\};$$

we do not need the $j = 0$ term since $|\Omega_{U_0}| = 1$ (U_0 is an irreducible representation of the torus G_0 and hence is 1-dimensional). Therefore, the $W(G, T)$-orbit $\mathcal{O} \subseteq C_\Omega$ is equal to

$$\{\alpha_1 + \ldots + \alpha_m : \alpha_j \in \mathcal{O}_j\},$$

where $\mathcal{O}_j$ is a $W(G_j, T_j)$-orbit in $\{\alpha - \beta : \alpha, \beta \in \Omega_{U_j}\} \subseteq X(T_j)_{\mathbb{Q}}$. In particular, $|\mathcal{O}| = \prod_{j=1}^m |\mathcal{O}_j|$.

Suppose that $\mathcal{O}_j = \{0\}$ for all $i \leqslant j \leqslant m$. Then $\mathcal{O}$ is contained in $\bigoplus_{1 \leqslant j < i} X(T_j)_{\mathbb{Q}}$ which is the span of $\bigcup_{1 \leqslant j < i} \mathcal{S}_j$ in $X(T)_{\mathbb{Q}}$ by the assumption at the beginning of the lemma. This implies that $\mathcal{O}$ is not a subset of the set $\mathcal{U}_i$ from Algorithm 7.1. However, this contradicts our choice of $\mathcal{O}$. Therefore, $\mathcal{O}_j \neq \{0\}$ for some $i \leqslant j \leqslant m$. In particular, $i \leqslant m$.

We may thus assume that $\mathcal{O}_i \neq \{0\}$ after possibly swapping G_i and G_j. We have $\mathcal{O}_i \subseteq \mathcal{U}_i$ since $\mathcal{O}_i$ is not contained in $\bigoplus_{1 \leqslant j < i} X(T_j)_{\mathbb{Q}} = \operatorname{span}_{X(T)_{\mathbb{Q}}} (\bigcup_{1 \leqslant j < i} \mathcal{S}_j)$. Since $|\mathcal{O}| = \prod_{j=1}^m |\mathcal{O}_j|$ and $\mathcal{O}_i \subseteq \mathcal{U}_i$, the minimality condition in our choice of $W(G, T)$-orbit $\mathcal{O}$ implies that $|\mathcal{O}_j| = 1$ for all $j \in \{1, \ldots, m\} - \{i\}$. We have $\mathcal{O}_j = \{0\}$ for all $j \in \{1, \ldots, m\} - \{i\}$, since otherwise we would have a nonzero element of $X(T_j)_{\mathbb{Q}}$ fixed by $W(G_j, T_j)$ which contradicts Lemma 7.6. Therefore, $\mathcal{O} = \mathcal{O}_i$.

Since $\mathcal{O} = \mathcal{O}_i \neq \{0\}$ is a $W(G_i, T_i)$-set, it spans $X(T_i)_{\mathbb{Q}}$ by Lemma 7.6. Recall that $\mathcal{S}_i$ is the set of elements of C_{Ω} that lie in the span of $\mathcal{O}$ in $X(T)_{\mathbb{Q}}$, i.e., $X(T_i)_{\mathbb{Q}}$. Therefore, $\mathcal{S}_i$ equals $\{\alpha - \beta : \alpha, \beta \in \Omega_{U_i}, \alpha \neq \beta\}$ and spans $X(T_i)_{\mathbb{Q}}$. We have now verified the claim. $\qquad\square$

We shall assume that the groups $G_1, \ldots, G_m$ have been reordered so that the conditions of Lemma 7.9 hold.

Lemma 7.10. *We have $m = s$.*

Proof. We have $s \leqslant m$ by Lemma 7.9. Suppose that $s < m$ and hence there is an integer $s < i \leqslant m$.

Take an irreducible $U \subseteq V$ representation of G. There are irreducible representations $\rho_j \colon G_j \to \mathrm{GL}_{U_j}$ for all $0 \leqslant j \leqslant m$ such that the representation $U_0 \otimes \cdots \otimes U_m$ of $G_0 \times \cdots \times G_m$ is isomorphic to the representation U of $G_0 \times \cdots \times G_m$ obtained by composing φ with the representation U of G.

Since G_i is almost simple, the kernel of ρ_i is finite or G_i. Therefore, $U \subseteq V$ can be chosen so that $\rho_i \colon G_i \to \mathrm{GL}_{U_i}$ has finite kernel; otherwise, this would contradict that the kernel of ρ is in the center of G. In particular, $\Omega_{U_i} \neq \{0\}$ is a $W(G, T)$-orbit in Ω_V and is a subset of $X(T_i)_{\mathbb{Q}}$. The set $C_{\Omega_{U_i}} \subseteq X(T_i)_{\mathbb{Q}}$ is nonempty; otherwise Ω_{U_i} would consist of one nonzero element stable under the action of $W(G_i, T_i)$-action and this would contradict Lemma 7.6.

By Lemma 7.9, the set $\bigcup_{1 \leqslant j \leqslant s} \mathcal{S}_j$ spans $\oplus_{1 \leqslant j \leqslant s} X(T_j)_{\mathbb{Q}}$. However, $\oplus_{1 \leqslant j \leqslant s} X(T_j)_{\mathbb{Q}}$ does not contain $C_{\Omega_{U_i}}$ since $i > s$. In Algorithm 7.1, this implies that $C_{\Omega_{U_i}} \subseteq \mathcal{U}_{s+1}$ and in particular $\mathcal{U}_{s+1} \neq \emptyset$. However, $\mathcal{U}_{s+1}$ is empty by the definition of s. This contradicts our initial assumption that $s < m$. Since $s \leqslant m$, we deduce that $s = m$. $\qquad\square$

The decomposition of $R(G, T)$ into irreducible root systems is $R(G, T) = \bigcup_{i=1}^{s} R(G_i, T_i)$ by (7.3) and Lemma 7.10. For each $1 \leqslant i \leqslant s$, we have $R(G_i, T_i) \subseteq X(T_i)_{\mathbb{Q}}$ and $X(T_i)_{\mathbb{Q}}$ is spanned by $\mathcal{S}_i$ by Lemma 7.9(a).

Take any $1 \leqslant i \leqslant s$, By Lemma 7.9(b), there is an irreducible and minuscule representation

$$\rho_i \colon G_i \to \mathrm{GL}_{V_i}$$

such that $\mathcal{S}_i = \{\alpha - \beta : \alpha, \beta \in \Omega_{V_i}, \alpha \neq \beta\}$, where $\Omega_{V_i} \subseteq X(T_i)$ is the set of weights of T_i acting on V_i. The representation ρ_i is nontrivial since otherwise $\mathcal{S}_i = \{\alpha - \beta : \alpha, \beta \in \Omega_{V_i}, \alpha \neq \beta\}$ is empty which is impossible by the construction of the sets $\mathcal{S}_i$. Since G_i is almost simple, we deduce that the kernel of ρ_i is contained in the center of G_i.

Now observe that the assumptions in the beginning of §7 hold with (G, T, ρ) replaced by (G_i, T_i, ρ_i). Applying Algorithm 7.1 to the triple (G_i, T_i, ρ_i), we obtain $s = 1$ and the new set "$\mathcal{S}_1$" agrees with our set $\mathcal{S}_i$. The triple (G_i, T_i, ρ_i) satisfies the conditions of §7.1.1 and hence Propositions 7.2, 7.3 and 7.5 hold for it.

