Subvarieties of Shimura varieties.*

Bas Edixhoven Andrei Yafaev

May 29, 2001

Contents

*Both authors were partially supported by the European Research Training Network Contract HPRN-CT-2000-00120 "arithmetic algebraic geometry". Adresses: IRMAR, Campus de Beaulieu, 35042 Rennes cedex, France; edix@maths.univ-rennes1.fr, ayafaev@maths.univ-rennes1.fr

1 Introduction.

The aim of this article is to prove a special case of the following conjecture of André and Oort on subvarieties of Shimura varieties. For the terminology, notation, history and results obtained so far we refer to the introduction of [8], and the references therein.

Conjecture 1.1 (André-Oort) *Let (G, X) be a Shimura datum. Let K be a compact open subgroup of $G(\mathbb{A}_\mathrm{f})$ and let S be a set of special points in $\mathrm{Sh}_K(G, X)(\mathbb{C})$. Then every irreducible component of the Zariski closure of S in $\mathrm{Sh}_K(G, X)_\mathbb{C}$ is a subvariety of Hodge type.*

The choice of the special case that we will prove is motivated by work of Wolfart [20], (see also Cohen and Wüstholz [4]) on algebraicity of values of hypergeometric functions at algebraic numbers. The hypergeometric functions considered in [20] are the multi-valued holomorphic $F(a, b, c)$ on $\mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$ defined by:

$$F(a,b,c)(z) = 1 + \frac{ab}{c}z + \frac{a(a+1)b(b+1)}{c(c+1)}\frac{z^2}{2!} + \cdots, \quad z \in \mathbb{C}, \quad |z| < 1,$$

with a, b and c rational numbers, $-c$ not in $\mathbb{N}$. For the following properties of the $F(a, b, c)$ the reader is referred to [20]. The functions $F(a, b, c)$ satisfy the differential equations:

$$z(z-1)F(a,b,c)'' + ((a+b+1)z - c)F(a,b,c)' + abF(a,b,c) = 0.$$

Suppose from now on that a, b, c, $a - c$ and $b - c$ are all not integers. Then, up to a factor in $\overline{\mathbb{Q}}^*$, $F(a, b, c)(z)$ is a quotient of a certain period $P(a, b, c)(z)$ of a certain sub abelian variety $A(a, b, c, z)$ of the jacobian of the smooth projective model of the curve given by the equation $y^N = x^A(1 - x)^B(1 - zx)^C$, for suitable N, A, B, and C depending on (a, b, c), by a period $P_0(a, b, c)$ depending only on (a, b, c). More precisely, $P(a, b, c)(z)$ is the integral of the differential form $y^{-1}dx$ (all of whose residues are zero) over a suitable cycle. The fixed period $P_0(a, b, c)$ is a period of an abelian variety of CM type. Using a theorem of Wüstholz [21, Thm. 5] (on Grothendieck's conjecture on the relation between relations between periods and correspondences (see [1]) in the case of abelian varieties) it follows that if z and one value of $F(a, b, c)$ at z are algebraic, then $A(a, b, c, z)$ is also of CM type, with the same type as $P_0(a, b, c)$, and hence all values of $F(a, b, c)$ at z are algebraic. Because of this, it makes sense to ask the following question:

> under what conditions on (a, b, c) is the set $E(a, b, c)$ of z in $\mathbb{P}^1(\overline{\mathbb{Q}}) - \{0, 1, \infty\}$ such that $F(a, b, c)(z)$ is in $\overline{\mathbb{Q}}$ finite?

Wolfart proposes in [20, Theorem] that the answer should depend only on the monodromy group $\Delta(a,b,c)$ (with its two-dimensional representation) of the differential equation. If this monodromy group is finite, then $F(a,b,c)$ is algebraic over $\overline{\mathbb{Q}}(z)$, and hence $E(a,b,c)$ equals $\mathbb{P}^1(\overline{\mathbb{Q}}) - \{0,1,\infty\}$. Suppose now that the monodromy group is infinite. Then one distinguishes two cases: $\Delta(a,b,c)$ is arithmetic or not. In terms of Shimura varieties, these two cases correspond to the image of $\mathbb{P}^1(\mathbb{C}) - \{0,1,\infty\}$ in a suitable moduli space of polarized abelian varieties under the map that sends z to the isomorphism class of $A(a,b,c,z)$ being of Hodge type or not. If this image is of Hodge type, then the set of z in $\overline{\mathbb{Q}}$ such that $A(a,b,c,z)$ is of CM type with type that of $P_0(a,b,c)$ is dense in $\mathbb{P}^1(\mathbb{C})$ (even for the Archimedean topology), and Wolfart shows that under certain additional conditions on (a,b,c) the set $E(a,b,c)$ is infinite. Suppose now that the image of $\mathbb{P}^1(\mathbb{C}) - \{0,1,\infty\}$ is not of Hodge type. Then Wolfart's Theorem claims that $E(a,b,c)$ is finite. But Walter Gubler has pointed out an error in Wolfart's proof: in [20, §9], there is no reason that the group $\overline{\Delta}$ fixes the image of $\mathbb{H}$ in the product of copies of the unit disk under the product of the maps D_ω, and therefore the identity $\delta^\sigma(f(w)) = f(\delta(w))$ for δ in $\overline{\Delta}$ is not proved.

Since by Wüstholz's theorem all $A(a,b,c,z)$ with z in $E(a,b,c)$ are of a fixed CM type, hence isogeneous and hence contained in one Hecke orbit, the following theorem completes Wolfart's program.

Theorem 1.2 *Let (G,X) be a Shimura datum and let K be a compact open subgroup of $G(\mathbb{A}_f)$. Let V be a finite dimensional faithful representation of G, and for h in X let V_h be the corresponding $\mathbb{Q}$-Hodge structure. For $x = \overline{(h,g)}$ in $\mathrm{Sh}_K(G,X)(\mathbb{C})$, let $[V_x]$ denote the isomorphism class of V_h. Let Z be an irreducible closed algebraic curve contained in $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ such that $Z(\mathbb{C})$ contains an infinite set of special points x such that all $[V_x]$ are equal. Then Z is of Hodge type. In particular, if Z is an irreducible closed algebraic curve contained in $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ such that $Z(\mathbb{C})$ contains an infinite set of special points that lie in one Hecke orbit, then Z is of Hodge type.*

This theorem, in the case where the special points in question lie in one Hecke orbit, was first proved in the second author's thesis [22], in which one chapter (providing a lower bound for Galois orbits) was written by the first author. The main difference between this article and the thesis is that now we consider isomorphism classes of $\mathbb{Q}$-Hodge structures in stead of Hecke orbits. This makes it possible to reduce the proof of the theorem to the case where Z is Hodge generic and G of adjoint type (the proof in the thesis could not achieve this and was therefore more difficult to follow).

The proof given in this article is nice because it is entirely in "(G,X)-language"; the main tools are algebraic groups and their groups of adelic points. But it is not completely satisfactory in the sense that it should be possible to proceed as in [8], i.e., without distinguishing the two cases as we do in Section 7. On the other hand, the proof in the first of these two cases can lead to a generalization to arbitrary Shimura varieties of Moonen's result in [14, §5] (Conjecture 1.1 for moduli spaces of abelian varieties, and sets of special points for which there is a prime at which they are all "canonical"). Finally, it would be nice to replace the condition that all $[V_x]$ are the same in the theorem above by the condition that all associated Mumford-Tate groups are isomorphic (this would give a statement that does not depend on the choice of a representation).

2 The strategy.

The aim of this section is to explain the strategy of the proof of Theorem 1.2. In Sections 4–6 we will prove the necessary ingredients, that will then be put together in Section 7.

We observe that the compact open subgroup K in Conjecture 1.1 is irrelevant: for (G, X) a Shimura datum, K and K' open compact in $G(\mathbb{A}_{\mathrm{f}})$ with $K \subset K'$, an irreducible subvariety Z of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ is of Hodge type if and only if its image in $\mathrm{Sh}_{K'}(G, X)_{\mathbb{C}}$ is. A bit more general: if moreover g is in $G(\mathbb{A}_{\mathrm{f}})$ and T_g is the correspondence from $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ to $\mathrm{Sh}_{K'}(G, X)_{\mathbb{C}}$ induced by g, then Z is of Hodge type if and only if one (or equivalently, all) of the irreducible components of $T_g Z$ is (are) of Hodge type. Another observation is that the irreducible components of intersections of subvarieties of Hodge type are again of Hodge type (this is clear from the interpretation of subvarieties of Hodge type as loci where certain classes are Hodge classes). Hence there does exist a smallest subvariety of Hodge type of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ that contains Z; our first concern is now to describe that subvariety.

Proposition 2.1 *Let (G, X) be a Shimura datum, K a compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$ and let Z be a closed irreducible subvariety of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$. Let s in Z be Hodge generic. Let (x, g) in $X \times G(\mathbb{A}_{\mathrm{f}})$ lie over s, and let G' be the Mumford-Tate group of x. Then we have a morphism of Shimura data from (G', X') to (G, X) with X' the $G'(\mathbb{R})$-conjugacy class of x. Let K' be the intersection of $G'(\mathbb{A}_{\mathrm{f}})$ and gKg^{-1}. Then the inclusion of G' in G, followed by right multiplication by g induces a morphism $f\colon \mathrm{Sh}_{K'}(G', X')_{\mathbb{C}} \to \mathrm{Sh}_K(G, X)_{\mathbb{C}}$. This morphism is finite and its image contains Z. Let Z' be an irreducible component of $f^{-1}Z$. Then Z is of Hodge type if and only if Z' is.*

Proof. This follows from Proposition 2.8 and Section 2.9 of [13]. □

Proposition 2.1 shows that Conjecture 1.1 is true if and only if it is true for S whose Zariski closure is irreducible and Hodge generic. Similarly, Proposition 2.1 reduces the proof of Theorem 1.2 to the case where Z is Hodge generic. We note that even if $Z(\mathbb{C})$ has an infinite intersection with the Hecke orbit of a special point, this is not necessarily so for Z', because the inverse image in $\mathrm{Sh}_{K'}(G', X')_{\mathbb{C}}$ of a Hecke orbit in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ is a disjoint union of a possibly infinite number of Hecke orbits. This explains why we work with equivalence classes of $\mathbb{Q}$-Hodge structures.

Proposition 2.2 *Let (G, X) be a Shimura datum, let G^{ad} be the quotient of G by its center, and let X^{ad} be the $G^{\mathrm{ad}}(\mathbb{R})$-conjugacy class of morphisms from $\mathbb{S}$ to $G^{\mathrm{ad}}_{\mathbb{R}}$ that contains the image of X. Let K^{ad} be a compact open subgroup of $G^{\mathrm{ad}}(\mathbb{A}_{\mathrm{f}})$, and let K be a compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$ whose image in $G^{\mathrm{ad}}(\mathbb{A}_{\mathrm{f}})$ is contained in K^{ad}. Then the induced morphism from $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ to $\mathrm{Sh}_{K^{\mathrm{ad}}}(G^{\mathrm{ad}}, X^{\mathrm{ad}})_{\mathbb{C}}$ is finite. Let Z be a closed irreducible subvariety of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$, and let Z^{ad} be its image in $\mathrm{Sh}_{K^{\mathrm{ad}}}(G^{\mathrm{ad}}, X^{\mathrm{ad}})_{\mathbb{C}}$. Then Z is of Hodge type if and only if Z^{ad} is.*

Proof. By [13, §2.1], X is just a union of connected components of X^{ad}. Let S and S^{ad} be the connected components of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ and of $\mathrm{Sh}_{K^{\mathrm{ad}}}(G^{\mathrm{ad}}, X^{\mathrm{ad}})_{\mathbb{C}}$ that contain Z and Z^{ad}, respectively. Let X^+ be a connected component of X and let g in $G(\mathbb{A}_{\mathrm{f}})$ be such that S is the image in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ of $X^+ \times \{g\}$. Then the inverse images of Z and Z^{ad} in $X^+ \times \{g\}$ are equal, hence the property of being of Hodge type for them is equivalent. □

We want to use Proposition 2.2 to reduce the proof of Theorem 1.2 to the case where G is semi-simple of adjoint type. In order to do that, all we need to do is to construct a faithful representation W of G^{ad} such that $Z^{\mathrm{ad}}(\mathbb{C})$ contains a Zariski dense set of special points x with all $[W_x]$ equal.

