Around the André-Oort conjecture

Christopher Michael Daw

A thesis presented for the degree of

Doctor of Philosophy

(Mathematics)

Supervised by Andrei Yafaev

University College London (UCL)

2014

I confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Christopher Daw

Acknowledgements

Over the last four years, I have become hugely indebted to my supervisor, Andrei Yafaev, for his patience, his insight, his generosity and his understanding, not just in mathematics, but in all things. He has given me interesting questions from the outset and trusted me to learn in my own way. I thank him wholeheartedly for being the best mentor I could have hoped for.

I have also benefited greatly from the advice and wisdom of many other inspiring mathematicians. There are even those with whom I have never spoken, or even met, but who nonetheless have given me so much. For their particular generosity, I would like to thank Misha Gavrilovich, Minhyong Kim, Bruno Klingler, Yiannis Petridis, Jonathan Pila, Emmanuel Ullmo, Alex Wilkie and Boris Zilber.

I have been fortunate enough to meet many other students and, among them, make many friends. For all of the discussions, help and support, mathematical or otherwise, it is a pleasure to thank Ziyang Gao, Adam Harris and Martin Orr. I would also like to express my deepest gratitude to the department of mathematics at UCL. In all aspects, not least financial, it has fully supported me throughout my studies and has been a great place to learn and teach. In fact, I am indebted to so many institutions, and their members, for numerous conferences, workshops and visits. I thank them all.

Thank you to all of you who have played a part in getting me here. Thank you to my friends and my teachers, I just hope you know who you are. Thank you to Meg, the reason I'm happy every day. Thank you to my family, the best family I could ever wish for. All of the good things that happen to me are because of you.

Abstract

In this thesis we study the André-Oort conjecture, which is a statement regarding subvarieties of Shimura varieties that contain a Zariski dense set of special points. In particular, we investigate two different strategies for proving the conjecture. The first is the so-called Pila-Zannier strategy, which is a striking application of the Pila-Wilkie counting theorem from o-minimality and has led to a number of unconditional proofs in special cases. We present one such proof here, for Hilbert modular surfaces, and also explain how the Pila-Zannier strategy generalises to all Shimura varieties. We subsequently exhibit a result on torsion in the class groups of algebraic tori, obtained from an investigation into some of the relevant arithmetic.

The second strategy originated in the work of Edixhoven and ultimately led to a proof of the full conjecture under the generalised Riemann hypothesis by Klingler, Ullmo and Yafaev. However, this proof diverged from the original strategy of Edixhoven, which used only tools from arithmetic geometry, in that it also relied on ergodic theory. Here we explain how to eliminate ergodic theory from the proof, first in a special case and then in general, by introducing a new lower bound for the degrees of special subvarieties. First, however, we give an introduction to the theory of Shimura varieties for the purposes of studying this subject.

Contents

1 Introduction **8**

1.1 History 9

1.2 Literature review 12

2 Shimura varieties **16**

2.1 Hermitian symmetric domains 16

2.2 Conjugacy classes 19

2.3 The Deligne torus 21

2.4 Hodge structures 23

2.5 Abelian varieties 25

2.6 The Siegel upper half-space 28

2.7 Families of Hodge structures 30

2.8 The algebraic group 31

2.9 Shimura data 31

2.10 Congruence subgroups 33

2.11 Adéles 34

2.12 Neatness 35

2.13 Shimura varieties 36

2.14 Complex structure 37

2.15 Algebraic structure 37

2.16 Special subvarieties 39

2.17 Special points 40

2.18 Canonical model 41

3 The Pila-Zannier strategy **44**

3.1 Reductions 45

3.2 Galois orbits 46

3.3 Realisations 47

3.4 Heights 48

3.5 Definability 50

3.6 Ax-Lindemann-Weierstrass 51

3.7 Pila-Wilkie 51

3.8 Final reduction 52

3.9 Implementation 53

4 Hilbert modular surfaces **55**

4.1 Bounds on the heights of special points 57

4.2 Characterisation of special subvarieties 62

4.3 Definability 63

4.4 Proof of the main result 65

5 Torsion in class groups of CM tori **67**

5.1 Corollary on n-torsion. 70

5.2 A group theoretic argument. 71

5.3 Covering T. 73

5.4 Uniform boundedness. 77

5.5 Uniformisers. 78

5.6 Small split primes. 85

6 André-Oort for a product of modular curves **89**

6.1 Degrees of strongly special subvarieties 91

6.2 Choosing a suitable Hecke correspondence 92
6.3 Proof of the main result 95
6.4 Manin-Mumford 98

7 Degrees of strongly special subvarieties 101

7.1 Generalities 104
7.2 Reductions 105
7.3 Choosing a measure 106
7.4 Degrees of strongly special subvarieties 108
7.5 Volumes of strongly special subvarieties 109
7.6 Choosing a suitable Hecke correspondence 124
7.7 The geometric criterion 133
7.8 Proof of main result 137
7.9 The André-Oort conjecture 145

1 Introduction

The focus of this thesis is the following conjecture:

Conjecture 1.1. (André-Oort) *Let S be a Shimura variety and let Σ be a set of special points in S. Every irreducible component of the Zariski closure of $\cup_{s\in\Sigma}s$ is a special subvariety of S.*

Shimura varieties are a distinguished class of algebraic varieties that parametrise important objects from linear algebra called Hodge structures. Often these Hodge structures correspond to families of Abelian varieties.

Additional structure on a Shimura variety S arises through the existence of certain algebraic correspondences on S, or subvarieties of $S \times S$, called Hecke correspondences. We can think of these as one-to-many maps

$$T : S \to S.$$

We endow S with a set of so-called special subvarieties, defined as the set of all connected components of Shimura subvarieties and the irreducible components of their images under Hecke correspondences. This is analogous to the case of Abelian varieties (resp. algebraic tori), where special subvarieties are the translates of Abelian subvarieties (resp. subtori) by torsion points. A key property of special subvarieties is that connected components of their intersections are themselves special subvarieties. Thus, any subvariety Y of S is contained in a smallest special subvariety. If this happens to be a connected component of S itself, then we say that Y is Hodge generic in S.

We refer to the special subvarieties of dimension zero as special points. Special subvarieties contain a Zariski (in fact, analytically) dense set of special points. The André-Oort conjecture predicts that this property characterises special subvarieties.

Our investigations are inspired by several different approaches to Conjecture 1.1. In [KY] and [UYa], Klingler, Ullmo and Yafaev combine ergodic theory with tools from arithmetic geometry to prove André-Oort under the generalised Riemann hypothesis (GRH). On the other hand, in [Pil11], Pila gives an unconditional proof via o-minimality of the conjecture for a product of modular curves.

In this thesis, we explain how to remove the complicated theorems of ergodic theory from the proof of Klingler, Ullmo and Yafaev, thus yielding a new proof of the André-Oort conjecture under the GRH using only arithmetic geometry. In order to achieve this, we present a new lower bound for the degrees of special subvarieties. We test our strategy on a product of modular curves.