By Proposition 7.2 in the setting of §7.1.1, we find that $R(G_i, T_i) \subseteq \mathcal{S}_i$. The set $\mathcal{S}_i$ does not contain $R(G_j, T_j)$ for any $j \neq i$ since it is a subset of $X(T_i)_{\mathbb{Q}}$. This completes the proof of Proposition 7.2

Let W_i be the quotient of $W(G, T)$ that acts faithfully on $\mathcal{S}_i$. Since $\mathcal{S}_i \subseteq X(T_i)_{\mathbb{Q}}$, W_i is also the quotient of $W(G_i, T_i)$ that acts faithfully on $\mathcal{S}_i$. Let r_i be the dimension of the span of $\mathcal{S}_i$ in $X(T)_{\mathbb{Q}}$; equivalently, in $X(T_i)_{\mathbb{Q}}$. Propositions 7.3 and 7.5 now follow directly from the special cases of the propositions that hold for (G_i, T_i, ρ_i) with $1 \leqslant i \leqslant s$.

8. Finding root datum

Fix a nonzero abelian variety A over a number field K. Assume that Conjectures 4.3 and 4.5 hold for A. Denote by r the rank of $\mathrm{MT}_A = G_A^{\circ}$. The common rank of the ℓ-adic monodromy groups $G_{A, \ell}^{\circ}$ is r since we are assuming the Mumford–Tate conjecture. Let $\mathcal{S}_A$ be the set of prime ideals of $\mathcal{O}_K$ from Definition 3.4; it has density $1/[K_A^{\mathrm{conn}} : K]$ by Lemma 3.5(i).

The main goal of this section is to explain how one can compute the root datum of MT_A directly from the Frobenius polynomials of $P_{A,\mathfrak{q}}(x)$ and $P_{A,\mathfrak{p}}(x)$ for two appropriately chosen prime ideals $\mathfrak{q}$ and $\mathfrak{p}$ of $\mathcal{O}_K$.

More precisely, we will compute the abstract root datum $\Psi(\mathrm{MT}_A)$ along with the homomorphism $\mu_{\mathrm{MT}_A} \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Out}(\Psi(\mathrm{MT}_A))$ from §2.7. By Proposition 2.5, this information determines MT_A up to an inner twist. Along with this root data, we will also compute the set of weights, with multiplicities, of the natural representation $\mathrm{MT}_A \subseteq \mathrm{GL}_V$.

8.1. **Choice of primes.** We first select our two prime ideals.

(a) Let $\mathfrak{q}$ be any prime ideal in $\mathcal{S}_A$.
(b) Let $\mathfrak{p}$ be any prime ideal in $\mathcal{S}_A$ for which $[L(\mathcal{W}_{A,\mathfrak{p}}) : L] = |W(\mathrm{MT}_A)|$, where $L := \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$.

There are many possibilities for $\mathfrak{q}$ since $\mathcal{S}_A$ has positive density. The following lemma shows that for a fixed $\mathfrak{q}$, there are also many possibly $\mathfrak{p}$.

Lemma 8.1. *Fix $\mathfrak{q} \in \mathcal{S}_A$ and set $L = \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$. Then the set of prime ideals $\mathfrak{p} \in \mathcal{S}_A$ that do not satisfy (b) has density 0.*

Proof. Let G be the quasi-split inner form of the Mumford–Tate group MT_A. Let k_G be the subfield of $\overline{\mathbb{Q}}$ fixed by $\ker \mu_G$ with notation as in §2.7; it agrees with the similarly defined field k_{MT_A} by Proposition 2.5.

First suppose that $K_A^{\mathrm{conn}} = K$. Since $\mathfrak{q} \in \mathcal{S}_A$, we have a maximal torus $T_\mathfrak{q}$ of G as in Theorem 5.1. The splitting field of the torus $T_\mathfrak{q}$ is $L = \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$ and hence $k_G \subseteq L$. Corollary 6.2 implies that $\mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L) \cong W(\mathrm{MT}_A)$ for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ away from a set of density 0; note that this uses our assumption $K_A^{\mathrm{conn}} = K$. This proves the lemma in the special case $K_A^{\mathrm{conn}} = K$.

We now consider the general case. Let A' be the base change of A to K_A^{conn}. Note that A and A' have the same Mumford–Tate group and hence the same G. Take any prime ideal $\mathfrak{p} \in \mathcal{S}_A$ and choose a prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K_A^{\mathrm{conn}}}$ dividing $\mathfrak{p}$. The prime $\mathfrak{p}$ splits completely in K_A^{conn} by Lemma 3.3(i) and hence $N(\mathfrak{P}) = N(\mathfrak{p})$. By Lemma 3.5(ii), we have $\mathfrak{P} \in \mathcal{S}_{A'}$ and $P_{A',\mathfrak{P}}(x) = P_{A,\mathfrak{p}}(x)$. In particular, $L(\mathcal{W}_{A',\mathfrak{P}}) = L(\mathcal{W}_{A,\mathfrak{p}})$. Therefore, we have an inequality

$$
(8.1) \qquad |\{\mathfrak{p} \in \mathcal{S}_A : N(\mathfrak{p}) \leqslant x,\ [L(\mathcal{W}_{A,\mathfrak{p}}) : L] \neq |W(\mathrm{MT}_A)|\}|
$$
$$
\leqslant |\{\mathfrak{P} \in \mathcal{S}_{A'} : N(\mathfrak{P}) \leqslant x,\ [L(\mathcal{W}_{A',\mathfrak{P}}) : L] \neq |W(\mathrm{MT}_{A'})|\}|.
$$

A similar argument as above shows that $L = \mathbb{Q}(\mathcal{W}_{A',\mathfrak{Q}})$ for any prime ideal $\mathfrak{Q}$ of $\mathcal{O}_{K_A^{\mathrm{conn}}}$ that divides $\mathfrak{q}$. By the connected case of the lemma that we have already proved, we have

$$
|\{\mathfrak{P} \in \mathcal{S}_{A'} : N(\mathfrak{P}) \leqslant x,\ [L(\mathcal{W}_{A',\mathfrak{P}}) : L] \neq |W(\mathrm{MT}_{A'})|\}| = o(x/\log x).
$$

The general case of the lemma then follows from the inequality (8.1). $\qquad\square$

For the rest of §8, we fix prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ as in (a) and (b) above. For our later algorithmic considerations, we assume that the Frobenius polynomials $P_{A,\mathfrak{q}}(x)$ and $P_{A,\mathfrak{p}}(x)$ have been computed.

8.2. **Frobenius torus at $\mathfrak{p}$.** Let G be the quasi-split inner form of the Mumford–Tate group MT_A and let

$$
\rho \colon G_{\overline{\mathbb{Q}}} \xrightarrow{\sim} (\mathrm{MT}_A)_{\overline{\mathbb{Q}}} \subseteq \mathrm{GL}_{V_A,\overline{\mathbb{Q}}},
$$

be a representation where the isomorphism is one arising from G being an inner twist of MT_A. [V_A]

By Theorem 5.1, there is a maximal torus $T_\mathfrak{p}$ of G for which we have an isomorphism $X(T_\mathfrak{p}) = \Phi_{A,\mathfrak{p}}$ of $\mathrm{Gal}_\mathbb{Q}$-modules which we will use as an identification. Explicitly, there is a $t_\mathfrak{p} \in T_\mathfrak{p}(\mathbb{Q})$ as in Theorem 5.1 such that the isomorphism is given by $\alpha \mapsto \alpha(t_\mathfrak{p})$.