Construction 2.3 *Let G be a reductive algebraic group over $\mathbb{Q}$ and let V be a faithful finite dimensional representation. Let E be a finite extension of $\mathbb{Q}$ such that the representation V_E of G_E is a direct sum $V_1 \oplus \cdots \oplus V_r$ with each V_i absolutely irreducible. Let C be the center of G; then C_E acts via a character χ_i on V_i. For each i, we let $d_i = \dim_E(V_i)$, and we define $W_i := V_i^{\otimes_E d_i} \otimes_E \det_E(V_i)^*$. Then $W := W_1 \oplus \cdots \oplus W_r$ is a faithful representation of G^{ad}_E. We get a faithful representation of G^{ad} on W as $\mathbb{Q}$-vector space via the sequence of injective morphisms of algebraic groups:*

$$G^{\mathrm{ad}} \to \mathrm{Res}_{E/\mathbb{Q}} G^{\mathrm{ad}}_E \to \mathrm{Res}_{E/\mathbb{Q}} \mathbf{GL}_E(W) \to \mathbf{GL}_{\mathbb{Q}}(W).$$

Suppose now that Σ is a Zariski dense subset of X such that the $\mathbb{Q}$-Hodge structures V_x with x in Σ are all isomorphic to a fixed $\mathbb{Q}$-Hodge structure H. Then the $\mathbb{Q}$-Hodge structures with E-coefficients $E \otimes V_x$ are all isomorphic to $E \otimes H$. Now $E \otimes H$ is a direct sum of finitely many simple $\mathbb{Q}$-Hodge structures with E-coefficients. Hence there are, up to isomorphism, only finitely many ways to decompose $E \otimes H$ into a direct sum of r terms. Hence Σ is a finite disjoint union of subsets Σ_i such that for each i the $E \otimes V_x = V_{1,x} \oplus \cdots \oplus V_{r,x}$ with x in Σ_i are all isomorphic term by term. It follows that the W_x with x in Σ_i are all isomorphic. So it remains to prove Theorem 1.2 in the case where G is semi-simple of adjoint type and Z Hodge generic.

At this point we can describe the strategy of the proof of the main result. So let the notation now be as in Theorem 1.2, and suppose that G is semi-simple of adjoint type, that Z is Hodge generic, and that K is neat. Let Σ be an infinite subset of special points of Z such that all $[V_x]$ with x in Σ are equal. Let S be the irreducible component of $\mathrm{Sh}_K(G, X)$ that contains Z. We will show that there exist g in $G(\mathbb{A}_{\mathrm{f}})$ such that an irreducible component T_g^0 of the Hecke correspondence on S induced by g has the property that $T_g^0 Z = Z = T_{g^{-1}}^0 Z$ (with $T_{g^{-1}}^0$ the transpose of T_g^0) and is such that all the $T_g^0 + T_{g^{-1}}^0$-orbits in S are dense (for the Archimedean topology). This clearly implies that $Z = S$, so that Z is of Hodge type.

To find such a g, we proceed as follows. We will take g in $G(\mathbb{Q}_p)$, for some prime number p. For all but finitely many p, the image of Z under each irreducible component of any T_g with g in $G(\mathbb{Q}_p)$ is either empty or irreducible. The proof of this will be given in Section 5, its main ingredient is Theorem 5.2 by Nori. The density of all $T_g^0 + T_{g^{-1}}^0$-orbits will be proved in Section 6, under the assumption that no image of g under projection to a simple factor H of G is contained in a compact subgroup of $H(\mathbb{Q}_p)$. To get the equalities $T_g^0 Z = Z$ and $T_{g^{-1}}^0 Z = Z$ we try to find g such that $T_g Z \cap Z$ contains a large number of the given special points, compared to the degree of the correspondence T_g. In doing this, we distinguish two cases. In one case, the intersection will contain at least one big Galois orbit. In the other case, it contains infinitely many of the given special points. The main ingredient here is the description of the Galois action on special points, plus a lower bound on the number of points in the Galois orbits of our given special points that will be established in Section 4.

3 Some preliminaries.

3.1 Mumford-Tate groups.

For V a free $\mathbb{Z}$-module of finite rank, we define $\mathbf{GL}(V)$ to be the group scheme given by $\mathbf{GL}(V)(A) = \mathrm{GL}_A(V_A)$ for all rings A. For h a $\mathbb{Z}$-Hodge structure, i.e., a free $\mathbb{Z}$-module of finite rank, together with a morphism $h\colon \mathbb{S} \to \mathbf{GL}(V)_{\mathbb{R}}$, we let $\mathrm{MT}(V, h)$ be the Zariski closure in $\mathbf{GL}(V)$ of the usual Mumford-Tate group $\mathrm{MT}(V_{\mathbb{Q}}, h)$ in $\mathbf{GL}(V)_{\mathbb{Q}}$.

3.2 Variations of $\mathbb{Z}$-Hodge structure on Shimura varieties.

Let (G, X) be a Shimura datum, K a neat compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$ and $\rho\colon G \to \mathrm{GL}_n$ a representation that factors through $G \to G^{\mathrm{ad}}$, such that $\rho(K)$ is in $\mathrm{GL}_n(\hat{\mathbb{Z}})$. Then there is a variation of $\mathbb{Z}$-Hodge structures V on $\mathrm{Sh}_K(G,X)$ constructed as follows. On $X \times G(\mathbb{A}_{\mathrm{f}})/K$, we consider the variation of $\mathbb{Z}$-Hodge structure V_1 whose restriction to $X \times \{\overline{g}\}$ is $\mathbb{Q}^n \cap \rho(g)(\hat{\mathbb{Z}}^n) \times X$ (with the $\mathbb{Q}$-Hodge structure on $\mathbb{Q}^n \times \{x\}$ is given by the morphism $\rho_{\mathbb{R}} \circ x$ from $\mathbb{S}$ to $\mathrm{GL}_{n,\mathbb{R}}$). Then $G(\mathbb{Q})$ acts on V_1, and the quotient is the V that we want (for each $(x, \overline{g})$ in $X \times G(\mathbb{A}_{\mathrm{f}})/K$ and q in $G(\mathbb{Q})$ that stabilizes $(x, \overline{g})$, the image of q in $G^{\mathrm{ad}}(\mathbb{Q})$ is trivial, hence $\rho(q)$ is the identity).

A more conceptual way to describe V is as follows. We consider two actions of $G(\mathbb{Q}) \times G(\mathbb{A}_{\mathrm{f}})$ on $\mathbb{A}_{\mathrm{f}}^n \times X \times G(\mathbb{A}_{\mathrm{f}})$ given by:

$$\begin{aligned}(q,k) *_1 (v,x,g) &= (qv, qx, qgk),\\ (q,k) *_2 (v,x,g) &= (k^{-1}v, qx, qgk).\end{aligned}$$

The first action stabilizes $\mathbb{Q}^n \times X \times G(\mathbb{A}_{\mathrm{f}})$, and the second stabilizes $\hat{\mathbb{Z}}^n \times X \times G(\mathbb{A}_{\mathrm{f}})$. The quotient by the first action gives a locally constant sheaf $V_{\mathbb{Q}}$ of $\mathbb{Q}$-vector spaces on $\mathrm{Sh}_K(G,X)(\mathbb{C})$, and the second one a locally constant sheaf $V_{\hat{\mathbb{Z}}}$ of $\hat{\mathbb{Z}}$-modules. The automorphism:

$$\mathbb{A}_{\mathrm{f}}^n \times X \times G(\mathbb{A}_{\mathrm{f}}) \longrightarrow \mathbb{A}_{\mathrm{f}}^n \times X \times G(\mathbb{A}_{\mathrm{f}}), \quad (v,x,g) \mapsto (g^{-1}v, x, g)$$

transforms the first action into the second, hence gives an isomorphism between the two locally constant sheaves of $\mathbb{A}_{\mathrm{f}}$-modules on $\mathrm{Sh}_K(G,X)(\mathbb{C})$. Then V is the "intersection" of $V_{\mathbb{Q}}$ and $V_{\hat{\mathbb{Z}}}$ in $V_{\mathbb{A}_{\mathrm{f}}}$.

3.3 Representations of tori.

A torus over a scheme S is an S-group scheme T that is of the form $\mathbb{G}_{\mathrm{m}S}^r$, locally for the fpqc topology on S ([7, Exp. IX, Déf. 1.3]). If S is normal and noetherian, then a torus T/S is split over a suitable surjective finite etale cover of $S' \to S$, i.e., $T_{S'}$ is isomorphic to some $\mathbb{G}_{\mathrm{m}S'}^r$ ([7, Exp. IX, Thm. 5.16]); one may take $S' \to S$ Galois and S' connected. If S is integral normal and noetherian, with generic point η, then any isomorphism $f\colon T_{1,\eta} \to T_{2,\eta}$ with T_1 and T_2 tori over S extends uniquely to an isomorphism over S (use [7, Exp. X, Cor. 1.2]).

For S a connected scheme, $T \cong \mathbb{G}_{\mathrm{m}S}^r$ a split torus and V an $\mathcal{O}_S$-module, it is equivalent to give a T-action on V or an X-grading on V, with $X = \mathrm{Hom}(T, \mathbb{G}_{\mathrm{m}S})$ the character group of T ([7, Exp. I, §4.7]).

Suppose now that S is an integral normal noetherian scheme, that T is a torus over S and that $\pi\colon S' \to S$ is a connected finite etale Galois cover with group Γ over which T is split. Let X

be the character group of $T_{S'}$; then X is a free $\mathbb{Z}$-module of finite rank with a Γ-action. Then, to give an action of T on a quasi-coherent $\mathcal{O}_S$-module V is equivalent to giving an X-grading $V_{S'} = \pi^* V = \oplus_x V_{S',x}$ such that for all γ in Γ and all x in X one has $\gamma V_{S',x} = V_{S',\gamma x}$ (to see this, use finite etale descent of quasi-coherent modules as in [3, §6.2]). If V and W are two representations of T on locally free $\mathcal{O}_S$-modules of finite rank, then V and W are isomorphic, locally for the Zariski topology on S, if and only if for all x in X the ranks of $V_{S',x}$ and $W_{S',x}$ are equal (use that $\mathrm{Hom}_{\mathcal{O}_S}(V,W)^T$ is a direct summand of $\mathrm{Hom}_{\mathcal{O}_S}(V,W)$, whose formation commutes with base change).

Lemma 3.3.1 *Let p be a prime number, let T be a torus over $\mathbb{Z}_p$, let V be a free $\mathbb{Z}_p$-module of finite rank equipped with a faithful action of $T_{\mathbb{Q}_p}$ on $V_{\mathbb{Q}_p}$. Let T' be the scheme theoretic closure of $T_{\mathbb{Q}_p}$ in $\mathbf{GL}(V)$. Then the following conditions are equivalent:*

1. *$T'_{\mathbb{F}_p}$ is a torus;*
2. *T' is a torus;*
3. *the action of $T_{\mathbb{Q}_p}$ on $V_{\mathbb{Q}_p}$ extends to an action of T on V;*
4. *T stabilizes the lattice V in the sense that for all finite extensions K of $\mathbb{Q}_p$ the lattice V_{O_K} is fixed by all elements of $T(O_K)$.*

The set of $\mathbb{Z}_p$-lattices in $V_{\mathbb{Q}_p}$ that are fixed by T form exactly one orbit under $C(\mathbb{Q}_p)$, where C denotes the centralizer of T in $\mathbf{GL}(V)$.

Proof. Suppose first that $T'_{\mathbb{F}_p}$ is a torus. Then T', being a flat group scheme affine and of finite type over $\mathbb{Z}_p$ whose fibers over $\mathbb{F}_p$ and $\mathbb{Q}_p$ are tori, is a torus by [7, Exp. X, Cor. 4.9].