Firstly, however, we explore the strategy employed by Pila, and eventually obtain an unconditional proof of André-Oort for Hilbert modular surfaces (this is a joint work with A. Yafaev). We also obtain results under the GRH on the size of n-torsion in the class of group of an algebraic torus, which originated from investigations into Galois orbits of special points. These play a central role in both of the aforementioned approaches.

1.1 History

We appeal to [Pin05a]. Recall the following theorem:

Theorem 1.2. (Mordell-Weil) *For any Abelian variety A over a number field K, the group of rational points $A(K)$ is finitely generated.*

Mordell also made the following conjecture in the case $K = \mathbb{Q}$, famously proved by Faltings in 1983:

Conjecture 1.3. (Mordell) *For any irreducible smooth projective algebraic curve Z of genus at least 2 over a number field K, the set of rational points $Z(K)$ is finite.*

Another way of interpreting this conjecture is in terms of Abelian varieties: if $Z(K)$ is empty then there is nothing to prove. Otherwise, we can embed Z into its Jacobian variety J such that $Z(K) = J(K) \cap Z$. By the Mordell-Weil theorem, $J(K)$ is a finitely generated group. Thus, we have motivated a generalisation: consider an Abelian variety A over a field of characteristic zero; for any finitely generated subgroup $\Lambda \subset A$ and any irreducible curve $Z \subset A$ of genus at least 2, is the intersection $Z \cap \Lambda$ finite?

This point of view signalled a further line of enquiry. In their efforts to prove the Mordell conjecture, Manin and Mumford both raised the following question:

Conjecture 1.4. (Manin-Mumford) *Let A be an Abelian variety over $\mathbb{C}$ and let A_{tor} denote its subgroup of all torsion points. Let $Z \subset A$ be an irreducible closed algebraic subvariety such that $Z \cap A_{tor}$ is Zariski dense in Z. Then Z is a translate of an Abelian subvariety of A by a torsion point.*

Now let Λ_0 be a finitely generated subgroup of A. Define its division group to be

$$\Lambda := \{a \in A \mid \exists n \in \mathbb{N} : na \in \Lambda_0\}.$$

Lang combined the previous conjectures into the following:

Conjecture 1.5. (Mordell-Lang) *Let A be an Abelian variety over $\mathbb{C}$ and Λ the division group of a finitely generated subgroup of A. Let $Z \subset A$ be an irreducible closed algebraic subvariety such that $Z \cap \Lambda$ is Zariski dense in Z. Then Z is a translate of an Abelian subvariety of A.*

Let us briefly recall the definition of a Shimura variety from [Edi01]. Let $\mathbb{S}$ denote $\mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{m,\mathbb{C}}$, the algebraic group over $\mathbb{R}$ obtained by restriction of scalars from $\mathbb{C}$ to $\mathbb{R}$ of the multiplicative group. A Shimura datum is a pair (G, X), where G is a connected reductive affine algebraic group over $\mathbb{Q}$ and X is a $G(\mathbb{R})$-conjugacy class in the set of morphisms of algebraic groups $\mathrm{Hom}(\mathbb{S}, G_{\mathbb{R}})$, satisfying the three conditions of Deligne [Del77]. For a Shimura datum (G, X) and a compact open subgroup $K \subset G(\mathbb{A}_f)$, we denote by $\mathrm{Sh}_K(G, X)(\mathbb{C})$ the complex analytic variety $G(\mathbb{Q})\backslash(X \times G(\mathbb{A}_f))/K$, which by [BB66] naturally has the structure of a quasi-projective algebraic variety over $\mathbb{C}$, denoted $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$. The projective limit $\mathrm{Sh}(G, X)_{\mathbb{C}}$, over all K, of the $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ is a scheme (not of finite type) over $\mathbb{C}$ on which $G(\mathbb{A}_f)$ acts continuously. A morphism of Shimura data from (G_1, X_1) to (G_2, X_2) is a morphism $G_1 \to G_2$ mapping X_1 to X_2 and induces a morphism

$$\mathrm{Sh}(G_1, X_1)_{\mathbb{C}} \to \mathrm{Sh}(G_2, X_2)_{\mathbb{C}}.$$

Given a Shimura datum (G, X) and a compact open subgroup $K \subset G(\mathbb{A}_f)$, the special subvarieties of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ are the irreducible components of the images of the maps

$$\mathrm{Sh}(G', X')_{\mathbb{C}} \to \mathrm{Sh}(G, X)_{\mathbb{C}} \xrightarrow{\cdot g} \mathrm{Sh}(G, X)_{\mathbb{C}} \to \mathrm{Sh}_K(G, X)_{\mathbb{C}},$$

where $g \in G(\mathbb{A}_f)$ and (G', X') is a Shimura datum such that there exists a morphism $(G', X') \to (G, X)$. The special points are the zero-dimensional special subvarieties.

Therefore, the André-Oort conjecture is the Manin-Mumford conjecture written in the context of Shimura varieties. Special points take the place of torsion points and irreducible components of Shimura subvarieties and of their images under Hecke correspondences take the place of Abelian subvarieties translated by torsion points. The group structure of torsion points is replaced by an invariance under all Hecke correspondences, whereas both types of points carry an associated Galois action and form dense subsets for the strong topology. These analogies prompted André [And89] and Oort [Oor97] to independently pose special cases of the conjecture named for them today.

Far reaching generalisations of the two conjectures have led to several new questions in the context of mixed Shimura varieties, encapsulating André-Oort, Manin-Mumford, Mordell-Lang and others. Such problems are widely referred to as the Zilber-Pink conjectures (see, for example, [Pin05a], [Pin05b] and [Zil02]).

1.2 Literature review

The André-Oort conjecture is named for Yves André and Frans Oort, both having proposed the conjecture in lesser generality. In 1989, André [And89] postulated that any curve in an arbitrary Shimura variety containing infinitely many special points was special, whereas, in 1994, Oort [Oor97] formulated the conjecture as we know it today for the moduli spaces of principally polarised Abelian varieties.

Initial progress on Oort's question was made by Moonen [Moo98b], who answered it affirmatively for any set of special points and a prime p such that each point has an ordinary reduction mod p of which it is the canonical lift. Yafaev [Yaf05] would later find a suitable generalisation of this criterion for an arbitrary Shimura variety and prove the corresponding conjecture in that case.

In 1998, André [And98] proved his conjecture for a product of two modular curves. Edixhoven [Edi98] obtained the same result under the GRH, but with a method that he was later able to generalise to the case of an arbitrary product of modular curves [Edi05]. Edixhoven [Edi01] also proved the conjecture under the GRH for Hilbert modular surfaces.

Edixhoven and Yafaev [EY03] settled unconditionally the case of a curve in an arbitrary Shimura variety containing an infinite set of special points whose corresponding $\mathbb{Q}$-Hodge structures lie in one isomorphism class. This result was motivated by its applications to transcendence theory and, more specifically, to the algebraicity of values of hypergeometric functions at algebraic numbers (see [CW01] and [Wol88]).

Yafaev [Yaf01] generalised Edixhoven's strategy to the product of two Shimura curves and later obtained under the GRH lower bounds for Galois orbits of special points, allowing him to give a conditional proof of André's original conjecture [Yaf06]. Meanwhile, Clozel and Ullmo [CU05] gave an unconditional proof of the conjecture for sets of strongly special subvarieties using equidistribution. Collaborations between Ullmo and Yafaev [UYa] and Klingler and Yafaev [KY] culminated in a proof of the conjecture in full generality under the GRH, which combined equidistribution with the geometric arguments first introduced by Edixhoven.