Remark 8.2. We will construct the root datum of G with respect to the maximal torus $T_\mathfrak{p}$. Our identification $X(T_\mathfrak{p}) = \Phi_{A,\mathfrak{p}}$ gives a tangible place to start since the group $\Phi_{A,\mathfrak{p}}$ with its Galois action are computable directly from the polynomial $P_{A,\mathfrak{p}}(x)$, cf. §3.4.

Moreover, under this identification, we can assume by Theorem 5.1 that $\Omega_{\mathfrak{p}} := \mathcal{W}_{A,\mathfrak{p}}$ is the set of weights in $X(T_{\mathfrak{p}})$ of the representation ρ. The multiplicity of a weight α agrees with the multiplicity of it viewed as a root of $P_{A,\mathfrak{p}}(x)$.

8.3. Computing the Weyl group.
Define the field $L := \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$ and the Galois group

$$W := \mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L).$$

The group W acts faithfully on $\mathcal{W}_{A,\mathfrak{p}}$ and hence also faithfully on the group $\Phi_{A,\mathfrak{p}}$. Using our identification $X(T_{\mathfrak{p}}) = \Phi_{A,\mathfrak{p}}$, we can thus view W as a subgroup of $\mathrm{Aut}_{\mathbb{Z}}(X(T_{\mathfrak{p}}))$. We can also identify $W(G, T_{\mathfrak{p}})$ with a subgroup of $\mathrm{Aut}_{\mathbb{Z}}(X(T_{\mathfrak{p}}))$. The following lemma shows that W recovers the Weyl group of G.

Lemma 8.3. *We have* $W = W(G, T_{\mathfrak{p}})$.

Proof. Since $\mathfrak{q} \in \mathcal{S}_A$, we have a maximal torus $T_{\mathfrak{q}}$ of G as in Theorem 5.1. The splitting field of the torus $T_{\mathfrak{q}}$ is the field L. With notation as in §6, we have $k_G \subseteq L$ and hence $\varphi_{\mathfrak{p}}(\mathrm{Gal}_L) \subseteq W(G, T_{\mathfrak{p}})$. Using our identification of W with a subgroup of $\mathrm{Aut}_{\mathbb{Z}}(X(T_{\mathfrak{p}}))$, we have $W \subseteq W(G, T_{\mathfrak{p}})$. By our choice of $\mathfrak{p}$, we find that $|W| = [L(\mathcal{W}_{A,\mathfrak{p}}) : L]$ equals $|W(MT_A)| = |W(G, T_{\mathfrak{p}})|$. Therefore, $W = W(G, T_{\mathfrak{p}})$. $\square$

8.4. Computing the roots.
So far we have described how to compute the following from our polynomials $P_{A,\mathfrak{q}}(x)$ and $P_{A,\mathfrak{p}}(x)$:

- $X(T_{\mathfrak{p}})$ as a $\mathrm{Gal}_{\mathbb{Q}}$-module,
- the Weyl group $W(G, T_{\mathfrak{p}})$ and its action on $X(T_{\mathfrak{p}})$,
- the set of weights $\Omega_{\mathfrak{p}} \subseteq X(T_{\mathfrak{p}})$, with multiplicities, of the faithful representation $\rho \colon G_{\overline{\mathbb{Q}}} \hookrightarrow (\mathrm{GL}_{V_A})_{\overline{\mathbb{Q}}} = \mathrm{GL}_{V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}}$.

We now explain how to compute the set $R := R(G, T_{\mathfrak{p}}) \subseteq X(T_{\mathfrak{p}})$ of roots of G with respect to $T_{\mathfrak{p}}$.

By Proposition 4.8, every irreducible representation $U \subseteq V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ of $G_{\overline{\mathbb{Q}}}$ is minuscule. We are thus in the setting of §7 with the representation $\rho \colon G_{\overline{\mathbb{Q}}} \hookrightarrow \mathrm{GL}_{V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}}$. Applying Algorithm 7.1, we obtain nonempty finite subsets $\mathcal{S}_1, \ldots, \mathcal{S}_s$ of $X(T_{\mathfrak{p}})$ for some integer $s \geqslant 0$. Note this algorithm only makes use of the set $\Omega_{\mathfrak{p}}$ and the action of $W(G, T_{\mathfrak{p}})$ on $X(T_{\mathfrak{p}})$.

By Proposition 7.2, there is a unique irreducible component R_i of the root system $R(G, T_{\mathfrak{p}}) \subseteq X(T_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{R}$ with $R_i \subseteq \mathcal{S}_i$ for each $1 \leqslant i \leqslant s$. Moreover,

$$R(G, T_{\mathfrak{p}}) = \bigcup_{1 \leqslant i \leqslant s} R_i$$

is a disjoint union and is the decomposition into irreducible root systems. By Proposition 7.3 and 7.5, we can compute the Lie type of each R_i and then compute R_i itself; note that these propositions only requires the sets $\mathcal{S}_i \subseteq X(T_{\mathfrak{p}})$ and the action of $W(G, T_{\mathfrak{p}})$. We can thus compute $R(G, T_{\mathfrak{p}})$!

8.5. Computing the root datum of the Mumford–Tate group.
Define the group $Y := \mathrm{Hom}_{\mathbb{Z}}(X(T_{\mathfrak{p}}), \mathbb{Z})$; it has a natural pairing with $X(T_{\mathfrak{p}})$ and we can identify it with the group of cocharacters $X^{\vee}(T_{\mathfrak{p}})$. Lemma 2.2 implies that the root datum $\Psi(G, T_{\mathfrak{p}})$ can be determined from the action of $W(G, T_{\mathfrak{p}})$ on $X(T_{\mathfrak{p}})$ and the set of roots $R(G, T_{\mathfrak{p}})$; moreover, the proof shows how to construct the bijective map $\alpha \mapsto \alpha^{\vee}$ from $R(G, T_{\mathfrak{p}})$ to the set of coroots $R^{\vee}(G, T_{\mathfrak{p}})$. We thus know how to compute the root datum $\Psi(G, T_{\mathfrak{p}})$ since from §8.4 we have already found $X(T_{\mathfrak{p}})$, $R(G, T_{\mathfrak{p}})$ and the action of $W(G, T_{\mathfrak{p}})$ on $X(T_{\mathfrak{p}})$. Since we now know the root datum $\Psi(G, T_{\mathfrak{p}})$ and the action of $\mathrm{Gal}_{\mathbb{Q}}$ on $X(T_{\mathfrak{p}})$, we can also compute $\mu_G \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(G, T_{\mathfrak{p}}))$.

Since MT_A is an inner form of G, we may take $\Psi(MT_A)$ to be $\Psi(G, T_{\mathfrak{p}})$. The homomorphism $\mu_{MT_A} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(MT_A))$ agrees with μ_G by Lemma 2.5.

Finally note that $\Omega_{\mathfrak{p}} \subseteq X(T_{\mathfrak{p}})$ gives the weights of the representation $MT_A \subseteq GL_V$. The multiplicity of a weight $\alpha \in \Omega_{\mathfrak{p}}$ of ρ agrees with the multiplicity of α as a root of $P_{A,\mathfrak{p}}(x)$ (recall we are identifying $\Omega_{\mathfrak{p}}$ with $\mathcal{W}_{A,\mathfrak{p}}$).