Suppose that T' is a torus. Then $T' = T$ by [7, Exp. X, Cor. 1.2]). Hence the action of $T_{\mathbb{Q}_p}$ on $V_{\mathbb{Q}_p}$ extends to an action of T on V.

Now suppose that the action of $T_{\mathbb{Q}_p}$ on $V_{\mathbb{Q}_p}$ extends to an action of T on V. Then T stabilizes V, by definition. Also, the description above of representations of tori shows that T acts faithfully on V, so that T is a closed subscheme of $\mathbf{GL}(V)$, flat over $\mathbb{Z}_p$, and hence equal to the scheme theoretic closure of its generic fiber. So $T' = T$ and $T'_{\mathbb{F}_p}$ is a torus.

Finally, suppose that T stabilizes V. Let K be the splitting field of $T_{\mathbb{Q}_p}$. Then T_{O_K} is a split torus, and the action of $T_{\mathbb{Q}_p}$ on $V_{\mathbb{Q}_p}$ is given by an X-grading of V_K, where X is the character group of T_K. Let m be an integer that is prime to p such that the characters x in X with $V_{K,x} \neq 0$ have distinct images in X/mX. Since T stabilizes V, the m-torsion subgroup scheme $T[m]$ of T acts on V. This action corresponds to an X/mX-grading on V_{O_K} that is compatible with the

X-grading on V_K. Hence the X-grading on V_K extends to an X-grading on V_{O_K}, which shows that the action of $T_{\mathbb{Q}_p}$ on $V_{\mathbb{Q}_p}$ extends to an action of T on V.

Finally, let S be the set of $\mathbb{Z}_p$-lattices in $V_{\mathbb{Q}_p}$ that are fixed by T. Let W be any $\mathbb{Z}_p$-lattice in $V_{\mathbb{Q}_p}$. The $T_{\mathbb{Q}_p}$-action on $W_{\mathbb{Q}_p} = V_{\mathbb{Q}_p}$ corresponds to the X-grading on V_K. By finite etale descent, the O_K-submodule $\oplus_x(W_{O_K} \cap V_{K,x})$ of W_{O_K} is of the form W'_{O_K} for a unique $\mathbb{Z}_p$-lattice W' contained in W. Then W'_{O_K} is the direct sum of the $W'_{O_K} \cap V_{K,x}$, hence is a representation of T. Hence W' is in S; in fact, W' is the largest sublattice of W that is fixed by T. In particular, S is not empty. Let now V_1 and V_2 be two elements of S. Then both are representations of T. Since for each x the $V_{i,O_K,x}$ are of equal rank, V_1 and V_2 are isomorphic as representations of T. Let $g\colon V_1 \to V_2$ be an isomorphism. Then g is an element of $C(\mathbb{Q}_p)$ that sends V_1 to V_2. $\square$

4 Lower bounds for Galois orbits.

The aim of this section is to give certain lower bounds for the sizes of Galois orbits of special points on a Shimura variety. To be precise, we will prove the following theorem.

Theorem 4.1 *Let (G, X) be a Shimura datum, with G semi-simple of adjoint type, and let K be a neat compact open subgroup of $G(\mathbb{A}_f)$. Via a suitable faithful representation we view G as a closed algebraic subgroup of $\mathrm{GL}_{n,\mathbb{Q}}$, such that K is in $\mathrm{GL}_n(\hat{\mathbb{Z}})$. Let V be the induced variation of $\mathbb{Z}$-Hodge structures on $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$. Let s_0 be a special point of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$. Let $F \subset \mathbb{C}$ be a number field over which the Shimura variety $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ has a canonical model $\mathrm{Sh}_K(G,X)_F$. Then there exist real numbers $c_1 > 0$ and $c_2 > 0$ such that for all s in $\mathrm{Sh}_K(G,X)_F(\overline{\mathbb{Q}})$ such that the $\mathbb{Q}$-Hodge structure $V_{s,\mathbb{Q}}$ is isomorphic to $V_{s_0,\mathbb{Q}}$, we have:*

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s| > c_1 \prod_{\{p \text{ prime} \mid \mathrm{MT}(V_s)_{\mathbb{F}_p} \text{ is not a torus}\}} c_2 p.$$

Let us note that varying F and K does not affect the statement of the theorem: if F' and K' satisfy the same hypotheses as F and K, then the sizes of the Galois orbits differ by a bounded factor, and $K' \cap K$ has finite index in both K and K'. In the course of the proof of Theorem 4.1 we will assume that F is the splitting field of $M_{\mathbb{Q}}$, with M the Mumford-Tate group of s_0.

We note that $M(\mathbb{R})$ is compact: the kernel of the action of $G(\mathbb{R})$ on X consists precisely of the product of the compact factors, i.e., if $G_{\mathbb{R}}$ is the product of simple G_i's, then the kernel is the product of the $G_i(\mathbb{R})$ that are compact, and $M(\mathbb{R})$ stabilizes a point in the hermitian manifold X. It follows that $M(\mathbb{Q})$ is discrete in $M(\mathbb{A}_f)$.

4.2 Galois orbits and Mumford-Tate groups.

Let the notation be as in Theorem 4.1. We choose a set of representatives R in $G(\mathbb{A}_\mathrm{f})$ for the quotient $G(\mathbb{Q})\backslash G(\mathbb{A}_\mathrm{f})/K$; note that R is finite. Then for s in $\mathrm{Sh}_K(G,X)_F(\mathbb{C})$ there exists a unique g_s in R and an element $\tilde{s}$ in X unique up to $\Gamma_s := G(\mathbb{Q}) \cap g_s K g_s^{-1}$, such that $s = \overline{(\tilde{s}, g_s)}$. We fix a choice for $\tilde{s}_0$.

Let $s = \overline{(\tilde{s}, g_s)}$ be in $\mathrm{Sh}_K(G,X)_F(\overline{\mathbb{Q}})$ such that the $\mathbb{Q}$-Hodge structure $V_{s,\mathbb{Q}}$ is isomorphic to $V_{s_0,\mathbb{Q}}$. Then $\tilde{s}$ gives an embedding of the Mumford-Tate group $\mathrm{MT}(s)_\mathbb{Q}$ in G, and an inclusion of Shimura data from $(\mathrm{MT}(s)_\mathbb{Q}, \{\tilde{s}\})$ in (G,X). Note that $\mathrm{MT}(s)_\mathbb{Q}$ is isomorphic to $M_\mathbb{Q}$, hence has splitting field F. This gives morphisms of Shimura varieties over F:

(4.2.1) $$\mathrm{Sh}_{K_s \cap \mathrm{MT}(s)(\mathbb{A}_\mathrm{f})}(\mathrm{MT}(s)_\mathbb{Q})_F \longrightarrow \mathrm{Sh}_{K_s}(G,X)_F \xrightarrow{\cdot g_s} \mathrm{Sh}_K(G,X)_F,$$

with the first one given by the inclusion, the second one by right multiplication by g_s, and with $K_s = K \cap g_s K g_s^{-1}$. By construction, $V_{s,\mathbb{Q}}$ and $V_{s_0,\mathbb{Q}}$ are both $\mathbb{Q}^n$ with Hodge structures $\tilde{s}$ and $\tilde{s}_0 \colon \mathbb{S} \to \mathrm{GL}_{n,\mathbb{R}}$, respectively. Let h in $\mathrm{GL}_n(\mathbb{Q})$ be an automorphism of $\mathbb{Q}^n$ that is an isomorphism from $V_{s_0,\mathbb{Q}}$ to $V_{s,\mathbb{Q}}$. Then we have $\tilde{s} = \mathrm{inn}_h \circ \tilde{s}_0$. It follows that the reciprocity morphisms $r_{\tilde{s}}$ and $r_{\tilde{s}_0}$, viewed as morphisms of tori over $\mathbb{Q}$ from $\mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_{\mathrm{m}F}$ to G with images $\mathrm{MT}(s)_\mathbb{Q}$ and $M_\mathbb{Q}$ are related by: $r_{\tilde{s}} = \mathrm{inn}_h \circ r_{\tilde{s}_0}$. In particular, the isomorphism from $M_\mathbb{Q}$ to $\mathrm{MT}(s)_\mathbb{Q}$ induced by inn_h gives an isomorphism of Shimura varieties over F:

(4.2.2) $$\mathrm{Sh}(M_\mathbb{Q})_F \longrightarrow \mathrm{Sh}(\mathrm{MT}(s)_\mathbb{Q})_F$$

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts on $\mathrm{Sh}(M_\mathbb{Q}) = M(\mathbb{Q})\backslash M(\mathbb{A}_\mathrm{f})$ via its maximal abelian quotient, which we view, via class field theory, as a quotient of $(\mathbb{A} \otimes F)^*/(\mathbb{R} \otimes F)^{*,+}$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is then given by $r_{\tilde{s}_0} \colon \mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_{\mathrm{m}F} \to M_\mathbb{Q}$. We note that $(\mathbb{A} \otimes F)^*/(\mathbb{R} \otimes F)^{*,+}$ is the product of $(\mathbb{A}_\mathrm{f} \otimes F)^*$ and the finite group of connected components of $(\mathbb{R} \otimes F)^*$. Hence the size of the $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$-orbit of s in the $\mathrm{Sh}_K(G,X)_F(\overline{\mathbb{Q}})$ is, up to a bounded factor which is independent of s, the size of the $(\mathbb{A}_\mathrm{f} \otimes F)^*$-orbit. Since $F^{*,+}$ in $(\mathbb{A}_\mathrm{f} \otimes F)^*$ acts trivially, and since the class group $F^*\backslash(\mathbb{A}_\mathrm{f} \otimes F)^*/(\hat{\mathbb{Z}} \otimes O_F)^*$ is finite, proving the lower bound we want for the $(\mathbb{A}_\mathrm{f} \otimes F)^*$-orbits is equivalent to proving it for the $(\hat{\mathbb{Z}} \otimes O_F)^*$-orbits. Moreover, since the set R is finite, and since each $\cdot g_s \colon \mathrm{Sh}_{K_s}(G,X)_F \to \mathrm{Sh}_K(G,X)_F$ is finite, it is enough to prove the lower bound for the $(\hat{\mathbb{Z}} \otimes O_F)^*$-orbit in $\mathrm{Sh}_{K_s}(G,X)_F(\overline{\mathbb{Q}})$.

4.3 Getting rid of G.

In order to simplify our task (i.e., proving Theorem 4.1) we introduce the pair $(\mathrm{GL}_{n,\mathbb{Q}}, Y)$, with Y the $\mathrm{GL}_n(\mathbb{R})$ conjugacy class in $\mathrm{Hom}_\mathbb{R}(\mathbb{S}, \mathrm{GL}_{n,\mathbb{R}})$ that contains the image of X under ρ. Of course, this pair is not a Shimura datum (if $n > 2$).

For $s = \overline{(\tilde{s}, g_s)}$ in $\mathrm{Sh}_K(G,X)_F(\overline{\mathbb{Q}})$ and h in $\mathrm{GL}_n(\mathbb{Q})$ as in the previous section, we consider the following commutative diagram (of sets):

$$\begin{array}{ccc}
\mathrm{Sh}_{K_s\cap \mathrm{MT}(s)(\mathbb{A}_\mathrm{f})}(\mathrm{MT}(s)_\mathbb{Q})(\mathbb{C}) & \longrightarrow & \mathrm{Sh}_{K_s}(G,X)(\mathbb{C}) \xrightarrow{\cdot g_s} \mathrm{Sh}_K(G,X)(\mathbb{C}) \\
{\scriptstyle i_s}\big\uparrow & & \big\downarrow \\
\mathrm{Sh}_{K'_s}(M_\mathbb{Q})(\mathbb{C}) & \xrightarrow{f_s} & \mathrm{GL}_n(\mathbb{Q})\backslash\left(Y\times \mathrm{GL}_n(\mathbb{A}_\mathrm{f})\right)/\mathrm{GL}_n(\hat{\mathbb{Z}}),
\end{array}$$

where K'_s is the subgroup of $M(\mathbb{A}_\mathrm{f})$ that corresponds to $K_s\cap \mathrm{MT}(s)(\mathbb{A}_\mathrm{f})$ via inn_h, so that i_s is bijective, and where f_s is induced by the morphism $(M_\mathbb{Q}, \{s_0\}) \to (\mathrm{GL}_{n,\mathbb{Q}}, Y)$ given by the inclusion of $M_\mathbb{Q}$ in $\mathrm{GL}_{n,\mathbb{Q}}$ followed by inn_h, and $s_0 \mapsto \mathrm{inn}_h\circ\rho\circ s_0$.