Hope of an unconditional proof of the conjecture has arisen via a new strategy of Pila-Zannier [PZ08], implementing Pila's generalisation [Pil09b] of the so-called Pila-Wilkie counting theorem [PW06], which provides strong bounds for the number of points of bounded degree up to a given height on sets definable in o-minimal structures. Pila has given unconditional proofs of the conjecture for a product of two [Pil09a] and, subsequently, arbitrarily many [Pil11] modular curves. With Yafaev [DY11], we implemented this method to give an unconditional proof in the case of Hilbert modular surfaces.

At this point, there were several obstructions to the development of a proof via o-minimality in full generality. The principal obstruction, which remains a problem today, is the lack of unconditional lower bounds for Galois orbits of special points. However, Tsimerman [Tsi12] recently obtained unconditional bounds for the moduli spaces of principally polarised Abelian varieties of dimension at most 6. Consequently, Pila and Tsimerman [PT13] gave a proof of the conjecture for the moduli space of Abelian surfaces, also exhibiting special cases of the remaining obstructions. Namely, in the case of the moduli spaces of principally polarised Abelian varieties, they gave upper bounds for the heights of pre-special points in fundamental domains and, for the moduli space of Abelian surfaces they proved the so-called Ax-Lindemann-Weierstrass criterion. Ullmo and Yafaev [UY14] later gave a proof of this criterion in the co-compact case, which was followed by a proof due to Pila and Tsimerman [PT14] for the moduli spaces of principally polarised Abelian varieties and, finally, by a proof in full generality due to Klingler, Ullmo and Yafaev [KUY13]. Ullmo [Ull13] had previously explained how the result of Pila and Tsimerman would prove the conjecture for products of the moduli space of principally polarised Abelian varieties of dimension at most 6.

Finally, it also worth mentioning a few related results. Firstly, Kühne [Küh12] has obtained an effective statement of the André-Oort conjecture for a curve in $\mathbb{C}^2$. Secondly, Habegger and Pila [HP12] and Orr [Orr13] have both implemented techniques from o-minimality to prove certain cases of the aforementioned conjectures of Pink.

2 Shimura varieties

Firstly, we provide an introduction to the theory of Shimura varieties, as formulated by Deligne in his foundational articles [Del71] and [Del77]. This is not intended, by any means, to be a full treatment of the topic but rather a preparatory guide. We refer the reader to [Mil04] for a comprehensive account of Shimura varieties and for further details regarding the topics introduced here.

We are primarily interested in the connected components of Shimura varieties. These initially arise as quotients $\Gamma\backslash D$, where D is a certain type of complex manifold called a Hermitian symmetric domain, and Γ is a congruence subgroup, acting via holomorphic automorphisms. The prototypical example is the case of the upper half-plane

$$D = \mathbb{H} := \{z \in \mathbb{C} : \Im(z) > 0\}$$

and $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, where any element of $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

2.1 Hermitian symmetric domains

We refer the reader to [Mil04], §1 for a more detailed introduction to Hermitian symmetric domains. Unfortunately, the definition is not particularly enlightening:

Definition 2.1. *A Hermitian symmetric domain is a connected complex manifold D such that*

- *D is equipped with a Hermitian metric.*

- *The group* $\mathrm{Aut}(D)$ *of holomorphic isometries acts transitively on D.*

- *There exists a point $\tau \in D$ and an involution $\varphi \in$* $\mathrm{Aut}(D)$ *such that τ is an isolated fixed point of φ.*

- *D is of non-compact type.*

In fact, by [Mil04], Lemma 1.5, the neutral component $\mathrm{Aut}(D)^+$ acts transitively on D and, by [Mil04], Proposition 1.6, it coincides with $\mathrm{Hol}(D)^+$, where $\mathrm{Hol}(D)$ denotes the group of all holomorphic automorphisms. Note that, given the transitivity of the $\mathrm{Aut}(D)$ action, the third condition is true for all points.

Returning to our earlier example,

$$\mathrm{Hol}(\mathbb{H}) = \mathrm{SL}_2(\mathbb{R})/\{\pm\mathrm{id}\}$$

and, since $\mathrm{SL}_2(\mathbb{R})$ is connected, it consists only of isometries. The element

$$\varphi := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

fixes only $i \in \mathbb{H}$, whereas $\varphi^2 = -\mathrm{id}$. Hence, the image of φ in $\mathrm{Hol}(\mathbb{H})$ is an involution of $\mathbb{H}$ with an isolated fixed point.

However, from this definition follows a key property of Hermitian symmetric domains. By [Mil04], Theorem 1.9, if we denote by $\mathbb{U}(\mathbb{R})$ the circle group $\{z \in \mathbb{C} : |z| = 1\}$, then, for each point $\tau \in D$, there exists a unique homomorphism

$$u_\tau : \mathbb{U}(\mathbb{R}) \to \mathrm{Hol}(D)^+$$

such that, for all $z \in \mathbb{U}(\mathbb{R})$,

- $u_\tau(z)(\tau) = \tau$.
- $u_\tau(z)$ acts as multiplication by z on the tangent plane of D at τ.

For example, consider the point $i \in \mathbb{H}$ and let

$$h : \mathbb{U}(\mathbb{R}) \to \mathrm{SL}_2(\mathbb{R}) : z = a + ib \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Then, for all $z \in \mathbb{U}(\mathbb{R})$, $h(z)$ fixes i and

$$\frac{d}{dz}\left(\frac{az+b}{-bz+a}\right)\bigg|_i = \frac{a^2+b^2}{(a-bi)^2} = \frac{z}{\bar{z}}.$$

Therefore, if we define

$$u : \mathbb{U}(\mathbb{R}) \to \mathrm{SL}_2(\mathbb{R})/\{\pm\mathrm{id}\} : \mathrm{z} \mapsto \mathrm{h}(\sqrt{\mathrm{z}}) \bmod \pm\,\mathrm{id},$$

which is well-defined since $h(-1) = -\mathrm{id}$, then $u(z)$ acts on the tangent plane of $\mathbb{H}$ at i as multiplication by z.

Furthermore, note that, if $g \in \mathrm{Hol}(D)^+$ and $\tau \in D$, the uniqueness of $u_{g\tau}$ implies that it must be the conjugate

$$g u_\tau g^{-1} : z \mapsto g u_\tau(z) g^{-1}.$$

Therefore, since $\mathrm{Hol}(D)^+$ acts transitively on D, if we fix a point $\tau_0 \in D$, we have a $\mathrm{Hol}(D)^+$-equivariant bijection between D and the $\mathrm{Hol}(D)^+$-conjugacy class of u_{τ_0}.