8.6. **Computing the root datum of the Hodge group.** The Hodge group Hg_A of A was defined in §4.1. Recall that MT_A contains the group of scalars in GL_V and that $MT_A = \mathbb{G}_m \cdot Hg_A$.

We first describe an algebraic subgroup H of G that is a quasi-split inner form of Hg_A. We have $MT_A \subseteq GSp_{V,E}$ and $Hg_A = MT_A \cap Sp_{V,E}$, where E is an appropriate nondegenerate alternating pairing on V. Let $\nu \colon GSp_{V,E} \to (\mathbb{G}_m)_{\mathbb{Q}}$ be the similitude character. Define the homomorphism

$$\mu := \nu \circ \rho \colon G_{\overline{\mathbb{Q}}} \to (\mathbb{G}_m)_{\overline{\mathbb{Q}}}.$$

For each $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, we have

$$\sigma(\mu) = \nu \circ \sigma(\rho) \circ \rho^{-1} \circ \rho = \nu \circ \rho = \mu,$$

where we have used that $\sigma(\rho) \circ \rho^{-1}$ is an inner automorphism of $(MT_A)_{\overline{\mathbb{Q}}}$ and hence $\nu \circ (\sigma(\rho) \circ \rho^{-1}) = \nu|_{(MT_A)_{\overline{\mathbb{Q}}}}$. Therefore, μ arises by base change from a unique homomorphism $G \to \mathbb{G}_m$ defined over $\mathbb{Q}$ that we also denote by μ. Let $H \subseteq G$ be the kernel of μ. The homomorphism ρ induces an isomorphism between $H_{\overline{\mathbb{Q}}}$ and $(Hg_A)_{\overline{\mathbb{Q}}}$. In particular, H is a connected and reductive group defined over $\mathbb{Q}$. The group H is an inner form of Hg_A via ρ; note that each inner automorphism of $(MT_A)_{\overline{\mathbb{Q}}}$ arises from conjugation by some $Hg_A(\overline{\mathbb{Q}})$ since $MT_A = \mathbb{G}_m \cdot Hg_A$. The centers of MT_A and G are naturally isomorphic since they are inner forms of each other, so we can view the group $\mathbb{G}_m$ of homotheties as a subgroup of G and hence $G = \mathbb{G}_m \cdot H$. Since G is quasi-split, we find that H is a quasi-split inner form of Hg_A and is given by the isomorphism $\rho|_{H_{\overline{\mathbb{Q}}}} \colon H_{\overline{\mathbb{Q}}} \to (Hg_A)_{\overline{\mathbb{Q}}}$.

Thus to compute the abstract root datum $\Psi(Hg_A)$ and the homomorphism $\mu_{Hg_A} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(Hg_A))$, it suffices to compute them for the group H. Let T be the unique maximal torus of H contained in $T_{\mathfrak{p}}$. Restriction to $T_{\overline{\mathbb{Q}}}$ defines a surjective homomorphism

$$(8.2) \qquad\qquad\qquad\qquad X(T_{\mathfrak{p}}) \to X(T)$$

that respects the $\mathrm{Gal}_{\mathbb{Q}}$-actions. Using that $G = \mathbb{G}_m \cdot H$, we find that (8.2) gives a bijection between $R(G, T_{\mathfrak{p}})$ and $R(H, T)$. The Weyl group $W(G, T_{\mathfrak{p}})$ fixes the kernel of (8.2) and the induced action on $X(T)$ is faithfully. The action of the group $W(G, T_{\mathfrak{p}})$ on $X(T)$ agrees with $W(H, T)$. The set of roots $R(H, T) \subseteq X(T)$ and the action of $W(H, T)$ on $X(T)$ determine the root datum $\Psi(H, T)$ by Lemma 2.2 (and the proof shows how to compute it). The homomorphism (8.2) respects the $\mathrm{Gal}_{\mathbb{Q}}$-actions, so from $\Psi(H, T)$ and the $\mathrm{Gal}_{\mathbb{Q}}$-action on $X(T_{\mathfrak{p}})$, we can compute $\mu_H \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(H))$.

We have already described how to compute $W(G, T_{\mathfrak{p}})$ and $R(G, T_{\mathfrak{p}})$. So to make everything computable, it remains to describe the homomorphism (8.2) with respect to our identification $X(T_{\mathfrak{p}}) = \Phi_{A,\mathfrak{p}}$. The following lemma shows that we may take $X(T) = \Phi_{A,\mathfrak{p}}/\langle N(\mathfrak{p})\rangle$.

Lemma 8.4. *Under our identification $X(T_{\mathfrak{p}}) = \Phi_{A,\mathfrak{p}}$, the restriction homomorphism $X(T_{\mathfrak{p}}) \to X(T)$, $\alpha \mapsto \alpha|_{T_{\overline{\mathbb{Q}}}}$ has kernel $\langle N(\mathfrak{p})\rangle$.*

Proof. Let $\beta \colon T_{\mathfrak{p}} \to \mathbb{G}_m$ be the character defined by $\beta = \mu|_{T_{\mathfrak{p}}}$. The kernel of β is a commutative algebraic subgroup of H containing T. Since maximal tori of reductive groups are their own centralizers, we find that $T = \ker \beta$. So the kernel of $X(T_{\mathfrak{p}}) \to X(T)$ is $\langle \beta \rangle$. With our identification $X(T_{\mathfrak{p}}) = \Phi_{A,\mathfrak{p}}$ given by $\alpha \mapsto \alpha(t_{\mathfrak{p}})$, it thus suffices to show that $\beta(t_{\mathfrak{p}}) = N(\mathfrak{p})$.

The eigenvalues of an element in $Sp_{V,E}(\overline{\mathbb{Q}})$ occur in inverse pairs. Since the characteristic polynomial of $\rho(t_{\mathfrak{p}})$ is $P_{A,\mathfrak{p}}(x)$ and the roots of $P_{A,\mathfrak{p}}(x)$ have absolute value $N(\mathfrak{p})$ (with respect to any embedding into $\mathbb{C}$), we deduce that $\pm\rho(t_{\mathfrak{p}})/\sqrt{N(\mathfrak{p})}$ are precisely the elements of $Hg_A(\overline{\mathbb{Q}})$ that are scalar multiples of $\rho(t_{\mathfrak{p}})$. Therefore, $\nu(\pm\rho(t_{\mathfrak{p}})/\sqrt{N(\mathfrak{p})}) = 1$ and hence $\nu(\rho(t_{\mathfrak{p}})) = N(\mathfrak{p})$. In particular, $\beta(t_{\mathfrak{p}}) = \mu(t_{\mathfrak{p}}) = \nu(\rho(t_{\mathfrak{p}})) = N(\mathfrak{p})$. $\qquad\qquad\square$

Finally, the image $\Omega \subseteq X(T)$ of $\Omega_{\mathfrak{p}}$ under the restriction map $X(T_{\mathfrak{p}}) \to X(T)$ is the set of weights of the representation $\rho|_{H_{\overline{\mathbb{Q}}}}$ with respect to T.