The set $\mathrm{GL}_n(\mathbb{Q})\backslash(Y\times\mathrm{GL}_n(\mathbb{A}_\mathrm{f}))/\mathrm{GL}_n(\hat{\mathbb{Z}})$ is the set of isomorphism classes of $\mathbb{Z}$-Hodge structures W such that $W_\mathbb{R}$ is isomorphic to $V_{s_0,\mathbb{R}}$ (to (y,g) in $Y\times\mathrm{GL}_n(\mathbb{A}_\mathrm{f})$ one associates the Hodge structure $y\colon \mathbb{S}\to\mathrm{GL}_{n,\mathbb{R}}$ on the lattice $\mathbb{Q}^n\cap g\hat{\mathbb{Z}}^n$). Its subset of isomorphism classes of W such that $W_\mathbb{Q}$ is isomorphic to $V_{s_0,\mathbb{Q}}$ is in bijection with $S = C(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A}_\mathrm{f})/\mathrm{GL}_n(\hat{\mathbb{Z}})$, where $C_\mathbb{Q}$ is the centralizer in $\mathrm{GL}_{n,\mathbb{Q}}$ of $M_\mathbb{Q}$. Being the centralizer of a torus, $C_\mathbb{Q}$ is connected and reductive (actually, $C_{\overline{\mathbb{Q}}}$ is isomorphic to a product of $\mathrm{GL}_{d_i,\overline{\mathbb{Q}}}$'s).

Note that $M(\mathbb{A}_\mathrm{f})$ acts on S by left-multiplication. The image in S of $(\hat{\mathbb{Z}}\otimes O_F)^*{\cdot}s$ is now simply the $(\hat{\mathbb{Z}}\otimes O_F)^*$-orbit of the class of h, where $(\hat{\mathbb{Z}}\otimes O_F)^*$ acts via $r_{\tilde{s}_0}\colon (\hat{\mathbb{Z}}\otimes O_F)^*\to M(\mathbb{A}_\mathrm{f})$ and left multiplication by $M(\mathbb{A}_\mathrm{f})$. Let $L = \mathrm{GL}_n(\mathbb{A}_\mathrm{f})/\mathrm{GL}_n(\hat{\mathbb{Z}})$ be the set of $\mathbb{Z}$-lattices in $\mathbb{Q}^n$ (or, equivalently, $\hat{\mathbb{Z}}$-lattices in $\mathbb{A}_\mathrm{f}^n$). The following lemma can be seen as a comparison between the sizes of the $M(\hat{\mathbb{Z}})$-orbits $M(\hat{\mathbb{Z}})\overline{h}^S$ and $M(\hat{\mathbb{Z}})\overline{h}^L$ of h in L and in S.

Lemma 4.3.1 *There exists an integer $m\geq 1$ such that for all h in $\mathrm{GL}_n(\mathbb{A}_\mathrm{f})$ we have:*

$$|M(\hat{\mathbb{Z}})\,\overline{h}^S| \geq |M(\hat{\mathbb{Z}})\,\overline{h}^L|, \quad \textit{where } M(\hat{\mathbb{Z}}) \textit{ acts on } L \textit{ via } m\textit{th powers.}$$

Proof. The fact that $C(\mathbb{R})$ is not necessarily compact gives us some trouble, and so we decompose $C_\mathbb{Q}$ up to isogeny. There exists a connected reductive subgroup $M'_\mathbb{Q}$ of $C_\mathbb{Q}$ such that we have a short exact sequence:

$$1\longrightarrow F_\mathbb{Q}\longrightarrow M_\mathbb{Q}\times M'_\mathbb{Q}\longrightarrow C_\mathbb{Q}\longrightarrow 1, \tag{4.3.2}$$

with $F_\mathbb{Q} = M_\mathbb{Q}\cap M'_\mathbb{Q}$ a finite group scheme. To get such an $M'_\mathbb{Q}$, consider the decomposition up to isogeny of $C_\mathbb{Q}$ into its center (that contains $M_\mathbb{Q}$) and its semi-simple part, and use that the center decomposes up to isogeny into $M_\mathbb{Q}$ and another factor. All groups in (4.3.2) are closed subgroup schemes of $\mathrm{GL}_{n,\mathbb{Q}}$, which gives each of them a $\mathbb{Z}$-structure. There is a non-empty open part $\mathrm{Spec}(\mathbb{Z}[1/N])$ of $\mathrm{Spec}(\mathbb{Z})$ over which F is finite etale, M and M' tori, C reductive and the sequence exact (for the etale topology). Let $e \geq 1$ be an integer that annihilates $F_{\mathbb{Q}}$ and $M(\mathbb{Q}) \cap U$, where U is the maximal compact (open) subgroup of $M(\mathbb{A}_{\mathrm{f}})$ (see [17, Prop. 3.16]).

Let h be in $\mathrm{GL}_n(\mathbb{A}_{\mathrm{f}})$. Let x be in $M(\hat{\mathbb{Z}})$ and suppose that x stabilizes $\overline{h}$ in S. Then there exist q in $C(\mathbb{Q})$ and k in $\mathrm{GL}_n(\hat{\mathbb{Z}})$ such that in $\mathrm{GL}_n(\mathbb{A}_{\mathrm{f}})$ we have:

$$xh = qhk, \quad \text{i.e.,} \quad x = q{\cdot}hkh^{-1}. \tag{4.3.3}$$

Since x and q commute, we have:

$$x^e = q^e{\cdot}hk^eh^{-1}. \tag{4.3.4}$$

As $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), F(\overline{\mathbb{Q}}))$ is annihilated by e, there exist q_1 in $M(\mathbb{Q})$ and q_2 in $M'(\mathbb{Q})$ such that $q^e = q_1q_2$ in $C(\mathbb{Q})$. By (4.3.3), hkh^{-1} is in $C(\mathbb{A}_{\mathrm{f}})$. Since the sequence (4.3.2) extends as indicated over $\mathbb{Z}[1/N]$, there are k_1 and k_2 in $\mathrm{GL}_n(\mathbb{A}_{\mathrm{f}})$ such that:

$$hk^eh^{-1} = hk_1h^{-1}{\cdot}hk_2h^{-1}, \quad \text{with } hk_1h^{-1} \text{ in } M(\mathbb{A}_{\mathrm{f}}) \text{ and } hk_2h^{-1} \text{ in } M'(\mathbb{A}_{\mathrm{f}}). \tag{4.3.5}$$

Rewriting (4.3.4) gives:

$$x^e = q_1q_2{\cdot}hk_1h^{-1}{\cdot}hk_2h^{-1} = q_1{\cdot}hk_1h^{-1}{\cdot}q_2hk_2h^{-1}. \tag{4.3.6}$$

It follows that $q_2hk_2h^{-1}$ is in $F(\mathbb{A}_{\mathrm{f}})$, hence that:

$$x^{e^2} = q_1^e{\cdot}hk_1^eh^{-1}, \quad \text{in } M(\mathbb{A}_{\mathrm{f}}). \tag{4.3.7}$$

This identity shows that q_1^e is in $U \cap M(\mathbb{Q})$. Hence q_1 is in $U \cap M(\mathbb{Q})$, and since e annihilates $U \cap M(\mathbb{Q})$, we have:

$$x^{e^2} = hk_1^eh^{-1}, \quad \text{in } M(\mathbb{A}_{\mathrm{f}}). \tag{4.3.8}$$

We conclude that for $m = e^2$, we have, for x in $M(\hat{\mathbb{Z}})$ stabilizing $\overline{h}^S$, that x^m stabilizes $\overline{h}^L$ (for the usual action of $M(\mathbb{A}_{\mathrm{f}})$ on L). $\square$

Lemma 4.3.1 implies that in order to prove Theorem 4.1 we may as well prove the lower bound in question for the action of $M(\hat{\mathbb{Z}})$ on the set L, if we replace the reciprocity morphism $r_{\tilde{s}_0}$ by $mr_{\tilde{s}_0}$, for a suitable $m \geq 1$. Note that $mr_{\tilde{s}_0}$ is still surjective, as morphism of tori over $\mathbb{Q}$.

For h in $\mathrm{GL}_n(\mathbb{A}_{\mathrm{f}})$, its class in L is a $\mathbb{Z}$-lattice V_h in $\mathbb{Q}^n$, and $\mathbb{Q}^n$ is equipped with an action of $M_{\mathbb{Q}}$. Let $\mathrm{MT}(V_h)$ be the scheme theoretic closure of $M_{\mathbb{Q}}$ in $\mathbf{GL}(V_h)$. In this situation, Lemma 3.3.1 says that $\mathrm{MT}(V_h)_{\mathbb{F}_p}$ is a torus if and only if M fixes V_h.

We have reduced the proof of Theorem 4.1 to the following statement, that will be proved in the next section.

Proposition 4.3.9 *Let n be a positive integer. Let T be a torus over $\mathbb{Z}[1/n]$, acting on a free $\mathbb{Z}[1/n]$-module V of finite rank. Let $S = \mathrm{GL}(V_{\mathbb{A}_f})/\mathrm{GL}(V_{\hat{\mathbb{Z}}[1/n]})$ be the set of $\mathbb{Z}[1/n]$-lattices in $V_{\mathbb{Q}}$. Let $T(\hat{\mathbb{Z}}[1/n])$ act on S via left multiplications. For W in S, let P_W be the set of primes p that do not divide n and such that $T_{\mathbb{Z}_p}$ does not fix $W_{\mathbb{Z}_p}$. Then there exists a positive real number c such that for each W in S we have:*

$$|T(\hat{\mathbb{Z}}[1/n])\cdot W| \geq \prod_{p\in P_W} cp.$$

Equivalently, as S is a restricted product over the primes not dividing n, there is a positive real number c such that for all p not dividing n, and all $\mathbb{Z}_p$-lattices W in $V_{\mathbb{Q}_p}$ that are not fixed by $T_{\mathbb{Z}_p}$, we have:

$$|T(\mathbb{Z}_p)\cdot W| \geq cp.$$

4.4 Proof of Proposition 4.3.9.

We will now prove Proposition 4.3.9. Let K be a splitting field of $T_{\mathbb{Q}}$, and let X be the group of characters of T_K. Let p be a prime number that does not divide n, and let W be a $\mathbb{Z}_p$-lattice in $V_{\mathbb{Q}_p}$ that is not fixed by $T_{\mathbb{Z}_p}$. Let W' be the largest sublattice of W that is fixed by $T_{\mathbb{Z}_p}$, as constructed in the last part of the proof of Lemma 3.3.1. Let L be the kernel of multiplication by p on W/W'. We view L as a sub $\mathbb{F}_p$-vector space of $W'_{\mathbb{F}_p}$ via $L = (W\cap p^{-1}W')/W' = (pW\cap W')/pW'$, where the second equality comes from multiplication by p.

An element of $T(\mathbb{Z}_p)$ that stabilizes W, also stabilizes L. Hence $T(\mathbb{Z}_p)\cdot W$ has at least as many elements as $T(\mathbb{F}_p)\cdot L$, where we let $T(\mathbb{F}_p)$ act on the set of subspaces of $W'_{\mathbb{F}_p}$. By construction, L is non-zero, and has intersection zero with $W'_{\overline{\mathbb{F}}_p,x}$ for each x in X, where $W'_{\overline{\mathbb{F}}_p} = \oplus_x W'_{\overline{\mathbb{F}}_p,x}$ is the X-grading corresponding to the $T_{\mathbb{F}_p}$-action on $W'_{\mathbb{F}_p}$. This implies that L, viewed as an $\mathbb{F}_p$-valued point in some Grassmannian, is not fixed by the action of $T_{\mathbb{F}_p}$.