2.2 Conjugacy classes

By [Mil04], Proposition 1.7, for any Hermitian symmetric domain D, there exists a unique semisimple algebraic group G over $\mathbb{R}$ of adjoint type such that

$$G(\mathbb{R})^+ = \mathrm{Hol}(D)^+.$$

By a linear algebraic group G over $\mathbb{R}$, we simply mean a group that can be defined as a subgroup of $\mathrm{GL}_n(\mathbb{R})$ by real polynomials in the matrix coefficients. For example, $\mathbb{U}(\mathbb{R})$ is an algebraic group over $\mathbb{R}$ whose elements may be realised as those

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

such that $a = d$, $b = -c$ and, thus, $a^2+b^2 = 1$. However, since $\mathbb{U}(\mathbb{R})$ is defined by polynomials, we can think of $\mathbb{U}(\mathbb{R})$ as the real points of what is usually considered the algebraic group, which we denote $\mathbb{U}$. Then, for any $\mathbb{R}$-algebra A, $\mathbb{U}(A)$ is simply the group of solutions in A to the above polynomials.

By a semisimple algebraic group we mean a connected (for the Zariski topology) linear algebraic group that is isogenous to a product of almost-simple subgroups. By a simple algebraic group we mean a connected linear algebraic group that is not commutative and has no proper normal algebraic subgroups other than the identity. By an almost-simple subgroup we mean a subgroup that is a simple algebraic group modulo a finite centre. By adjoint we are referring to a group with trivial centre and, for an algebraic group G, we write G^{ad} for G modulo its centre.

As shown in [Mil04], §1, every representation

$$\mathbb{U}(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$$

is algebraic i.e. the image is given by polynomials in the matrix entries. In particular, for any $\tau \in D$, we may consider the homomorphism

$$u_\tau : \mathbb{U}(\mathbb{R}) \to G(\mathbb{R})^+$$

as an algebraic morphism $u_\tau : \mathbb{U} \to G$, yielding a morphism

$$u_\tau : \mathbb{U}(A) \to G(A)$$

for any $\mathbb{R}$-algebra A.

The group $\mathbb{U}$ is connected, commutative and consists entirely of semisimple elements. We refer to an algebraic group of this sort as a torus and, for any representation

$$\mathbb{U} \to \mathrm{GL}_n,$$

the image of $\mathbb{U}(\mathbb{R})$ in $\mathrm{GL}_n(\mathbb{C})$ can be simultaneously diagonalised by a single element. Furthermore, the eigenvalues are given by homomorphisms $\mathbb{U}_\mathbb{C} \to \mathbb{G}_m$ called characters, where we write $\mathbb{U}_\mathbb{C}$ for $\mathbb{U}$ considered as an algebraic group over $\mathbb{C}$ and $\mathbb{G}_m$ for the algebraic group such that, for any $\mathbb{C}$-algebra A, $\mathbb{G}_m(A) = A^*$. The characters are algebraic since, by definition, they are one-dimensional representations and, in this case, each character is of the form $z \mapsto z^n$, where $n \in \mathbb{Z}$.

By [Mil04], Theorem 1.21, the homomorphism u_τ always satisfies the following three properties:

- Only the characters $z \mapsto 1$, $z \mapsto z$ and $z \mapsto z^{-1}$ occur in the representation of $\mathbb{U}(\mathbb{R})$ on the Lie algebra $\mathfrak{g}_{\mathbb{C}}$ of $G_{\mathbb{C}}$.
- Conjugation by $u_\tau(-1)$ is a Cartan involution of G.
- $u_\tau(-1)$ maps to a non-trivial element in every simple factor of G.

The Lie algebra of $G_{\mathbb{C}}$ is the tangent plane of $G(\mathbb{C})$ at the identity. One definition is the kernel of the map

$$G(\mathbb{C}[\epsilon]) \to G(\mathbb{C})$$

induced by $\epsilon \mapsto 0$, where $\epsilon^2 = 1$. Then $G(\mathbb{C})$ acts on $\mathfrak{g}_{\mathbb{C}}$ by conjugation. For the definition of a Cartan involution see [Mil04], §1.

On the other hand, if G is any semisimple algebraic group over $\mathbb{R}$ of adjoint type and $u : \mathbb{U} \to G$ is a homomorphism satisfying the above three properties, then the $G(\mathbb{R})^+$-conjugacy class of u naturally has the structure of a Hermitian symmetric domain D, for which

$$G(\mathbb{R})^+ = \mathrm{Hol}(D)^+$$

and $u(-1)$ is the involution associated to u when regarded as a point of D.

2.3 The Deligne torus

Let $\mathbb{S}$ denote the real algebraic group such that $\mathbb{S}(\mathbb{R}) = \mathbb{C}^*$. This is a torus, usually referred to as the Deligne torus, and we have a short exact sequence

$$1 \to \mathbb{G}_m \xrightarrow{w} \mathbb{S} \to \mathbb{U} \to 1,$$

which on real points corresponds to

$$1 \to \mathbb{R}^* \xrightarrow{r \mapsto r^{-1}} \mathbb{C}^* \xrightarrow{z \mapsto z/\bar{z}} \mathbb{U}(\mathbb{R}) \to 1.$$

Therefore, any homomorphism $u : \mathbb{U} \to G$ yields a homomorphism

$$h : \mathbb{S} \to G,$$

defined by $h(z) = u(z/\bar{z})$. Furthermore, $\mathbb{U}(\mathbb{R})$ will act on $\mathfrak{g}_{\mathbb{C}}$ via the characters $z \mapsto 1$, $z \mapsto z$ and $z \mapsto z^{-1}$ if and only if $\mathbb{S}(\mathbb{R})$ acts on $\mathfrak{g}_{\mathbb{C}}$ via the characters $z \mapsto 1$, $z \mapsto z/\bar{z}$ and $z \mapsto \bar{z}/z$.

Conversely, let $h : \mathbb{S} \to G$ be a homomorphism such that $\mathbb{S}$ acts on $\mathfrak{g}_{\mathbb{C}}$ via the characters $z \mapsto 1$, $z \mapsto z/\bar{z}$ and $z \mapsto \bar{z}/z$. Then $w(\mathbb{G}_m(\mathbb{R}))$ acts trivially on $\mathfrak{g}_{\mathbb{C}}$, which implies that h is trivial on $w(\mathbb{G}_m(\mathbb{R}))$, since the adjoint representation of G on $\mathfrak{g}$ is faithful. Thus, h arises from a homomorphism $u : \mathbb{U} \to G$.

Therefore, to give a $G(\mathbb{R})^+$-conjugacy class D of homomorphisms $u : \mathbb{U} \to G$ satisfying the above three properties is the same as to give a $G(\mathbb{R})^+$-conjugacy class X^+ of homomorphisms $h : \mathbb{S} \to G$ satisfying the following:

- Only the characters $z \mapsto 1$, $z \mapsto z/\bar{z}$ and $z \mapsto \bar{z}/z$ occur in the representation of $\mathbb{S}(\mathbb{R})$ on $\mathfrak{g}_{\mathbb{C}}$.
- Conjugation by $h(i)$ constitutes a Cartan involution of G.
- The element $h(i)$ maps to a non-trivial element in every simple factor of G.

2.4 Hodge structures

Therefore, the question should be *why are we interested in such conjugacy classes of morphisms* $h : \mathbb{S} \to G$*?* To understand this, we need the definiton of a Hodge structure. For further details, we refer the reader to [Mil04], §2.