We claim that the map $\Omega_{\mathfrak{p}} \to \Omega$ is a bijection that respects multiplicities. If the claim fails, then by Lemma 8.4 and our identification $\Omega_{\mathfrak{p}} = \mathcal{W}_{A,\mathfrak{p}}$ there are distinct z and $z' \in \mathcal{W}_{A,\mathfrak{p}}$ such that $z'z^{-1} \in \langle N(\mathfrak{p}) \rangle$. Since z and z' are roots of $P_{A,\mathfrak{p}}(x)$, they have absolute value $\sqrt{N(\mathfrak{p})}$ under any embedding into $\mathbb{C}$. Therefore, $z = z'$ which contradicts that they are distinct and proves the claim.

8.7. Proof of Theorem 1.1.
Recall that $G_A^\circ = MT_A$. Let Σ be the set of nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that split completely in K_A^{conn}. By Lemma 3.3, we have $\mathcal{S}_A \subseteq \Sigma$ and the set $\Sigma - \mathcal{S}_A$ has density 0. So it suffices to proof the theorem with any $\mathfrak{q} \in \mathcal{S}_A$. Let S_2 be the set of $\mathfrak{p} \in \mathcal{S}_A$ for which condition (b) in §8.1 does not hold for our fixed $\mathfrak{q}$. The set S_2 has density 0 by Lemma 8.1. So it suffices to proof the theorem with any choice of $\mathfrak{p} \in \mathcal{S}_A - S_2$ since $\Sigma - (\mathcal{S}_A - S_2)$ has density 0.

Our primes $\mathfrak{q}$ and $\mathfrak{p}$ satisfies condition (a) and (b) in §8.1. In §§8.2–8.5, we have explained how given the polynomials $P_{A,\mathfrak{p}}(x)$ and $P_{A,\mathfrak{q}}(x)$, one can compute the abstract root datum $\Psi(MT_A)$, the homomorphism $\varphi_G \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Out}(\Psi(MT_A))$, and the set of weights Ω of the representation $MT_A \subseteq GL_{V_A}$ and their multiplicities. This proves Theorem 1.1.

8.8. Proof of Theorem 1.6.
The theorem is an immediate consequence of Theorem 1.1 and the construction of §8.6. Note that the part concerning the group ST_A° follows since it is a maximal compact subgroup of $Hg_A(\mathbb{C})$.

9. Some computational remarks

Fix a nonzero abelian variety A over a number field K. When trying to implement the algorithm described in §1.6, the most computationally intensive part is computing the splitting field of the polynomials $P_{A,\mathfrak{p}}(x)$.

9.1. Computing $\Phi_{A,\mathfrak{p}}$, revisited.
Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ for which A has good reduction. In §3.4, we described how to compute the group $\Phi_{A,\mathfrak{p}}$ from $P_{A,\mathfrak{p}}(x)$. The method outlined involves computing a splitting field $L/\mathbb{Q}$ of $P_{A,\mathfrak{p}}(x) \in \mathbb{Z}[x]$ and working with $\mathrm{Gal}(L/\mathbb{Q})$. Unfortunately, computing splitting fields can be extremely time consuming.

For simplicity, we now assume further that A has ordinary reduction at $\mathfrak{p}$; this can be verified by checking that the middle coefficient of $P_{A,\mathfrak{p}}(x)$ is 0 modulo $\mathfrak{p}$. We will now explain how to compute $\Phi_{A,\mathfrak{p}}$ without computing a splitting field L of $P_{A,\mathfrak{p}}(x)$ over $\mathbb{Q}$.

The function `GaloisGroup` implemented in `Magma` is suitable for are purposes, see [Els16] for an overview of the algorithm. The function produces the distinct roots $\pi_1, \ldots, \pi_n$ of $P_{A,\mathfrak{p}}(x)$ in a splitting field $L'/\mathbb{Q}_\ell$ for some prime ℓ; more precisely, approximations are produced for the π_i which can be computed to arbitrary accuracy. Using the numbering of these roots, there is an injective homomorphism $\mathrm{Gal}(\mathbb{Q}(\pi_1, \ldots, \pi_n)/\mathbb{Q}) \hookrightarrow S_n$. The function `GaloisGroup` also produces the image $\Gamma \subseteq S_n$ of this homomorphism. Note that the splitting field L' of $P_{A,\mathfrak{p}}(x)$ over $\mathbb{Q}_\ell$ is easy to compute. This Galois group algorithm also has the advantage that it does not impose any restrictions on the degree of $P_{A,\mathfrak{p}}(x)$.

For each root α of $P_{A,\mathfrak{p}}(x)$, $N(\mathfrak{p})/\alpha$ is also a root. We have $\alpha^2 \neq N(\mathfrak{p})$ for each root α of $P_{A,\mathfrak{p}}(x)$ since otherwise A would not have ordinary reduction at $\mathfrak{p}$. So the integer n is even and we can assume that the roots are chosen so that $\alpha_i \alpha_{i+n/2} = N(\mathfrak{p})$ for all $1 \leqslant i \leqslant n/2$. Let $\mathcal{O}_{L'}$ be the valuation ring of L'. There is enough flexibility in the above algorithm to ensure that ℓ is odd, $L'/\mathbb{Q}_\ell$ is unramified, and that all the π_i lie in $\mathcal{O}_{L'}^\times$.

Given $\pi_1, \ldots, \pi_n \in L'$ and Γ as above, the rest of §9.1 is devoted to computing $\Phi_{A,\mathfrak{p}}$.

Lemma 9.1. *There is a subset $S \subseteq \{1, \ldots, n\}$ satisfying the following conditions:*

    (a) For each $1 \leqslant i \leqslant n/2$, exactly one of the two values i and $i + n/2$ are in S.

    (b) For $e \in \mathbb{Z}^n$, $\prod_{i=1}^{n} \pi^{e_i}$ is a root of unity if and only if $\sum_{i \in \sigma(S)} e_i = 0$ for all $\sigma \in \Gamma$.

Proof. This is an immediate consequence of Lemma 3.6 and our assumption that A is ordinary at $\mathfrak{p}$. Note that for any prime ideal λ of $\mathcal{O}_L$ dividing $N(\mathfrak{p})$, with $L = \mathbb{Q}(\pi_1, \ldots, \pi_n)$, we have $\{v_\lambda(\pi_i), v_\lambda(\pi_{i+n/2})\} = \{0, v_\lambda(N(\mathfrak{p}))\}$. $\qquad\qquad\qquad\square$

For a tuple $e \in \mathbb{Z}^n$, the following lemma will allow us to determine when $\prod_{i=1}^{n} \pi_i^{e_i}$ equals 1 by using our approximations of the π_i in the ℓ-adic field L'.

Lemma 9.2. *Take any $e \in \mathbb{Z}^n$. Then $\prod_{i=1}^{n} \pi_i^{e_i} = 1$ if and only if $\prod_{i=1}^{n} \pi_i^{e_i} - 1 \in \ell^m \mathcal{O}_{L'}$ holds for some integer*

$$(9.1) \qquad\qquad m > |\Gamma| \frac{\log 2 + \max\{\sum_{i=1}^{n} a_i, \sum_{i=1}^{n} b_i\}/2 \cdot \log N(\mathfrak{p})}{f \log \ell},$$

where $a_i := \max\{e_i, 0\}$, $b_i := \max\{-e_i, 0\}$ and $f := [L' : \mathbb{Q}_\ell]$.