Let $T'_{\mathbb{F}_p}$ be the stabilizer of L in $T_{\mathbb{F}_p}$. Lemma 4.4.1 below says that the order of the group of connected components of $T'_{\overline{\mathbb{F}}_p}$ is bounded independently of p and W. Put $T''_{\mathbb{F}_p} := T_{\mathbb{F}_p}/T'_{\mathbb{F}_p}$. Then $T''_{\mathbb{F}_p}$ is a non-trivial torus over $\mathbb{F}_p$, and by Lemma 4.4.2, the morphism $T(\mathbb{F}_p)\to T''_{\mathbb{F}_p}(\mathbb{F}_p)$ has its cokernel of order bounded independently of p and W. The proof of Proposition 4.3.9 is now finished by noting that $T''_{\mathbb{F}_p}(\mathbb{F}_p)$ has at least $p-1$ elements (see [15, Lemma 3.5]).

Lemma 4.4.1 *Let k be an algebraically closed field, and T a k-torus. Let V be a finite dimensional k-vector space with an action by T. Then the set of stabilizers T_W, for W running through the set of subspaces of V, is finite. The set of groups of connected components of these stabilizers, up to isomorphism, is finite, and bounded in terms of the dimension of V and the set of characters of T that do occur in V.*

Proof. Let us consider the set S of subspaces W of a fixed dimension, call it d. Then we have a natural injection from S into $\mathbb{P}(\Lambda^d(V))$, compatible with the $T(k)$-action. The image of a W under this map is the line generated by $w_1 \wedge \cdots \wedge w_d$, where w is any k-basis of W. Hence the set of stabilizers of the elements of S is contained in the set of stabilizers of elements of $\mathbb{P}(\Lambda^d(V))$. This reduces the proof of the lemma to the case of one-dimensional subspaces (we replace V by $\Lambda^d(V)$).

Let X be the character group of T, and let $V = \oplus_x V_x$ be the X-grading of V given by the T-action. Of course, almost all V_x are zero. For v in V, we have $v = \sum_x v_x$, and we let $\mathrm{Supp}(v)$ be the set of x with $v_x \neq 0$. For v non-zero, the stabilizer in T of the element kv in $\mathbb{P}(V)$ is the intersection of the kernels of the $x - x'$ with x and x' in $\mathrm{Supp}(v)$. Since the set of such differences is finite, the claim follows. $\square$

Lemma 4.4.2 *Let T' be the kernel of a surjective morphism $T \to T''$ of tori over k, with k a finite field. Let Φ be the group of connected components of $T'_{\overline{k}}$. Then we have the exact sequence:*

$$0 \longrightarrow T'(k) \longrightarrow T(k) \longrightarrow T''(k) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), \Phi),$$

and the upper bound:

$$|\mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), \Phi)| \leq |\Phi|.$$

Proof. One has, of course, the long exact sequence coming from Galois cohomology:

$$0 \longrightarrow T'(k) \longrightarrow T(k) \longrightarrow T''(k) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), T'(\overline{k})).$$

We combine this with the sequence:

$$\mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), (T')^0(\overline{k})) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), T'(\overline{k})) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), \Phi)$$

coming from the short exact sequence:

$$0 \longrightarrow (T')^0 \longrightarrow T' \longrightarrow T'/(T')^0 \longrightarrow 0.$$

Lang's Theorem ([17, Thm. 6.1]) implies that $\mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), (T')^0(\overline{k})) = 0$. The upper bound for $|\mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), \Phi)|$ follows from the fact that this cohomology group is just the group of coinvariants for the action of $\mathrm{Gal}(\overline{k}/k)$ on Φ. $\square$

5 Images under Hecke correspondences.

In this section we prove that the images under irreducible components of certain Hecke correspondences of an irreducible Hodge generic subvariety of a Shimura variety defined by a semi-simple algebraic group of adjoint type are irreducible.

Theorem 5.1 *Consider a Shimura variety defined by a Shimura datum (G, X) where G is a semi-simple algebraic group of adjoint type. Let K be a neat compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$ that is the product of compact open subgroups K_p of $G(\mathbb{Q}_p)$. Let X^+ be a connected component of X and let S be the image of $X^+ \times \{1\}$ in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$. Let Z be an irreducible Hodge generic subvariety of S containing a non-singular special point. Then there exists a nonzero integer n such that if q is an element of $G(\mathbb{Q})^+ := G(\mathbb{Q}) \cap G(\mathbb{R})^+$ whose image in $G(\mathbb{Q}_l)$ is in K_l for every l dividing n, then $T_q(Z)$ is irreducible, with T_q the correspondence on S given by the action of q on X^+.*

Proof. By [6, 2.1.2] we have $S = \Gamma \backslash X^+$ with $\Gamma = G(\mathbb{Q})^+ \cap K$. For q in $G(\mathbb{Q})^+$ the correspondence T_q is defined as follows. Consider the diagram:

$$S \xleftarrow{\pi} X^+ \xrightarrow{q\cdot} X^+ \xrightarrow{\pi} S,$$

with π the quotient map for the action of Γ. The morphism $\pi \circ q\cdot$ is the quotient for the action of $q^{-1}\Gamma q$, hence π and $\pi \circ q\cdot$ both factor through the quotient $S_q = \Gamma_q \backslash X^+$ with $\Gamma_q = \Gamma \cap q^{-1}\Gamma q$. With these notations, T_q is the correspondence:

$$S \xleftarrow{\pi_{q,1}} S_q \xrightarrow{\pi_{q,2}} S.$$

In particular, $T_q Z = \pi_{q,2}(\pi_{q,1}^{-1} Z)$. In order to show that $T_q Z$ is irreducible, it suffices to show that $Z_q := \pi_{q,1}^{-1} Z$ is. Since $\pi_{q,1}$ is a covering, restriction to the smooth loci in Z and Z_q gives a covering $\pi_{q,1} \colon Z_q^{\mathrm{sm}} \to Z^{\mathrm{sm}}$. Since Z_q^{sm} is Zariski-dense in Z_q, it is enough to prove that Z_q^{sm} is irreducible.

In order to find an integer n as in the Theorem, we choose a faithful representation ξ of G on a $\mathbb{Q}$-vector space V. Then ξ gives a polarizable variation of Hodge structures on the constant sheaf V_X ([12, 1.8]). Since K is neat, Γ acts freely on X^+, hence V_{X^+} descends to S. Let $V_{\hat{\mathbb{Z}}}$ be a K-invariant $\hat{\mathbb{Z}}$-lattice in $V_{\mathbb{A}_{\mathrm{f}}}$, and let $V_{\mathbb{Z}} = V_{\hat{\mathbb{Z}}} \cap V$. Then $V_{\mathbb{Z}}$ is a Γ-invariant lattice in V. This gives us a polarizable variation $\mathcal{V}_{\mathbb{Z}}(\xi)$ of $\mathbb{Z}$-Hodge structure on S, hence on Z^{sm}. Let s be a Hodge generic point in Z^{sm} and x a point of X^+ lying above it. This gives an isomorphism between the fiber $\mathcal{V}_{\mathbb{Z}}(\xi)_s$ of $\mathcal{V}_{\mathbb{Z}}(\xi)$ at s and $V_{\mathbb{Z}}$, such that the Mumford-Tate group of $\mathcal{V}_{\mathbb{Z}}(\xi)_s$ corresponds to $\xi(G)$.

On the other hand, the fundamental group $\pi_1(Z^{\mathrm{sm}}, s)$ acts on $\mathcal{V}_{\mathbb{Z}}(\xi)_s$ and hence on $V_{\mathbb{Z}}$; let Π be its image in $\mathrm{GL}(V_{\mathbb{Z}})$. Then Π is a finitely generated subgroup of $\mathrm{GL}(V_{\mathbb{Z}})$. By a theorem of André (see [13, Theorem 1.4]), the connected component of the Zariski closure of Π in the algebraic group $\mathrm{GL}(V)$ is $\xi(G)$. Since Γ is an arithmetic subgroup of $G(\mathbb{Q})$, it is Zariski dense in G, and the Zariski closure of $\xi(\Gamma)$ is $\xi(G)$.

Since $\mathcal{V}_{\mathbb{Z}}(\xi)$ exists over S, the image Π of $\pi_1(Z^{\mathrm{sm}}, s)$ is contained in that of $\pi_1(S, s)$, i.e., in $\xi(\Gamma)$. The inclusion $\Pi \subset \xi(\Gamma) \stackrel{\xi^{-1}}{\hookrightarrow} \Gamma$ makes Γ into a $\pi_1(Z^{\mathrm{sm}}, s)$-set. For q in $G(\mathbb{Q})^+$, the $\pi_1(Z^{\mathrm{sm}}, s)$-set that corresponds to the covering $\pi_{q,1}\colon Z_q^{\mathrm{sm}} \to Z^{\mathrm{sm}}$ is isomorphic to $\Gamma/q^{-1}\Gamma q \cap \Gamma$, hence Z^{sm} is connected (and hence irreducible) if and only if $\Gamma/q^{-1}\Gamma q \cap \Gamma$ is transitive. Now since $\pi_1(Z^{\mathrm{sm}}, s)$ and Γ have the same Zariski closure in the $\mathbb{Z}$-group scheme $\mathrm{GL}(V_{\mathbb{Z}})$, Nori's Theorem 5.2 below gives a non-zero integer n, such that for all non-zero integers m prime to n, $\pi_1(Z^{\mathrm{sm}}, s)$ and Γ have the same image in $\mathrm{GL}(V_{\mathbb{Z}/m\mathbb{Z}})$. (Indeed, $G(\mathbb{C})$ is a semi-simple complex Lie group, hence $\pi_1(G(\mathbb{C})$ is finite by [18, thm. 2(c)].) Let now q be in $G(\mathbb{Q})^+$, such that q_l is in K_l for all l dividing n. Then all we have to show is that there is a non-zero integer $m = \prod_l l^{m_l}$, prime to n, such that $\Gamma \cap q^{-1}\Gamma q$ contains the kernel of the natural map $\Gamma \to \mathrm{GL}(V_{\mathbb{Z}/m\mathbb{Z}})$. We have:

$$q^{-1}\Gamma q \cap \Gamma = q^{-1}Kq \cap K \cap G(\mathbb{Q})^+ = \left(\prod_l q^{-1}K_l q \cap K_l\right) \cap G(\mathbb{Q})^+.$$

For l with $q_l \in K_l$ (in particular, for l dividing n), we have $q^{-1}K_l q \cap K_l = K_l$, and we put $m_l = 0$. For the remaining finitely many l, we take m_l sufficiently large such that:

$$\ker\left(K_l \longrightarrow \mathrm{GL}(V_{\mathbb{Z}/l^{m_l}\mathbb{Z}})\right) \subset q^{-1}K_l q.$$

Then we have the last inclusion for all l, so by taking the product over all l we have:

$$\ker\left(K \longrightarrow \mathrm{GL}(V_{\mathbb{Z}/m\mathbb{Z}})\right) \subset q^{-1}Kq, \quad \text{hence} \quad \ker\left(\Gamma \longrightarrow \mathrm{GL}(V_{\mathbb{Z}/m\mathbb{Z}})\right) \subset q^{-1}\Gamma q.$$

□

Theorem 5.2 (Nori (Thm. 5.3 of [15])) *Let H be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Z})$. Let $\overline{H}$ be its Zariski closure in $\mathrm{GL}_{n,\mathbb{Z}}$. Suppose that $\overline{H}(\mathbb{C})$ has a finite fundamental group, then the closure of H in $\mathrm{GL}_n(\hat{\mathbb{Z}})$ is open in the closure of $\overline{H}(\mathbb{Z})$ in $\mathrm{GL}_n(\hat{\mathbb{Z}})$.*

Remark 5.3 A careful reader might be worried by our use of Theorem 5.3 of Nori's article [15], because Theorem 5.2 of the same article is clearly wrong. Probably, the problem with Theorem 5.2 is only typographical: should $[A, A](\hat{R})$ be replaced by $[A, A](R)^\wedge$, the closure of $[A, A](R)$ in $\mathrm{GL}_n(\hat{R})$? Or by $[A(R), A(R)]^\wedge$? Anyway, Theorem 5.3 can be deduced from Theorem 5.4, which in turn can be found in other references ([17, Thm. 7.14], [16]).