For a real vector space V, we define complex conjugation on

$$V(\mathbb{C}) := V \otimes_{\mathbb{R}} \mathbb{C}$$

by $\overline{v \otimes z} := v \otimes \overline{z}$. A Hodge decomposition of V is a decomposition

$$V(\mathbb{C}) = \bigoplus_{(p,q)\in\mathbb{Z}\times\mathbb{Z}} V^{p,q}$$

such that $\overline{V^{p,q}} = V^{q,p}$. A Hodge structure is a real vector space V with a Hodge decomposition. The set of pairs (p, q) such that $V^{p,q} \neq 0$ is called the type of the Hodge structure and we refer to a Hodge structure of type $(-1, 0), (0, -1)$ as a complex structure.

For each $n \in \mathbb{Z}$,

$$\bigoplus_{p+q=n} V^{p,q}$$

is stable under complex conjugation and equal to $V_n(\mathbb{C})$ for some real subspace V_n of V. The decomposition $V = \oplus_n V_n$ is called the weight decomposition of V. If $V = V_n$, then V is said to have weight n. The Hodge filtration associated with a Hodge structure V of weight n is

$$F := \{\cdots \supset F^p \supset F^{p+1} \supset \cdots\},\ F^p := \oplus_{r\geq p} V^{r,n-r}.$$

A $\mathbb{Z}$-(resp. $\mathbb{Q}$-)Hodge structure is a free $\mathbb{Z}$-module (resp. $\mathbb{Q}$-vector space) V of finite rank (resp. dimension) equipped with a Hodge decomposition of

$$V(\mathbb{R}) := V \otimes \mathbb{R}$$

such that the weight decomposition is defined over $\mathbb{Q}$.

We can identify $\mathbb{S}$ with a closed subgroup of GL_2 as follows: for any $\mathbb{R}$-algebra A, we realise $\mathbb{S}(A)$ as those matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{GL}_2(A).$$

Diagonalising, $\mathbb{S}_{\mathbb{C}}$ is isomorphic to $\mathbb{G}_m^2$, with complex conjugation on $\mathbb{S}(\mathbb{C})$ corresponding to $(z_1, z_2) \mapsto (\overline{z_2}, \overline{z_1})$. Therefore, the elements of $\mathbb{S}(\mathbb{R})$ map to the elements $(z, \overline{z})$, stable under conjugation. More generally, the characters of $\mathbb{S}_{\mathbb{C}}$ are the homomorphisms

$$(z_1, z_2) \mapsto z_1^p z_2^q,$$

for any $(p, q) \in \mathbb{Z} \times \mathbb{Z}$, with complex conjugation acting as $(p, q) \mapsto (q, p)$.

Consequently, to give a representation of $\mathbb{S}$ on a real vector space V is the same as to give a $\mathbb{Z} \times \mathbb{Z}$-grading of $V(\mathbb{C})$ such that $\overline{V^{p,q}} = V^{q,p}$ for all p and q, which is precisely the definition of a Hodge structure on V. We thus define morphisms, tensor products and duals of Hodge structures as morphisms, tensor products and duals of representations of $\mathbb{S}$. We normalise the relation so that (z_1, z_2) acts on $V^{p,q}$ as $z_1^{-p} z_2^{-q}$. A complex structure on a real vector space V is then precisely a Hodge structure $\mathbb{S} \to \mathrm{GL}(V)$ coming from a homomorphism $\mathbb{C} \to \mathrm{End}(V)$.

For $n \in \mathbb{Z}$ and $R = \mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, we let $R(n)$ be the (R-)Hodge structure $V = R$, where $\mathbb{S}$ acts on $V(\mathbb{R}) = \mathbb{R}$ by the character $(z\overline{z})^n$ and, hence,

$$V(\mathbb{C}) = V_{-n}(\mathbb{C}).$$

This is referred to as a Tate twist. For an (R-)Hodge structure V of weight n, a Hodge tensor is a multilinear form $t : V^r \to R$ such that the map

$$V \otimes V \otimes \cdots \otimes V \to R(-nr/2)$$

is a morphism of Hodge structures.

If we denote by $C := h(i)$ the so-called Weil operator, then a polarisation on V is a Hodge tensor

$$\psi : V \times V \to R$$

such that

$$\psi_C : V(\mathbb{R}) \times V(\mathbb{R}) \to \mathbb{R} : (x, y) \mapsto \psi(x, Cy)$$

is symmetric and positive definite. A polarisation on an (R-)Hodge structure $V = \oplus_n V_n$ is a system $(\psi_n)_n$ of polarisations on the V_n.

2.5 Abelian varieties

Consider an Abelian variety A over $\mathbb{C}$ of dimension g. Then A is isomorphic to a complex torus $\mathbb{C}^g/\Lambda$, where Λ is the $\mathbb{Z}$-module generated by an $\mathbb{R}$-basis for $\mathbb{C}^g$. The isomorphism $\Lambda \otimes \mathbb{R} \cong \mathbb{C}^g$ defines a complex structure on $\Lambda \otimes \mathbb{R}$ and there exists an alternating form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

such that $\psi_{\mathbb{R}}(x, Cy)$ is symmetric and positive definite and

$$\psi_{\mathbb{R}}(Cx, Cy) = \psi_{\mathbb{R}}(x, y),$$

for all $x, y \in \Lambda \otimes \mathbb{R}$. In other words, $\Lambda \cong H_1(A, \mathbb{Z})$ is a $\mathbb{Z}$-Hodge structure of weight -1 equipped with a polarisation. In fact, by [Mil04], Theorem 6.8, the functor $A \mapsto H_1(A, \mathbb{Z})$ is an equivalence from the category of Abelian varieties over $\mathbb{C}$ to the category of polarised $\mathbb{Z}$-hodge structures of type $(-1, 0), (0, -1)$. Therefore, the answer to the question of the previous section is that *one can study the problem of parametrising Abelian varieties in terms of Hodge structures.*

Consider the case of Abelian varieties of dimension one, otherwise known as elliptic curves. An elliptic curve over $\mathbb{C}$ is the quotient of $\mathbb{C}$ by a free $\mathbb{Z}$-module Λ of rank 2. Two elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^*$. We recall the exposition found in [Har13].

Often, when considering elliptic curves, we fix $\mathbb{C}$ and vary Λ. Instead, however, we may fix $\Lambda := \mathbb{Z}^2$ and vary the complex structure on $\mathbb{Z}^2 \otimes \mathbb{R} = \mathbb{R}^2$ i.e. we vary the morphism

$$h : \mathbb{C}^* \to \mathrm{GL}_2(\mathbb{R}),$$

coming from a homomorphism $\mathbb{C} \to \mathrm{M}_2(\mathbb{R})$ of $\mathbb{R}$-algebras. Given such a morphism, we obtain an isomorphism of complex vector spaces $i_h : \mathbb{R}^2 \to \mathbb{C}$ defined by

$$i_h^{-1}(z) = h(z) \cdot i_h^{-1}(1) := h(z) \cdot e_0,$$

where we choose $e_0 = (1, 0) \in \mathbb{R}^2$. The quotient $\mathbb{C}/i_h(\mathbb{Z}^2)$ is an elliptic curve.