Proof. Define the algebraic integer $\alpha := \prod_{i=1}^{n} \pi^{a_i} - \prod_{i=1}^{n} \pi^{b_i}$ in the number field $L := \mathbb{Q}(\pi_1, \ldots, \pi_n)$. By Weil, we know that each π_i has absolute value $N(\mathfrak{p})^{1/2}$ under any embedding $L \hookrightarrow \mathbb{C}$. Therefore,

$$(9.2) \qquad\qquad |N_{L/\mathbb{Q}}(\alpha)| \leqslant (2 N(\mathfrak{p})^{\max\{\sum_i a_i, \sum_i b_i\}/2})^{|\Gamma|}.$$

Using the inclusion $L \subseteq L'$, we can identify L' with the completion L_λ of L at some prime ideal λ of $\mathcal{O}_L$ dividing ℓ.

First suppose that $\prod_{i=1}^{n} \pi_i^{e_i} - 1 \in \ell^m \mathcal{O}_{L'}$ for an integer m satisfying (9.1). Since the π_i are units in $\mathcal{O}_{L'}$ and $L'/\mathbb{Q}_\ell$ is unramified, this implies that $\alpha \in \lambda^m$. Therefore, $N(\lambda^m) = \ell^{fm}$ divides the integer $|N_{L/\mathbb{Q}}(\alpha)|$. So if $\alpha \neq 0$, then $\ell^{fm} \leqslant |N_{L/\mathbb{Q}}(\alpha)|$. However, by (9.1) and (9.2), we find that $\ell^{fm} > |N_{L/\mathbb{Q}}(\alpha)|$. Therefore, $\alpha = 0$ and hence $\prod_i \pi_i^{e_i} = 1$.

The other implication in the lemma is trivial. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Observe that the above lemma gives a way to determine if $\prod_{i=1}^{n} \pi_i^{e_i} = 1$ holds for a fixed $e \in \mathbb{Z}$. By increasing the accuracy of the approximations of π_i, one can assume that $\pi_i + \ell^m \mathcal{O}_{L'}$ is known for the smallest integer m satisfying (9.1). Since the π_i are units in $\mathcal{O}_{L'}$, one can then compute $\prod_{i=1}^{n} \pi_i^{e_i} + \ell^m \mathcal{O}_{L'}$. Using Lemma 9.2, we can then verify whether or not we have $\prod_{i=1}^{n} \pi_i^{e_i} = 1$.

Take any subset $S \subseteq \{1, \ldots, n\}$ satisfying condition (a) of Lemma 9.1. We now explain how to verify if it satisfies condition (b). Define the finite field $\mathbb{F} = \mathcal{O}_{L'}/\ell \mathcal{O}_{L'}$. Let M_S be the group consisting of $e \in \mathbb{Z}^n$ satisfying $\sum_{i \in \sigma(S)} e_i = 0$ for all $\sigma \in \Gamma$. Let

$$\varphi \colon M_S \to \mathbb{F}^\times$$

be the homomorphism that sends a tuple $e \in \mathbb{Z}^n$ to the image of $\prod_{i=1}^{n} \pi_i^{e_i} \in \mathcal{O}_{L'}^\times$ in $\mathbb{F}^\times$. Let M be the kernel of φ. By our choice of extension $L'/\mathbb{Q}_\ell$, the roots of unity in L' can be distinguished by their images in $\mathbb{F}^\times$. So condition (b) holds for the set S if and only if $\prod_{i=1}^{n} \pi_i^{e_i} = 1$ for a set of e that generate the group M. Using the remarks following Lemma 9.2, one can thus verify whether condition (b) holds or not.

One can thus compute the set $\mathscr{S}$ of subsets $S \subseteq \{1, \ldots, n\}$ that satisfy conditions (a) and (b) of Lemma 9.1. For making this computation practical, note that for a set $S \subseteq \{1, \ldots, n\}$, we have $S \in \mathscr{S}$ if and only if $\sigma(S) \in \mathscr{S}$ for all $\sigma \in \Gamma$. Let M' be the subgroup of $\mathbb{Z}^n$ generated by the sets M_S with $S \in \mathscr{S}$. For $e \in \mathbb{Z}^n$, Lemma 9.1 implies that $\prod_{i=1}^{n} \pi_i^{e_i}$ is a root of unity if and only if $e \in M'$.

Arguing as above, one can compute the subgroup $M \subseteq M'$ such that $\prod_{i=1}^{n} \pi_i^{e_i} = 1$ if and only if $e \in M$. Therefore, the map $\mathbb{Z}^n \to \Phi_{A,\mathfrak{p}}$, $e \mapsto \prod_{i=1}^{n} \pi_i^{e_i}$ induces an isomorphism

$$(9.3) \qquad\qquad\qquad\qquad \mathbb{Z}^n/M \xrightarrow{\sim} \Phi_{A,\mathfrak{p}}.$$

This is our explicit description of the group $\Phi_{A,\mathfrak{p}}$.

Observe that the action of $\Gamma \subseteq S_n$ on $\mathbb{Z}^n$ induces an action on $\mathbb{Z}^n/M$. With respect to the embedding $\mathrm{Gal}(\mathbb{Q}(\pi_1, \ldots, \pi_n)/\mathbb{Q}) \xrightarrow{\sim} \Gamma \subseteq S_n$ and the isomorphism (9.3), this describes the Galois action on $\Phi_{A,\mathfrak{p}}$.

9.2. **Remarks on computing root data.** With notation and assumptions as in §8, fix primes $\mathfrak{p}$ and $\mathfrak{q}$ as in §8.1. In §9.1, we described how to compute the group $\Phi_{A,\mathfrak{p}}$ and the group $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})/\mathbb{Q})$ acting on it. Note that with the method described, the splitting field $\mathbb{Q}(\mathcal{W}_{A,\mathfrak{p}})$ of $P_{A,\mathfrak{p}}(x)$ is not actually computed; the roots of $P_{A,\mathfrak{p}}(x)$ are given in some nonarchimedean field and the action of Γ is given as a permutation of its roots.

We now describe how to compute the subgroup $W := \mathrm{Gal}(L(\mathcal{W}_{A,\mathfrak{p}})/L)$ of Γ, where $L := \mathbb{Q}(\mathcal{W}_{A,\mathfrak{q}})$. We may assume that $P_{A,\mathfrak{p}}(x)$ and $P_{A,\mathfrak{q}}(x)$ are relatively prime; this is automatic if the residue fields of $\mathfrak{p}$ and $\mathfrak{q}$ have different characteristics. Let Γ_0 be the Galois group of $P_{A,\mathfrak{p}}(x) \cdot P_{A,\mathfrak{q}}(x)$ over $\mathbb{Q}$. Let m and n be the number of distinct roots of $P_{A,\mathfrak{p}}(x)$ and $P_{A,\mathfrak{q}}(x)$, respectively. As in §9.1, we can compute Γ_0 as a subgroup of $S_m \times S_n$, where the first and second factors describe the Galois action on the distinct roots of $P_{A,\mathfrak{p}}(x)$ and $P_{A,\mathfrak{q}}(x)$, respectively, with roots given explicitly in a suitable local field. We can identify Γ with the image of Γ_0 under the projection $\varphi \colon S_n \times S_m \to S_n$, $(a,b) \mapsto a$. The subgroup W of Γ is then the image under φ of the group $\Gamma_0 \cap (S_n \times \{1\})$.