6 Density of Hecke orbits.

We will now prove the following result about the density of Hecke orbits in Shimura varieties.

Theorem 6.1 *Let (G, X) be a Shimura datum with $G = G_1 \times \cdots \times G_r$ a semi-simple algebraic group of adjoint type with simple factors $G_1, \ldots, G_r$. Let K be a compact open subgroup of $G(\mathbb{A}_f)$ that is the product of compact open subgroups K_p of $G(\mathbb{Q}_p)$. Let X^+ be a connected component of X, let S be the image of $X^+ \times \{1\}$ in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$, and put $\Gamma = G(\mathbb{Q})^+ \cap K$. Then there exists an integer n such that for all prime numbers $p \geq n$ the following holds.*

Let q be an element of $G(\mathbb{Q}_p)$ such that for all j the projection of q in $G_j(\mathbb{Q}_p)$ is not contained in a compact subgroup. The connected components of the correspondence that T_q induces on S are the T_{q_i}, induced by q_i in $G(\mathbb{Q})^+$ acting on X^+, such that:

$$G(\mathbb{Q})^+ \cap KqK = \coprod_i \Gamma q_i^{-1} \Gamma.$$

Then, for all i and for all s in S, the $T_{q_i} + T_{q_i^{-1}}$-orbit $\cup_{n \geq 0} (T_{q_i} + T_{q_i^{-1}})^n s$ is dense in S for the Archimedean topology.

Proof. Let $p_j \colon G \to G_j$ denote the jth projection. For each j, let n_j be as in Proposition 6.2 applied to G_j and $p_j(K)$, and let n be the maximum of the n_j. Let $p \geq n$ be prime, and let q in $G(\mathbb{Q}_p)$ and the q_i in $G(\mathbb{Q})$ be as in the Theorem. For each i, let Γ_i denote the subgroup of $G(\mathbb{Q})^+$ generated by Γ and q_i. Then we have $S = \Gamma \backslash X^+$, and for s in S, the $T_{q_i} + T_{q_i^{-1}}$-orbit of s is the image in S of a Γ_i-orbit in X^+. Hence it suffices to prove that each Γ_i is dense in $G(\mathbb{R})^+$.

Let H be the closure in $G(\mathbb{R})^+$ of say Γ_1. Then H is a Lie subgroup of $G(\mathbb{R})$. We let H^+ be the connected component of the identity. Now Γ normalizes H^+, hence its Lie algebra. Since Γ is Zariski dense in $G_{\mathbb{R}}$ ([17, Thm. 4.10], note that no $G_i(\mathbb{R})$ is compact), this implies that H^+ is a product of simple factors of $G(\mathbb{R})^+$. We claim that if H^+ contains a simple factor of $G_i(\mathbb{R})^+$, then it contains all of $G_i(\mathbb{R})^+$. This follows from two facts. One: $H^+ \cap G(\mathbb{Q})$ is dense in H^+. Two: for every i, and for every factor $G_{i,j}$ of $G_{i,\overline{\mathbb{Q}}}$ the map $G_i(\mathbb{Q}) \to G_{i,j}(\overline{\mathbb{Q}})$ is injective. The second fact is a direct consequence of the statement ([2, 6.21(ii)]) that $G_i = \mathrm{Res}_{F/\mathbb{Q}} G'_i$ for some finite extension F of $\mathbb{Q}$ and some absolutely simple group G'_i over F.

Let now I be the subset of $\{1, \ldots, r\}$ of the i such that H^+ does not contain $G_i(\mathbb{R})^+$, let G_I be the product of the G_i with i in I, and let $f \colon G(\mathbb{R})^+ \to G_I(\mathbb{R})^+$ be the projection. Then H^+ is the kernel of f, hence $f(H)$ is discrete in $G_I(\mathbb{R})$. But then $f(\Gamma_1)$, being a subgroup of $f(H)$, is discrete. Now suppose that I is not empty. By Proposition 6.2, $f(\Gamma)$ has infinite index in $f(\Gamma_1)$, which contradicts the fact that $f(\Gamma) \backslash G_I(\mathbb{R})^+$ has finite volume (see [17, Thm. 4.13]). Hence I is empty, and $H = G(\mathbb{R})^+$. □

Proposition 6.2 *Let G be a simple (hence adjoint) algebraic group over $\mathbb{Q}$ with $G(\mathbb{R})$ not compact. Let K be a compact open subgroup of $G(\mathbb{A}_f)$ and put $\Gamma = G(\mathbb{Q})^+ \cap K$. Then there is an integer n such that for all prime numbers $p \geq n$ the following holds.*

Let g be an element of $G(\mathbb{Q}_p)$ that is not contained in a compact subgroup. Let q be an element of $G(\mathbb{Q}) \cap KgK$. Then $\Gamma q \Gamma$ contains an element q' such that Γ has infinite index in the group generated by Γ and q'.

Proof. Let V be a finite dimensional absolutely irreducible faithful representation of G_E, where E is a suitable finite extension of $\mathbb{Q}$. As Γ is Zariski dense in $G_{\overline{\mathbb{Q}}}$ ([17, Thm. 4.10]), V is an absolutely irreducible representation of Γ. By the double centralizer theorem ([10, XVII, Cor. 3.5]), $\mathrm{End}_E(V)$ is spanned (over E) by the images of the γ in Γ. Let O_E be the ring of integers of E, and let V_{O_E} be a Γ-invariant O_E-lattice in V. Let $\gamma_1, \ldots, \gamma_m$ be in Γ whose images $\overline{\gamma_1}, \ldots, \overline{\gamma_m}$ span $\mathrm{End}_E(V)$. Let n be the index of $O_E\overline{\gamma_1} + \cdots + O_E\overline{\gamma_m}$ in $\mathrm{End}_{O_E}(V_{O_E})$. For p prime put $O_{E,p} = \mathbb{Z}_p \otimes O_E$, and $E_p = \mathbb{Q}_p \otimes E$. For $p > n$ we have $O_{E,p}\overline{\gamma_1} + \cdots + O_{E,p}\overline{\gamma_m} = \mathrm{End}_{O_{E,p}}(V_{O_{E,p}})$.

Let now $p > n$ be prime, and let g be an element of $G(\mathbb{Q}_p)$ that is not contained in a compact group. Then not all eigenvalues of g acting on $\overline{\mathbb{Q}}_p \otimes_{\mathbb{Q}} V$ (as $\overline{\mathbb{Q}}_p$-vector space) have absolute value 1. Replacing g, q and q' by their inverses if necessary, we may suppose that at least one of the eigenvalues of g has absolute value > 1. Then the matrix of g with respect to an $O_{E,p}$-basis of $V_{O_{E,p}}$ has at least one coefficient that is not in $O_{E,p}$.

Let q be an element of KgK. Then we have, in $G(\mathbb{Q}_p)$, $q = k_1 g k_2$, with k_1 and k_2 in the image K_p of K. So in $\mathrm{GL}_{E_p}(V_{E_p})$ we have $\overline{q} = \overline{k_1}\,\overline{g}\,\overline{k_2}$ with $\overline{k_1}$ and $\overline{k_2}$ in $\mathrm{GL}_{O_{E,p}}(V_{O_{E,p}})$. But then we have $\overline{g} = \overline{k_1}^{-1}\overline{q}\,\overline{k_2}^{-1}$. It follows that all $u\overline{g}v$ with u and v in $\mathrm{End}_{O_{E,p}}(V_{O_{E,p}})$ are O_{E_p}-linear combinations of elements of the form $\overline{\gamma q \gamma'}$ with γ and γ' in Γ. Hence there are such γ and γ' such that the trace of $q' = \gamma q \gamma'$ is not in $O_{E,p}$. But then q' has an eigenvalue (in $\overline{\mathbb{Q}}_p$) of absolute value > 1, hence q' is not contained in a compact subgroup of $G(\mathbb{Q}_p)$. If q is in $G(\mathbb{Q}) \cap KgK$, then we get a q' in $\Gamma q \Gamma$ of which no non-trivial power lies in Γ. $\square$

One would like to have a generalization of Proposition 6.2 that requires only a weaker hypothesis on q and that gives a better understanding of the primes p that are to be excluded. The following Proposition, that will not be used in the rest of this article, gives such a result in the simply connected case. It would be useful to have a version of it in the adjoint case (maybe the results in [11] can be used here).

Proposition 6.3 *Let G be a semi-simple algebraic group over $\mathbb{Q}$ whose adjoint is simple. Suppose that $G(\mathbb{R})$ is not compact. Let K be a compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$. For p prime let K_p be the image of K_p under projection to $G(\mathbb{Q}_p)$. Let p be a prime for which K_p is a maximal compact subgroup of $G(\mathbb{Q}_p)$ and let q be an element of $G(\mathbb{Q})$ such that the image of q in $G(\mathbb{Q}_p)$ is not in K_p. Then $\Gamma = G(\mathbb{Q}) \cap K$ is of infinite index in the group Γ_q generated by Γ and q.*

Proof. By strong approximation ([17, Thm. 7.12]), $G(\mathbb{Q})$ is dense in $G(\mathbb{A}_{\mathrm{f}})$. Hence Γ is dense in K. Suppose that Γ_q/Γ is finite. Let $\overline{\Gamma}$ and $\overline{\Gamma_q}$ be the closures of Γ and Γ_q in $G(\mathbb{Q}_p)$. We have

$\overline{\Gamma} = K_p$. Since Γ_q is a finite union of Γ-cosets, $\overline{\Gamma_q}$ is a finite union of $\overline{\Gamma}$-cosets. Hence $\overline{\Gamma_q}$ is compact. As q is not in K_p, and K_p is a maximal compact open subgroup of $G(\mathbb{Q}_p)$, we have a contradiction. □

7 Proof of the main result.

The aim of this section is to prove Theorem 1.2. So let (G, X) be a Shimura datum, let K be a compact open subgroup of $G(\mathbb{A}_f)$, let V be a faithful finite dimensional representation of G and let Z be a closed irreducible curve in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ that contains an infinite set Σ of special points x such that all $[V_x]$ with x in Σ are equal.

As we have seen in Section 2, it suffices to prove the result in the case where G is semi-simple and adjoint, K is neat and Z Hodge generic. So we suppose that. We write $G = G_1 \times \cdots \times G_r$ with the G_i simple. We will also suppose that K is the product of compact open subgroups K_p of the $G(\mathbb{Q}_p)$. We let S be the connected component of $\mathrm{Sh}_K(G, X)$ that contains Z. We assume that we have a $\mathbb{Z}$-structure on V given by the choice of a K-invariant $\hat{\mathbb{Z}}$-lattice in $V_{\mathbb{A}_f}$. Then V induces a variation of $\mathbb{Z}$-Hodge structure on S. For each s in S we have its Mumford-Tate group $\mathrm{MT}(V_s)$ which is a closed sub group scheme of the $\mathbb{Z}$-group scheme $\mathbf{GL}(V_s)$.

Let X^+ be a connected component of X. After replacing Z by an irreducible component of its image under a suitable Hecke correspondence, we may suppose that S is the image of $X^+ \times \{1\}$ in $\mathrm{Sh}_K(G, X)$.

Theorem 7.1 *Assume that p is a prime and m an element of $G(\mathbb{Q}_p)$, such that:*

1. *p does not divide the integer n of Theorem 5.1, applied to the subvariety Z of $\mathrm{Sh}_K(G, X)$;*
2. *$p \geq n$ with n as in Theorem 6.1 applied to (G, X), K and X^+, and for every $\mathbb{Q}$-simple factor G_i of G, the image of m in $G_i(\mathbb{Q}_p)$ is not contained in a compact subgroup;*
3. *$Z \subset T_m Z$, with T_m the correspondence induced by m on $\mathrm{Sh}_K(G, X)$.*

Then $Z = S$, hence Z is of Hodge type.