Therefore, let

$$h_0 : \mathbb{C}^* \to \mathrm{GL}_2(\mathbb{R}) : a + ib \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

and let $h := \gamma h_0 \gamma^{-1}$, where

$$\gamma = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+.$$

Note that, for any such h, the standard symplectic form given by

$$(u, v) \mapsto u^t \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} v$$

is a polarisation for the corresponding $\mathbb{Z}$-Hodge structure.

For $h_0(z)$, the z-eigenspace in $\mathbb{R}^2 \otimes \mathbb{C}$ is the complex subspace generated by $(-i, 1)$. The $\overline{z}$-eigenspace is its complex conjugate, generated by $(i, 1)$. Therefore, for $h(z)$, the z-eigenspace is generated by

$$\begin{pmatrix} x & y \\ w & z \end{pmatrix} \begin{pmatrix} -i \\ 1 \end{pmatrix} = \begin{pmatrix} -xi + y \\ -wi + z \end{pmatrix}$$

or, equivalently, $(\overline{\tau}_h, 1)$, where $\tau_h := xi + y/wi + z$, and the $\overline{z}$-eigenspace is generated by $(\tau_h, 1)$. Note that this latter subspace is precisely the middle term in the filtration associated to the $\mathbb{Z}$-Hodge structure given by h.

Now, i_h extends $\mathbb{C}$-linearly to a map

$$i_{h,\mathbb{C}} : \mathbb{R}^2 \otimes \mathbb{C} = \mathbb{C} \cdot \begin{pmatrix} \overline{\tau}_h \\ 1 \end{pmatrix} \oplus \mathbb{C} \cdot \begin{pmatrix} \tau_h \\ 1 \end{pmatrix} \to \mathbb{C}$$

and, since it commutes with the action of $\mathbb{C}$ on both sides, we deduce that $i_{h,\mathbb{C}}$ is the quotient of $\mathbb{R}^2 \otimes \mathbb{C}$ by the $\overline{z}$-eigenspace. Therefore, since $i_h(e_0) = 1$ and $i_h((0, 1)) = i_h(-\tau_h e_0 + (\tau_h, 1)) = -\tau_h$,

$$i_h(\mathbb{Z}^2) = \mathbb{Z} \oplus \mathbb{Z}\tau_h.$$

We conclude that $\mathbb{C}/i_h(\mathbb{Z}^2)$ varies over all isomorphism classes of elliptic curves as h varies over the $\mathrm{GL}_2(\mathbb{R})^+$-conjugacy class of h_0. The map $h \mapsto \tau_h$ is a $\mathrm{GL}_2(\mathbb{R})^+$-equivariant bijection between this conjugacy class and $\mathbb{H}$.

For Abelian varieties of dimension g, the situation is similar. We replace $\mathbb{Z}^2$ by $\mathbb{Z}^{2g}$ and fix the standard symplectic form given by

$$-J := \begin{pmatrix} 0 & -\mathrm{id} \\ \mathrm{id} & 0 \end{pmatrix}.$$

We let

$$h_0 : \mathbb{C}^* \to \mathrm{GL}_{2g}(\mathbb{R}) : a + bi \mapsto a + bJ,$$

which factors through the group

$$\mathrm{GSp}_{2g}(\mathbb{R}) = \{g \in \mathrm{GL}_{2g}(\mathbb{R}) : g^t J g = \det(g) J\}.$$

Then the $\mathrm{GSp}_{2g}(\mathbb{R})^+$-conjugacy class of h_0 corresponds to the set of $\mathbb{Z}$-Hodge structures on $\mathbb{Z}^{2g}$ having type $(-1,0),(0,-1)$ for which J induces a polarisation. Using the description of the Hodge filtration, as in the case of elliptic curves, one can identify this set in a $\mathrm{GSp}_{2g}(\mathbb{R})^+$-equivariant manner with a Hermitian symmetric domain

$$\mathbb{H}_g := \{Z = X + iY \in M_{g\times g}(\mathbb{C}) : Z = Z^t, Y > 0\}$$

called the Siegel upper half-space of genus g.

2.6 The Siegel upper half-space

Having fixed a $g \in \mathbb{N}$, we denote the Hodge structure corresponding to a point $\tau \in \mathbb{H}_g$ by V_τ and we denote the corresponding Hodge filtration by F_τ.

For any given $(p,q) \in \mathbb{Z} \times \mathbb{Z}$, the dimension $d(p,q)$ of $V_\tau^{p,q}$ is constant as τ varies over $\mathbb{H}_g$ and we have a continuous map

$$\tau \mapsto [V_\tau^{p,q}] : \mathbb{H}_g \to \mathrm{G}_{d(p,q)}(V(\mathbb{C})),$$

from $\mathbb{H}_g$ to the complex projective variety of $d(p,q)$-dimensional subspaces of $V(\mathbb{C})$.

Furthermore, the subspace dimensions of F_τ are also constant as τ varies over $\mathbb{H}_g$ and, if we denote by $\mathrm{F}_d(V(\mathbb{C}))$ the complex projective variety parametrising such filtrations of $V(\mathbb{C})$, then the map

$$f : \tau \mapsto [F_\tau] : \mathbb{H}_g \to \mathrm{F}_d(V(\mathbb{C}))$$

is holomorphic. In light of these properties, we refer to the set of Hodge structures corresponding to the points of $\mathbb{H}_g$ as a holomorphic family of Hodge structures.

Finally, the differential of f at τ is a $\mathbb{C}$-linear map

$$df_\tau : T_\tau \mathbb{H}_g \to T_{[F_\tau]} \mathrm{F}_d(V(\mathbb{C}))$$

from the tangent plane of $\mathbb{H}_g$ at τ to the tangent plane of $\mathrm{F}_d(V(\mathbb{C}))$ at $[F_\tau]$. By [Mil04], (17), $T_{[F_\tau]} \mathrm{F}_d(V(\mathbb{C}))$ is a subset of

$$\bigoplus_p \mathrm{Hom}(F_\tau^p, V(\mathbb{C})/F_\tau^p)$$

but, in this case, the image of df_τ is actually contained in the space

$$\bigoplus_p \mathrm{Hom}(F_\tau^p, F_\tau^{p-1}/F_\tau^p)$$

and we say that this holomorphic family of Hodge structures is a variation of Hodge structures.

2.7 Families of Hodge structures

We abstract the above situation as follows: let V be a finite dimensional $\mathbb{R}$-vector space and let T be a finite set of tensors on V, including a nondegenerate bilinear form t_0. Fix an $n \in \mathbb{N}$ and let

$$d : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$$

be a symmetric function such that $d(p, q) = 0$ for almost all (p, q), including every (p, q) such that $p + q \neq n$.