We can then proceed as in §1.6, to compute the root datum $\Psi(G_A^\circ)$ up to isomorphism, the *image* of the homomorphism $\mu_{G_A^\circ} \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Out}(\Psi(G_A^\circ))$, and the set of weights of the representation $G_A^\circ \subseteq \mathrm{GL}_{V_A}$ and their multiplicities. Note that the image of $\mu_{G_A^\circ}$ is given by Γ/W.

10. PROOF OF PROPOSITION 1.13

We have fixed an embedding $\overline{K} \subseteq \mathbb{C}$ and $\mathrm{End}(A_{\overline{K}}) = \mathrm{End}(A_\mathbb{C})$. So there is no harm in replacing A by its base extension by $\mathbb{C}$; this does not change the group MT_A or its representation V_A. After replacing A by an isogenous abelian variety, we may assume that $A = \prod_{i=1}^{s} A_i$ with $A_i = C_i^{e_i}$, where $e_i \geqslant 1$ and the C_i are simple abelian varieties over $\mathbb{C}$ that are pairwise nonisogenous. We have

$$\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q} \cong B_1 \times \cdots \times B_s,$$

where $B_i := \mathrm{End}(A_i) \otimes_\mathbb{Z} \mathbb{Q}$. Note that B_i is a central simple algebra over its center L_i. The field L_i is a number field and let m_i be the positive integer satisfying $\dim_{L_i} B_i = m_i^2$.

We first assume that A is a simple abelian variety over $\mathbb{C}$, i.e., $s = 1$ and $e_1 = 1$. In particular, $B_1 = \mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}$ is a division algebra with center L_1. Define $r := [L_1 : \mathbb{Q}]$. Recall that we can identify B_1 with the subring of $\mathrm{End}_\mathbb{Q}(V_A)$ that commutes with the action of MT_A. Since B_1 is a division algebra, we find that V_A is an irreducible representation of MT_A .

Observe that the algebraic group MT_A and its faithful representation V_A satisfy the assumptions of §3.2 of [Ser79]. From §3.2 of [Ser79] (especially the irreducible case considered before Proposition 8), we find that the following hold:

- Γ acts transitively on Ω,
- the representation $V_A \otimes_\mathbb{Q} \overline{\mathbb{Q}}$ of $(\mathrm{MT}_A)_{\overline{\mathbb{Q}}}$ decomposes as the direct sum of r irreducible and minuscule representations that each occur with multiplicity m_1,
- each weight in Ω of V_A has multiplicity m_1.

From the above minuscule property, we find that Ω consists of r distinct W-orbits. Fix a W-orbit $\mathcal{O} \subseteq \Omega$ and let H be the stabilizer of $\mathcal{O} \subseteq \Omega$. We have $[\Gamma : H] = r$ since Γ acts transitively on Ω and

hence also transitively on the W-orbits in Ω. Using the natural isomorphism $\mathrm{Gal}(k/\mathbb{Q}) = \Gamma/W$, we let L' be the subfield of k corresponding to the group H/W; it is a number field of degree r. Using the transitivity of the action of Γ again, we find that the number field L', up to isomorphism, does not depend on the choice of $\mathcal{O}$.

In the setting of the proposition, we have $s = s' = 1$, $\Omega_1 = \Omega$, $\mathcal{O}_1 := \mathcal{O}$, $L_1' = L'$ and $\mathfrak{m}_1' = \mathfrak{m}_1$. So to complete the proof in the simple case, it remains to show that the fields L_1 and L' are isomorphic.

Since $\mathrm{Gal}_{L'}$ stabilizes the W-orbit $\mathcal{O}$, we find that there is a representation $U \subseteq V_A \otimes_{\mathbb{Q}} L'$ of $(\mathrm{MT}_A)_{L'}$ whose set of weights is $\mathcal{O}$ and each occurs with multiplicity $\mathfrak{m}_1$ (in particular, $U \otimes_{L'} \overline{\mathbb{Q}} \subseteq V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is an isotypic representation of $(\mathrm{MT}_A)_{\overline{\mathbb{Q}}}$). So $L \otimes_{\mathbb{Q}} L'$ acts on the L'-vector space U by homotheties. In particular, the homomorphism $L \otimes_{\mathbb{Q}} L' \to L'$ induced by this action gives an embedding $L \hookrightarrow L'$ of fields. Since L and L' are both number fields of degree r, we deduce that they are isomorphic.

Now consider the case where $s = 1$, i.e., $A = C_1^{e_1}$ with $e_1 \geqslant 1$ and C_1 a simple abelian variety over $\mathbb{C}$. We have $V_A = V_{C_1}^{\oplus e_1}$ and the action of MT_{C_1} on V_A induces an isomorphism $\mathrm{MT}_{C_1} = \mathrm{MT}_A$. In particular, MT_{C_1} and MT_A have the same root datum and the same set of weights Ω. For $\alpha \in \Omega$, the multiplicity of α as a weight of MT_A acting on V_A is e_1 times the multiplicity as a weight of MT_{C_1} acting on V_{C_1}. So using the previous case, it suffices to show that the rings $B_1 = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $B' := \mathrm{End}(C_1) \otimes_{\mathbb{Z}} \mathbb{Q}$ have isomorphic centers and that $\dim_{\mathbb{Q}} B_1 = e_1^2 \dim_{\mathbb{Q}} B'$. This is clear since $B_1 \cong M_{e_1}(B')$.

Finally, we consider the general case. We have $V_A = \bigoplus_{i=1}^s V_{A_i}$ which induces a homomorphism $\mathrm{MT}_A \hookrightarrow \prod_{i=1}^s \mathrm{MT}_{A_i}$ such that each projection $\mathrm{MT}_A \to \mathrm{MT}_{A_i}$ is surjective. Note that V_{A_i} is a representation of MT_A and agrees with the action via the natural homomorphism $\mathrm{MT}_A \to \mathrm{MT}_{A_i}$. This induces surjective homomorphisms

$$W \to W(\mathrm{MT}_{A_i}, T_i) \quad \text{and} \quad \Gamma/W \to \Gamma(\mathrm{MT}_{A_i}, T_i)/W(\mathrm{MT}_{A_i}, T_i),$$

where T_i is the image of T.

Let $\Omega_i \subseteq X(T)$ be the set of weights of the representation V_{A_i}; it is stable under the Γ-action. Choose any W-orbit $\mathcal{O}_i \subseteq \Omega_i$ and let H_i be the subgroup of Γ that stabilizes $\mathcal{O}_i$. From the previous cases, we find that Γ acts transitively on Ω_i, each weight $\alpha \in \Omega_i$ of the representation V_{A_i} has multiplicity $\mathfrak{m}_i$, and L_i is isomorphic to the subfield of k fixed by $H_i/W \subseteq \Gamma/W = \mathrm{Gal}(k/\mathbb{Q})$.

We claim that the sets Ω_i are pairwise disjoint. Assuming the claim, we find that sets $\Omega_1, \ldots, \Omega_s$ are the Γ-orbits of Ω and each $\alpha \in \Omega_1$ has multiplicity $\mathfrak{m}_i$ as a weight of V_A. By reordering the A_i, we may assume that these are the same Γ-orbits as in the setup of the proposition and hence $s' = s$. We now have $\mathfrak{m}_i' = \mathfrak{m}_i$ and the field L_i' is isomorphic to L_i.