Proof. Assume that p and m satisfy the three conditions. We have $S = \Gamma\backslash X^+$, with Γ the intersection of K and $G(\mathbb{Q})^+$. The connected components of the correspondence that T_m induces on S are the T_{m_i}, induced by m_i in $G(\mathbb{Q})^+$ acting on X^+, such that:

$$G(\mathbb{Q})^+ \cap KmK = \coprod_i \Gamma m_i^{-1} \Gamma.$$

Let q be one of the m_i such that $Z \subset T_q Z$. Since q^{-1} is in KmK, and m in $G(\mathbb{Q}_p)$, the image of q in $G(\mathbb{Q}_l)$ is in K_l for all $l \neq p$, in particular, for all l not dividing n. By Theorem 5.1, $T_q Z$ and $T_{q^{-1}} Z$ are irreducible, and hence equal to Z. By Theorem 6.1, all $T_q + T_{q^{-1}}$-orbits in S are dense, hence $Z = S$. □

For each s in Σ we choose an element $\tilde{s}$ of X^+ such that $s = \overline{(\tilde{s}, 1)}$. Then we have for each s in Σ the Mumford-Tate group $\mathrm{MT}(V_s) = \mathrm{MT}(\tilde{s})$ as a closed sub group scheme of $\mathbf{GL}(V)$. We give G a $\mathbb{Z}$-structure $G_{\mathbb{Z}}$ by taking its Zariski closure in $\mathbf{GL}(V)$.

Since all $V_{s,\mathbb{Q}}$ for s in Σ are isomorphic, all $\mathrm{MT}(\tilde{s})_{\mathbb{Q}}$ are isomorphic. Let $F \subset \mathbb{C}$ be a finite extension of $\mathbb{Q}$ that splits all these tori. Then F contains the reflex field of (G, X). By taking F large enough, we may and do assume that Z is defined over F (as an absolutely irreducible closed F-subscheme Z_F of $\mathrm{Sh}_K(G, X)_F$).

In the rest of the proof of Theorem 1.2 we will distinguish two cases, depending on the behavior of the $\mathrm{MT}(V_s)$ for s in Σ.

Definition 7.2 For s in Σ, let $i(s)$ be the number of prime numbers p such that $\mathrm{MT}(V_s)_{\mathbb{F}_p}$ is not a torus.

This function $i\colon \Sigma \to \mathbb{Z}$ depends on the choice of the $\mathbb{Z}$-structure on V, but an other choice would give a function that differs from i by a bounded function. Also, replacing Z by an irreducible component of the image of Z under a Hecke correspondence only changes the function i by a bounded function. The two cases that we will distinguish depend on whether or not i is bounded.

7.3 The case where i is bounded.

In this section we assume that the function $i : \Sigma \to \mathbb{Z}$ defined above is bounded. It follows that for all but finitely many prime numbers p, the subset Σ_p of s in Σ with $\mathrm{MT}(V_s)_{\mathbb{F}_p}$ a torus is Zariski dense in Z.

Proposition 7.3.1 *Let p be a prime such that $G_{\mathbb{F}_p}$ is smooth over $\mathbb{F}_p$. Then the set of subtori $\mathrm{MT}(\tilde{s})_{\mathbb{Z}_p}$ of $G_{\mathbb{Z}_p}$ for s in Σ_p meets only a finite number of $G_{\mathbb{Z}}(\mathbb{Z}_p)$-conjugacy classes of subtori of $G_{\mathbb{Z}_p}$.*

Proof. Let p be prime. Let s_1 and s_2 be in Σ_p. Let h in $\mathrm{GL}(V_{\mathbb{Q}})$ be an isomorphism from $(V_{\mathbb{Q}}, \tilde{s}_1)$ to $(V_{\mathbb{Q}}, \tilde{s}_2)$. Then h induces an isomorphism of $\mathbb{Z}$-Hodge structures from $(h^{-1}V, \tilde{s}_1)$ to $(V, \tilde{s}_2)$. Hence $h^{-1}V_{\mathbb{Z}_p}$ is a $\mathbb{Z}_p$-lattice in $V_{\mathbb{Q}_p}$ such that the Zariski closure of $\mathrm{MT}(\tilde{s}_1)_{\mathbb{Q}_p}$ in $\mathbf{GL}(h^{-1}V_{\mathbb{Z}_p})$ is a torus. Lemma 3.3.1 (applied to $T = \mathrm{MT}(V, \tilde{s}_1)_{\mathbb{Z}_p}$ and the free $\mathbb{Z}_p$-module $h^{-1}V_{\mathbb{Z}_p}$) gives an element c in $\mathrm{GL}(V_{\mathbb{Q}_p})$ centralizing $\mathrm{MT}(V, \tilde{s}_1)_{\mathbb{Q}_p}$ such that $h^{-1}V_{\mathbb{Z}_p} = cV_{\mathbb{Z}_p}$. Hence there exists

k in $\mathrm{GL}(V_{\mathbb{Z}_p})$ such that $h^{-1} = ck$. We have $\mathrm{MT}(\tilde{s}_2)_{\mathbb{Z}_p} = k\mathrm{MT}(\tilde{s}_1)_{\mathbb{Z}_p}k^{-1}$. So we have that all $\mathrm{MT}(\tilde{s})_{\mathbb{Z}_p}$ for s in Σ_p lie in one $\mathrm{GL}(V_{\mathbb{Z}_p})$-orbit.

The set of $\mathrm{MT}(\tilde{s})_{\mathbb{F}_p}$ for s in Σ_p is contained in one $\mathrm{GL}(V_{\mathbb{F}_p})$-orbit, and hence is a finite set. If s_1 and s_2 in Σ_p are such that $\mathrm{MT}(\tilde{s}_1)_{\mathbb{F}_p} = \mathrm{MT}(\tilde{s}_2)_{\mathbb{F}_p}$, then $\mathrm{MT}(\tilde{s}_1)_{\mathbb{Z}_p}$ and $\mathrm{MT}(\tilde{s}_2)_{\mathbb{Z}_p}$ are conjugated by an element of $G(\mathbb{Z}_p)$ by [7, Exp. XI, Cor. 5.2], which says that the "transporteur" in $G(\mathbb{Z}_p)$ between $\mathrm{MT}(\tilde{s}_1)_{\mathbb{Z}_p}$ and $\mathrm{MT}(\tilde{s}_2)_{\mathbb{Z}_p}$ is smooth over $\mathbb{Z}_p$. □

Let p be a prime with the following properties:

1. p satisfies the conditions of Theorem 7.1;
2. Σ_p is Zariski dense in Z;
3. $G_{\mathbb{F}_p}$ is smooth over $\mathbb{F}_p$;
4. $K_p = G_{\mathbb{Z}}(\mathbb{Z}_p)$;
5. all the $\mathrm{MT}(\tilde{s})_{\mathbb{Q}_p}$ for s in Σ are split.

Indeed, the first four conditions only exclude finitely many primes, and the last condition is verified by a set of primes of positive density (Chebotarev). We replace Σ by a suitable Zariski dense subset of Σ_p such that the $\mathrm{MT}(\tilde{s})_{\mathbb{Z}_p}$ lie in one $G_{\mathbb{Z}}(\mathbb{Z}_p)$-conjugacy class.

Let s_0 be an element of Σ, and let $M = \mathrm{MT}(\tilde{s}_0)$. The reciprocity morphism r from $\mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_{\mathrm{m}F}$ to $M_{\mathbb{Q}}$ is surjective, hence $r((\mathbb{Q}_p \otimes F)^*)$ is of finite index, say e, in $M(\mathbb{Q}_p)$. For each i, the image M_i of M in G_i is non-trivial by the axioms for what constitutes a Shimura datum (condition (2.1.1.3) in [6, 2.1]). By hypothesis, $M_{\mathbb{Q}_p}$ and hence the $M_{i,\mathbb{Q}_p}$ are split tori. For a split torus T over $\mathbb{Q}_p$, $T(\mathbb{Q}_p)$ modulo its maximal compact subgroup is a free $\mathbb{Z}$-module of rank the dimension of T. Since $M(\mathbb{Q}_p)$ modulo its maximal compact subgroup is not equal to a finite union of proper sub $\mathbb{Z}$-modules, we can take an element m of $M(\mathbb{Q}_p)$ that satisfies the following conditions:

1. m is in the image of multiplication by e on $M(\mathbb{Q}_p)$;
2. for every simple factor G_i of G, the image of m in $G_i(\mathbb{Q}_p)$ is not contained in a compact subgroup.

We will show that $Z \subset T_m Z$, so that Z is of Hodge type by Theorem 7.1. Let s be in Σ. We have:

$$T_m s = \{\overline{(\tilde{s}, k_1 m k_2)} \mid k_1 \in K_p,\ k_2 \in K_p\}.$$

By hypothesis, there exists an h in $G_{\mathbb{Z}}(\mathbb{Z}_p)$ such that $\mathrm{MT}(\tilde{s})_{\mathbb{Z}_p} = hM_{\mathbb{Z}_p}h^{-1}$. It follows that hmh^{-1} is in $\mathrm{MT}(\tilde{s})(\mathbb{Q}_p)$, and even in the image of the reciprocity morphism for $\tilde{s}$, so that:

$$\overline{(\tilde{s}, hmh^{-1})} \text{ is in } \mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s.$$

We conclude that $\overline{(\tilde{s}, hmh^{-1})}$ is in the intersection of $T_m s$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s$. As $T_m s$ is contained in $T_m Z$, and $\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s$ is contained in Z, $\overline{(\tilde{s}, hmh^{-1})}$ is in $Z \cap T_m Z$. As both Z and $T_m Z$ are defined over F, we have:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s \subset Z \cap T_m Z.$$

It follows that Z is contained in $T_m Z$. This ends the proof of Theorem 1.2 in the case where i is bounded.

Remark 7.3.2 The proof of Theorem 1.2 that we have just given, in the case where the function i is bounded, does not use that Z is a curve. Hence it proves Theorem 1.2 without the condition that Z is a curve, but with the extra condition that i is bounded.

This kind of result can be useful. For example Vatsal and Cornut (see [19] and [5]) consider sets of Heegner points on products of modular curves where the discriminants of the endomorphism rings of the elliptic curves in question are products of a fixed finite set of prime numbers (of course, the André-Oort conjecture in this case was already proved by Moonen in [14, §5], since it concerns a Shimura datum related to moduli of abelian varieties).

7.4 The case where i is not bounded.

In this section we assume that $i(s)$ is not bounded when s ranges through the points of Σ. The strategy for proving Theorem 1.2 in this case is as follows. For s in Σ with $i(s)$ big enough, we show that there exists a prime number p and an element m in $G(\mathbb{Q}_p)$ that satisfy the first two conditions in Theorem 7.1, such that $Z \cap T_m Z$ contains $\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s$ and such that $|\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s|$ exceeds the "intersection number" of Z and $T_m Z$. Then it follows that Z and $T_m Z$ do not intersect properly, and hence that Z is contained in $T_m Z$ (it is here that we use that Z is a curve). Theorem 7.1 then says that Z is of Hodge type.

We cite the following result (see [8, Thm. 7.2]) that bounds the intersection of Z and its images under Hecke correspondences, if finite.

Theorem 7.4.1 *Let (G, X) be a Shimura datum, let K_1 and K_2 be compact open subgroups of $G(\mathbb{A}_{\mathrm{f}})$, and let Z_1 and Z_2 be closed subvarieties of the Shimura varieties $S_1 := \mathrm{Sh}_{K_1}(G, X)_{\mathbb{C}}$ and $S_2 := \mathrm{Sh}_{K_2}(G, X)_{\mathbb{C}}$, respectively. Suppose that Z_1 or Z_2 is of dimension at most one. Then there exists an integer c such that for all g in $G(\mathbb{A}_{\mathrm{f}})$ for which $T_g Z_1 \cap Z_2$ is finite, one has:*

$$|T_g Z_1 \cap Z_2| \leq c \deg(\pi_1 \colon S_g \to S_1),$$

where $S_g = \mathrm{Sh}_{K_g}(G,X)_{\mathbb{C}}$ with $K_g = K_1 \cap gK_2g^{-1}$, and with T_g and π_1 the morphism that is induced by the inclusion of K_g in K_1.