Consider the set $S(d, T)$ of Hodge structures on V such that, for all $(p, q) \in \mathbb{Z} \times \mathbb{Z}$,

$$\dim V^{p,q} = d(p, q),$$

every $t \in T$ is a Hodge tensor and t_0 is a polarisation. This is naturally a subspace of

$$\prod_{(p,q):d(p,q)\neq 0} \mathrm{G}_{d(p,q)}(V(\mathbb{C}))$$

and so $S(d, T)$ can be given the subspace topology and, by [Mil04], Theorem 2.14, (assuming it is non-empty) any connected component has a unique complex structure such that the corresponding set of Hodge structures constitute a holomorphic family. Furthermore, if such a family is actually a variation of Hodge structures, then the corresponding connected component S^+ has the structure of a Hermitian symmetric domain. In fact, every Hermitian symmetric domain is of the form S^+ for a suitable V, T and d.

2.8 The algebraic group

Recall the topological space $S(d,T)$ from the previous section and let S^+ be a connected component. Fix a point $h_0 \in S^+$ and let G be the smallest algebraic subgroup of $\mathrm{GL}(V)$ such that

$$h : \mathbb{S} \to \mathrm{GL}(V)$$

factors through G for every $h \in S^+$ i.e. the intersection of all subgroups having this property. As in the proof of [Mil04], Theorem 2.14 (a), for any $g \in G(\mathbb{R})^+$, $gh_0g^{-1} \in S^+$ and, in fact, the map

$$g \mapsto gh_0g^{-1} : G(\mathbb{R})^+ \to S^+$$

is surjective. In other words, S^+ is the $G(\mathbb{R})^+$-conjugacy class of h_0.

2.9 Shimura data

Motivated by our example of Abelian varieties, we want to consider $\mathbb{Z}$-(or $\mathbb{Q}$)-Hodge structures. This will be achieved by choosing an algebraic group G defined over $\mathbb{Q}$ and embedding this into $\mathrm{GL}(V)$ for some $\mathbb{Q}$-vector space V. The $\mathbb{Z}$-structure will come from the choice of a lattice in V.

Definition 2.2. *A Shimura datum is a pair (G,X), where G is a reductive group over $\mathbb{Q}$ and X is a $G(\mathbb{R})$-conjugacy class of morphisms $h : \mathbb{S} \to G_{\mathbb{R}}$ such that, for one (or, equivalently, all) $h \in X$,*

- *Only the characters $z \mapsto 1$, $z \mapsto z/\bar{z}$ and $z \mapsto \bar{z}/z$ occur in the representation of $\mathbb{S}$ on the Lie algebra $\mathfrak{g}^{\mathrm{ad}}_{\mathbb{C}}$ of $G^{\mathrm{ad}}_{\mathbb{C}}$.*

- *Conjugation by $h(i)$ is a Cartan involution of G^{ad}.*

- *For every simple factor H of G^{ad}, the map $\mathbb{S} \to H_{\mathbb{R}}$ is not trivial.*

By a reductive algebraic group we refer to a connected linear algebraic group with trivial unipotent radical. The unipotent radical of an algebraic group is the unipotent part of its radical, which is the neutral component of its maximal normal, solvable subgroup. The semisimple groups are those algebraic groups with trivial radical. In particular, they are reductive.

Now let (G, X) be a Shimura datum. By the first of the axioms above, $\mathbb{G}_m(\mathbb{R}) = \mathbb{R}^*$, which is naturally a subgroup of $\mathbb{S}(\mathbb{R}) = \mathbb{C}^*$, acts trivially on $\mathfrak{g}^{\mathrm{ad}}_{\mathbb{C}}$. As the action of G on $\mathfrak{g}^{\mathrm{ad}}$ factors through G^{ad} and the action of G^{ad} is faithful, the image of $\mathbb{R}^*$ in $G(\mathbb{R})$ must belong to the centre. In particular, the restriction of any $h \in X$ to $\mathbb{G}_m$ is independent of h and we refer to its reciprocal w as the weight homomorphism since, for any representation $\rho : G_{\mathbb{R}} \to \mathrm{GL}(V)$, $\rho \circ w$ defines the weight decomposition of the Hodge structure given by $\rho \circ h$ on V.

Now let $\rho : G_{\mathbb{R}} \to \mathrm{GL}(V)$ be a faithful representation. By [Mil04], Proposition 5.9, X has a unique structure of a complex manifold such that the family of Hodge structures induced on V by $\rho \circ h$ as h varies over X is holomorphic. In fact, the first axiom implies that it is a variation of Hodge structures. Therefore, from our earlier discussion of families of Hodge structures, X is a finite disjoint union of Hermitian symmetric domains.

Alternatively, consider a connected component X^+ of X. By [Mil04], Proposition 5.7 (a), we may consider X^+ as a $G^{\mathrm{ad}}(\mathbb{R})^+$-conjugacy class of morphisms $\mathbb{S} \to G^{\mathrm{ad}}_{\mathbb{R}}$. Let $h \in X^+$ and decompose $G^{\mathrm{ad}}_{\mathbb{R}}$ into a product of simple factors H_i (over $\mathbb{R}$) so that $h = (h_i)_i$, where h_i is the projection of h to H_i. By [Mil04], Lemma 4.7, if $H_i(\mathbb{R})$ is compact then h_i is trivial. Otherwise, given the conditions satisfied by h, there exists a Hermitian symmetric domain D_i such that $H_i(\mathbb{R})^+$ coincides with $\mathrm{Hol}(D_i)^+$ and D_i is in natural one-to-one correspondence with the $H_i(\mathbb{R})^+$-conjugacy class X_i^+ of h_i. Therefore, the product D of the D_i is a Hermitian symmetric domain on which $G^{\mathrm{ad}}(\mathbb{R})^+$ acts via a surjective homomorphism $G^{\mathrm{ad}}(\mathbb{R})^+ \to \mathrm{Hol}(D)^+$ with compact kernel and there is a natural identification of D with $X^+ = \prod_i X_i^+$.

Definition 2.3. *A morphism of Shimura data*

$$(G_1, X_1) \to (G_2, X_2)$$

is a morphism $\phi : G_1 \to G_2$ such that, for every $h \in X_1$, $\phi \circ h \in X_2$. If ϕ is a closed immersion, we refer to (G_1, X_1) as a Shimura subdatum.

Definition 2.4. *Let (G, X) be a Shimura datum. Let X^{ad} be the $G^{\mathrm{ad}}(\mathbb{R})$-conjugacy class of morphisms $\mathbb{S} \to G^{\mathrm{ad}}_{\mathbb{R}}$ containing the image of X. Then $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ is a Shimura datum called the adjoint Shimura datum and*

$$(G, X) \to (G^{\mathrm{ad}}, X^{\mathrm{ad}})$$

is a morphism of Shimura data.

2.10 Congruence subgroups

Let G be a reductive subgroup of GL_n defined over $\mathbb{Q}$. We denote by $G(\mathbb{Z})$ the group $G(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$. Recall the following definition, independent of the embedding of G in GL_n:

Definition 2.5. *A subgroup Γ of $G(\mathbb{Q})$ is arithmetic if $\Gamma \cap G(\mathbb{Z})$ has finite index in Γ and $G(\mathbb{Z})$ i.e. Γ and $G(\mathbb{Z})$ are commensurable.*

Now suppose that (G, X) is a Shimura datum. We would like to consider the corresponding Hodge structures up to isomorphism and this is the role of the group Γ. We may also wish to distinguish additional structure to that already encoded in the group G. The most obvious such structure is distinguished by the following class of arithmetic subgroups:

Definition 2.6. *The principal congruence subgroup of level N is defined as the group*

$$\Gamma(N) := \{g \in G(\mathbb{Z}) : g \equiv \mathrm{id} \ mod\ N\},$$

where the congruence relation is entry-wise.