It remains to prove the claim. Suppose that there are nondisjoint Ω_i and Ω_j with $1 \leqslant i < j \leqslant s$. We have $\Omega_i = \Omega_j$ since they are transitive Γ-sets. The representations $V_{A_i}^{\oplus \mathfrak{m}_j}$ and $V_{A_j}^{\oplus \mathfrak{m}_i}$ of MT_A thus have the same weights and multiplicities, and so are isomorphic. In particular, this implies that there is a nonzero linear map $V_{A_i} \to V_{A_j}$ that respects the MT_A-actions. However, since $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ agrees with the subring of $\mathrm{End}(V_A)$ that commutes with the MT_A-action, we deduce that there is a nonzero homomorphism $A_i \to A_j$ of abelian varieties. This is impossible since A_i and A_j are powers of nonisogenous simple abelian varieties. This contradiction proves the claim.

References

[And96] Yves André, *Pour une théorie inconditionnelle des motifs*, Inst. Hautes Études Sci. Publ. Math. **83** (1996), 5–49 (French). MR1423019 ↑1, 4.2

[BGK10] Grzegorz Banaszak, Wojciech Gajda, and Piotr Krasoń, *On the image of Galois l-adic representations for abelian varieties of type III*, Tohoku Math. J. (2) **62** (2010), no. 2, 163–189, DOI 10.2748/tmj/1277298644. MR2663452 ↑1.8

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR2062673 ↑1.3, 4.1

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑1.6, 7.1.1

[Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968 (French). MR0240238 ↑7.1.1, 7.1.1

[Bou75] ———, *Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées*, Actualités Scientifiques et Industrielles, No. 1364. Hermann, Paris, 1975 (French). MR0453824 ↑7.1.1

[CFC19] Victoria Cantoral Farfán and Johan Commelin, *The Mumford-Tate conjecture implies the algebraic Sato-Tate conjecture of Banaszak and Kedlaya* (2019). arXiv:1905.04086. ↑1

[CFS19] Edgar Costa, Francesc Fité, and Andrew V. Sutherland, *Arithmetic invariants from Sato-Tate moments*, C. R. Math. Acad. Sci. Paris **357** (2019), no. 11-12, 823–826, DOI 10.1016/j.crma.2019.11.008 (English, with English and French summaries). MR4038255 ↑1.11

[CLV19] Edgar Costa, Davide Lombardo, and John Voight, *Identifying central endomorphisms of an abelian variety via Frobenius endomorphisms* (2019). arXiv:1906.02803. ↑i

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), no. 317, 1303–1339, DOI 10.1090/mcom/3373. MR3904148 ↑1.8

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982. ↑4.2

[Els16] Andreas-Stephan Elsenhans, *Computation of Galois groups in* `magma`, Mathematical and computational approaches in advancing modern science and engineering, Springer, [Cham], 2016, pp. 621–628. MR3838226 ↑9.1

[EG20] Melissa Emory and Heidi Goodson, *Sato–Tate Distributions of $y^2 = x^p − 1$ and $y^2 = x^{2p} − 1$* (2020). arXiv:2004.10583. ↑1.9

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381]. ↑3.1

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442, DOI 10.1112/S0010437X12000279. MR2982436 ↑1.9

[FKS19] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato–Tate groups of abelian threefolds: a preview of the classification* (2019). arXiv:1911.02071. ↑1.9

[FLGS18] Francesc Fité, Elisa Lorenzo García, and Andrew V. Sutherland, *Sato-Tate distributions of twists of the Fermat and the Klein quartics*, Res. Math. Sci. **5** (2018), no. 4, Paper No. 41, 40, DOI 10.1007/s40687-018-0162-0. MR3864839 ↑1.9

[FS14] Francesc Fité and Andrew V. Sutherland, *Sato-Tate distributions of twists of $y^2 = x^5 − x$ and $y^2 = x^6 + 1$*, Algebra Number Theory **8** (2014), no. 3, 543–585, DOI 10.2140/ant.2014.8.543. MR3218802 ↑1.9

[FS16] ———, *Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 − cx$*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 103–126, DOI 10.1090/conm/663/13351. MR3502940 ↑1.9

[LP95] Michael Larsen and Richard Pink, *Abelian varieties, l-adic representations, and l-independence*, Math. Ann. **302** (1995), no. 3, 561–579. ↑1.6, 1.8, 4.2

[LP97] ———, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. ↑3.1, 3.3

[Mil17] J. S. Milne, *Algebraic groups*, Cambridge Studies in Advanced Mathematics, vol. 170, Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field. MR3729270 ↑2.9

[Noo95] Rutger Noot, *Classe de conjugaison du Frobenius des variétés abéliennes à réduction ordinaire*, Ann. Inst. Fourier (Grenoble) **45** (1995), no. 5, 1239–1248 (French, with English and French summaries). MR1370746 ↑1.6, 4.3

[Noo09] ———, *Classe de conjugaison du Frobenius d'une variété abélienne sur un corps de nombres*, J. Lond. Math. Soc. (2) **79** (2009), no. 1, 53–71. ↑4.3

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263 ↑1, 7.1.2

[Poh68] Henry Pohlmann, *Algebraic cycles on abelian varieties of complex multiplication type*, Ann. of Math. (2) **88** (1968), 161–180, DOI 10.2307/1970570. MR228500 ↑1.7

[Rag04] M. S. Raghunathan, *Tori in quasi-split-groups*, J. Ramanujan Math. Soc. **19** (2004), no. 4, 281–287. MR2125504 ↑2.9

[Ser77] Jean-Pierre Serre, *Représentations ℓ-adiques*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), 1977, pp. 177–193. ↑4.2

[Ser79] _____, *Groupes algébriques associés aux modules de Hodge-Tate*, Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Astérisque, vol. 65, Soc. Math. France, Paris, 1979, pp. 155–188 (French). MR563476 ↑4.4, 10

[Ser94] _____, *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques*, Motives (Seattle, WA, 1991), 1994, pp. 377–400. ↑1.2, ii

[Ser98] _____, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute; Revised reprint of the 1968 original. MR1484415 ↑

[Ser00] _____, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. ↑3.1, 6.2

[Ser03] _____, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440 (electronic). ↑6.2

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, DOI 10.2307/1970722. MR236190 ↑1.7

[Shi81] Tetsuji Shioda, *Algebraic cycles on abelian varieties of Fermat type*, Math. Ann. **258** (1981/82), no. 1, 65–80, DOI 10.1007/BF01450347. MR641669 ↑1.7, 1.16

[Spr79] T. A. Springer, *Reductive groups*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–27. MR546587 ↑2

[Yu15] Chia-Fu Yu, *A note on the Mumford-Tate conjecture for CM abelian varieties*, Taiwanese J. Math. **19** (2015), no. 4, 1073–1084, DOI 10.11650/tjm.19.2015.4730. MR3384679 ↑1.7

[Zyw14] David Zywina, *The splitting of reductions of an abelian variety*, Int. Math. Res. Not. IMRN **18** (2014), 5042–5083, DOI 10.1093/imrn/rnt113. MR3264675 ↑1.5, 1.8, 6.2, 6.2

[Zyw19] _____, *An effective open image theorem for abelian varieties* (2019). arXiv:1910.14171. ↑1.15

[Zyw20] _____, GitHub repository related to *Determining monodromy groups of abelian varieties*, 2020. https://github.com/davidzywina/monodromy. ↑

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA

E-mail address: zywina@math.cornell.edu

URL: http://www.math.cornell.edu/~zywina