Applied in our situation, this theorem gives the following result.

Corollary 7.4.2 *There exists an integer c such that for all m in $G(\mathbb{A}_{\mathrm{f}})$ with $Z \cap T_m Z$ finite one has:*

$$|Z \cap T_m Z| < c\, |K/K \cap mKm^{-1}|.$$

We note that if p is a prime such that $K_p = G(\mathbb{Z}_p)$, and if m is in $G(\mathbb{Q}_p)$, then $K/K \cap mKm^{-1}$ is the K_p-orbit of the lattice $mV_{\mathbb{Z}_p}$ in the set of $\mathbb{Z}_p$-lattices in $V_{\mathbb{Q}_p}$, and hence $|K/K \cap mKm^{-1}|$ is at most $|\mathrm{GL}(V_{\mathbb{Z}_p}){\cdot}mV_{\mathbb{Z}_p}|$. In order to get prime numbers p and elements m in $G(\mathbb{Q}_p)$ that verify the first two conditions in Theorem 7.1 and are such that $|K/K \cap mKm^{-1}|$ is not too big, we prove the following.

Proposition 7.4.3 *Let n, r, e and B be nonnegative integers. There exists an integer k with the following property. Let p be a prime number and let M be a split subtorus of $\mathrm{GL}_{n,\mathbb{Q}_p}$, such that $M_{\mathbb{Z}_p}$ (obtained from Zariski closure in $\mathrm{GL}_{n,\mathbb{Z}_p}$) is a torus. Suppose that with respect to a suitable $\mathbb{Z}$-basis of the character group $X^*(M_{\mathbb{Q}_p})$ all coordinates of the differences of the characters that intervene in $\mathbb{Q}_p^n$ have absolute value at most B. Let $q_i\colon M \to M_i$ be r quotients of M, with each M_i non-trivial. Then there exists an element m in $M(\mathbb{Q}_p)$ such that no $q_i(m)$ lies in a compact subgroup of $M_i(\mathbb{Q}_p)$, and such that $|\mathrm{GL}(V_{\mathbb{Z}_p}){\cdot}m^eV_{\mathbb{Z}_p}| < p^k$.*

Proof. Let n, r, e and B be given. Let p be a prime number, let M be a split subtorus of $\mathrm{GL}_{n,\mathbb{Q}_p}$, such that $M_{\mathbb{Z}_p}$ a torus. Then we have a direct sum decomposition into character spaces:

$$\mathbb{Z}_p^n = \oplus_{\chi \in X^*(M)} L_\chi.$$

Let d be the dimension of M, and let $f\colon \mathbb{Z}^d \to X^*(M)$ be an isomorphism such that for each pair (χ_1, χ_2) with $L_{\chi_1} \neq 0 \neq L_{\chi_2}$ one has $\|f^{-1}(\chi_1 - \chi_2)\| \leq B$, where $\|\cdot\|$ denotes the maximum norm on $\mathbb{Z}^d$. We identify $X^*(M)$ and its dual $X_*(M)$ with $\mathbb{Z}^d$ via f and its dual. Then the kernels of the $X_*(q_i)$ give us r subgroups S_i of $\mathbb{Z}^d$ of rank less than d. For T a split torus over $\mathbb{Q}_p$ one has $T(\mathbb{Q}_p) = X_*(T) \otimes \mathbb{Q}_p^*$, and hence the valuation map $v_p\colon \mathbb{Q}_p^* \to \mathbb{Z}$ induces an isomorphism from $T(\mathbb{Q}_p)$ modulo its maximal compact subgroup to $X_*(T)$. It follows that for an element m of $M(\mathbb{Q}_p)$ no $q_i(m)$ is in a compact subgroup if and only if the image of m in $\mathbb{Z}^d$ avoids all S_i.

The quotient $\mathbb{Z}^d/(r+2)\mathbb{Z}^d$ has $(r+2)^d$ elements, whereas the union of the images of the S_i has at most $(r+2)^{d-1}r$ elements, which is less than $(r+2)^d$. Let x be an element of $\mathbb{Z}^d$ with $\|x\| < r+2$ whose image in $\mathbb{Z}^d/(r+2)\mathbb{Z}^d$ is not in the union of the images of the S_i. Let m be an element in $M(\mathbb{Q}_p)$ with image x in $\mathbb{Z}^d$. Let a and b be the smallest and largest integers such that $p^a\mathbb{Z}_p^n \subset m^e\mathbb{Z}_p^n \subset p^b\mathbb{Z}_p^n$. Then the $\mathrm{GL}_n(\mathbb{Z}_p)$-orbit of $m^e\mathbb{Z}_p^n$ is contained in the set of $\mathbb{Z}_p$-lattices between $p^a\mathbb{Z}_p^n$ and $p^b\mathbb{Z}_p^n$. The number of such lattices is the number of subgroups of $(\mathbb{Z}/p^{a-b}\mathbb{Z})^d$, hence is at most $p^{(a-b)d^2}$ (use that every subgroup is generated by d elements).

It remains to bound $a-b$. On L_χ, m^e acts, up to an element of $\mathbb{Z}_p^*$, by multiplication by $p^{\langle f^{-1}\chi, ex\rangle}$, where $\langle\cdot,\cdot\rangle$ denotes the standard pairing. Hence a and b are the maximum and minimum of the $\langle f^{-1}\chi, ex\rangle$, with $L_\chi \neq 0$. It follows that $a-b \leq edB(r+1)$. As $d \leq n$, we can take $k = en^3B(r+1)$. □

Applied to our situation, we get the following consequence (note that the $\mathrm{MT}(\tilde{s})_{\mathbb{Q}}$ with s in Σ lie in one $\mathrm{GL}(V_{\mathbb{Q}})$-conjugacy class).

Corollary 7.4.4 *There exists an integer k with the following property. Let s be in Σ, and let p be a prime such that $\mathrm{MT}(\tilde{s})_{\mathbb{Q}_p}$ is split, and $\mathrm{MT}(\tilde{s})_{\mathbb{F}_p}$ is a torus. Then there exists an element m in $\mathrm{MT}(\tilde{s})(\mathbb{Q}_p)$ such that:*

1. *m is in the image of the reciprocity morphism $r_{\tilde{s}}\colon (\mathbb{Q}_p \otimes F)^* \to \mathrm{MT}(\tilde{s})(\mathbb{Q}_p)$;*
2. *for all i, the image of m in $G_i(\mathbb{Q}_p)$ is not in a compact subgroup;*
3. *if $Z \cap T_m Z$ is finite, then $|Z \cap T_m Z| \leq p^k$.*

Theorem 4.1 provides us with positive reals numbers c_1 and c_2 such that for all s in Σ we have:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s| > c_1 c_2^{i(s)} i(s)!.$$

For x in $\mathbb{R}$, let $\pi_{F,1}(x)$ be the number of prime numbers $p \leq x$ such that F is split over $\mathbb{Q}_p$. Chebotarev's density theorem (see [9, Ch. VIII, §4]) says that for x in $\mathbb{R}$ large enough, one has:

$$\pi_{F,1}(x) \geq \frac{1}{2[F:\mathbb{Q}]}\cdot\frac{x}{\log(x)}.$$

Elementary calculus shows that for all y in $\mathbb{Z}$ large enough, there exists x in $\mathbb{R}$ such that:

$$\frac{1}{2[F:\mathbb{Q}]}\cdot\frac{x}{\log(x)} > y \quad \text{and} \quad x^k < c_1 c_2^y y!.$$

As the function $i\colon \Sigma \to \mathbb{Z}$ is not bounded, we conclude that there exists an s in Σ, a prime number p and an element m in $\mathrm{MT}(\tilde{s})(\mathbb{Q}_p)$ such that m and p satisfy the first two conditions of Theorem 7.1, and even the last one because $Z \cap T_m Z$ contains $\mathrm{Gal}(\overline{\mathbb{Q}}/F)\cdot s$.

Acknowledgements

We would like to thank Paula Cohen for pointing out to us that it would be interesting to prove Conjecture 1.1 in the case of a set of special points that is contained in one Hecke orbit. We thank Paula Cohen and Gisbert Wüstholz for making preliminary versions of their preprint [4] available to us, and for useful conversations and correspondence. We thank Jürgen Wolfart for explaining to us the problem in his article [20]. We thank Yves André and Richard Pink for the work they have done as referees of the thesis of the second author. We thank Rutger Noot for useful discussions on Shimura varieties.

References

[1] Y. André. *Quelques conjectures de transcendance issues de la géométrie algébrique.* Preprint Inst. Math. de Jussieu, 121 (1997).

[2] A. Borel and J. Tits. *Groupes réductifs.* Publ. Math. IHES 27, 1965, 55-150.

[3] S. Bosch, W. Lütkebohmert and M. Raynaud. *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, Band 21. Springer-Verlag, 1990.

[4] P.B. Cohen and G. Wüstholz. *Application of the André-Oort conjecture to some questions in transcendence.* To appear in "A Panorama in Number Theory", G. Wüstholz (editor), Cambridge University Press, 2001.

[5] C. Cornut. *A conjecture of Mazur on higher Heegner points.* Preprint. Available on the author's home page.

[6] P. Deligne. *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques.* Automorphic forms, representations and L-functions, Proc. Sympos. Pure Math., XXXIII, Part 2, 247–289, Amer. Math. Soc., Providence, R.I., 1979.

[7] M. Demazure and A. Grothendieck. *SGA 3: Schémas en groupes.* Lecture Notes in Mathematics 151–153, Springer-Verlag, 1970.

[8] S.J. Edixhoven. *On the André-Oort conjecture for Hilbert modular surfaces.* Moduli of abelian varieties, Progress in Mathematics 195 (2001), 133–155, Birkhäuser. Available on the author's home page.

[9] S. Lang. *Algebraic number theory.* Graduate Texts in Mathematics 110, Springer-Verlag, second edition, 1994.

[10] S. Lang. *Algebra.* Second edition. Addison-Wesley Publishing Company, 1984.

[11] G.A. Margulis. *Discrete subgroups of semisimple Lie groups.* Ergebnisse, 3. Folge, Bd. 17, Springer-Verlag, 1991.

[12] B. Moonen. *Models of Shimura varieties in mixed characteristics.* Pages 261–350 in “Galois representations in arithmetic algebraic geometry”, edited by A.J. Scholl and R.L. Taylor. Cambridge University Press 1998.

[13] B. Moonen. *Linearity properties of Shimura varieties I.* Journal of algebraic geometry, 7 (1998), 539–567.

[14] B. Moonen. *Linearity properties of Shimura varieties. II.* Compositio Math. 114 (1998), no. 1, 3–35.

[15] M. Nori. *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$. Invent. Math. 88, 257-275 (1987).

[16] R. Pink. *Strong approximation for Zariski dense subgroups over arbitrary global fields.* Preprint (4.11.1998), 33 p.

[17] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory.* Academic Press, 1994.

[18] J-P. Serre. *Algèbes de Lie semi-simples complexes.* W.A. Benjamin, inc. 1966.

[19] N. Vatsal. *Special values of anticyclotomic* L*-functions.* Preprint, August 2000, University of British Columbia. Available on the author’s home page.

[20] J. Wolfart. *Werte hypergeometrische Functionen.* Invent. math. 92 (1988), 187–216.

[21] G. Wüstholz. *Algebraic groups, Hodge theory, and transcendence.* Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986), 476–483, Amer. Math. Soc., Providence, RI, 1987.

[22] A. Yafaev. *Sous-variétés des variétés de Shimura.* Ph.D. thesis, University of Rennes, December 2000.