In the case of Abelian varieties, where $G = \mathrm{GSp}_{2g}$ and we consider the $\mathbb{Z}$-Hodge structure on $\Lambda = H_1(A, \mathbb{Z})$, the group $\Gamma(N)$ also distinguishes between different bases for the N-torsion subgroup $\frac{1}{N}\Lambda/\Lambda$, rather than simply the isomorphism class of Λ along with its polarisation.

Of course, the definition of the principal congruence subgroup depends on the embedding of G in GL_n. Therefore, we define a congruence subgroup of $G(\mathbb{Q})$ to be a subgroup containing some $\Gamma(N)$ as a subgroup of finite index. This notion does not depend on the embedding.

2.11 Adéles

The ring of finite (rational) adèles $\mathbb{A}_f$ comprises the elements

$$\alpha = (\alpha_p) \in \prod_p \mathbb{Q}_p$$

such that, for almost all primes p, $\alpha_p \in \mathbb{Z}_p$. It is endowed with the topology for which a basis of open sets are those of the form $\prod_p U_p$, where U_p is open in $\mathbb{Q}_p$, and $U_p = \mathbb{Z}_p$ for almost all p. Similarly, for an algebraic group G, defined over $\mathbb{Q}$, one can choose an embedding into GL_n and define $G(\mathbb{A}_f)$ as those elements

$$g = (g_p)_p \in \prod_p G(\mathbb{Q}_p)$$

such that $g_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ for almost all p. However, this definition of $G(\mathbb{A}_f)$ is independent of the embedding into GL_n and so is the basis of open sets, defined analogously to the above.

By [Mil04], Proposition 4.1, for any compact open subgroup K of $G(\mathbb{A}_f)$, $K \cap G(\mathbb{Q})$ is a congruence subgroup Γ of $G(\mathbb{Q})$ and every congruence subgroup arises this way. Loosely speaking, considering the congruence relation defining Γ prime-by-prime gives rise to K, and vice-versa.

Later, we will also need the more general definition of $\mathbb{A}_{E,f}$, the finite adèles over a number field E, which we define as $\mathbb{A}_f \otimes E$ or, equivalently, as the ring of elements

$$\alpha = (\alpha_v) \in \prod_v E_v,$$

over all finite places v of E, such that, for almost all v, $\alpha_v \in \mathcal{O}_{E_v}$. The adèle ring $\mathbb{A}_E$ arises when we include factors for the infinite places of E. Therefore, any $\alpha \in \mathbb{A}_E$ can be written as a pair $(\alpha_\infty, \alpha_f)$, where $\alpha_f \in \mathbb{A}_{E,f}$.

2.12 Neatness

Let G be an algebraic subgroup of GL_n defined over $\mathbb{Q}$. The following definition is independent of the embedding into GL_n:

Definition 2.7. *An element $g \in G(\mathbb{Q})$ is neat if the subgroup of $\overline{\mathbb{Q}}^*$ generated by its eigenvalues is torsion free.*

One says that a congruence subgroup Γ is neat if all of its elements are neat. There is also a notion of neatness for compact open subgroups of $G(\mathbb{A}_f)$, for which we refer the reader to [KY], 4.1.4. In particular, if K is neat then so is the congruence subgroup $G(\mathbb{Q}) \cap gKg^{-1}$, for any $g \in G(\mathbb{A}_f)$. Every compact open subgroup K of $G(\mathbb{A}_f)$ contains a neat compact open subgroup K' of finite index in K.

2.13 Shimura varieties

Finally, we give the definition of a Shimura variety:

Definition 2.8. *Let (G, X) be a Shimura datum and let K be a compact open subgroup of $G(\mathbb{A}_f)$. The Shimura variety attached to (G, X) and K is the double coset space*

$$\mathrm{Sh}_K(G, X)(\mathbb{C}) := G(\mathbb{Q})\backslash X \times (G(\mathbb{A}_f)/K).$$

This definition invariably seems abstruse at first. However, it is a simple calculation to see that

$$\mathrm{Sh}_K(G, X)(\mathbb{C}) = \coprod_{g \in \mathcal{C}} \Gamma'_g \backslash X,$$

where $\mathcal{C}$ is a set of representatives for the double coset space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K$ and $\Gamma'_g := G(\mathbb{Q}) \cap gKg^{-1}$ is a congruence subgroup. Note that, by [PR91], Theorem 5.1, $\mathcal{C}$ is a finite set. However, since we are interested in connected components, choose a connected component X^+ of X and denote by $G(\mathbb{Q})_+$ its stabiliser in $G(\mathbb{Q})$. Then

$$\mathrm{Sh}_K(G,X)(\mathbb{C}) = \coprod_{g\in\mathcal{C}_+} \Gamma_g\backslash X^+,$$

where $\mathcal{C}_+$ is a set of representatives for the double coset space $G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K$ and $\Gamma_g := G(\mathbb{Q})_+ \cap gKg^{-1}$. By [Mil04], Lemma 5.12, $\mathcal{C}_+$ is also a finite set.

2.14 Complex structure

Any arithmetic subgroup Γ of $G(\mathbb{Q})$ acts on X through $G^{\mathrm{ad}}(\mathbb{Q})$ and, by [Mil04], Proposition 3.2, its image is also arithmetic. For any arithmetic subgroup Γ of $G(\mathbb{Q})$, the intersection $\Gamma \cap G(\mathbb{Q})_+$ acts on X^+. We say that its image under the map $G^{\mathrm{ad}}(\mathbb{R})^+ \to \mathrm{Hol}(X^+)^+$ is an arithmetic subgroup of $\mathrm{Hol}(X^+)^+$.

If Γ is neat then the image of $\Gamma \cap G(\mathbb{Q})_+$ in $\mathrm{Hol}(X^+)^+$ is neat and, in particular, torsion free. By [Mil04], Proposition 3.1, such an arithmetic subgroup of $\mathrm{Hol}(X^+)^+$ acts freely on X^+ and the corresponding quotient has a unique complex structure such that the quotient map is a local isomorphism. In general then, $\Gamma\backslash X^+$ has the structure of a (possibly singular) complex analytic variety.

2.15 Algebraic structure

The fundamental result of Baily and Borel [BB66] states that the quotient of X^+ by any torsion free, arithmetic subgroup of $\mathrm{Hol}(X^+)^+$ has a canonical realisation as a complex quasi-projective algebraic variety. In particular, if

K is neat, $\mathrm{Sh}_K(G,X)(\mathbb{C})$ is the analytification of a quasi-projective variety $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$.

A further theorem of Borel [Bor72] states that, for any smooth quasi-projective variety V over $\mathbb{C}$, any holomorphic map from $V(\mathbb{C})$ to $\mathrm{Sh}_K(G,X)(\mathbb{C})$ is regular. For example, given any inclusion $K_1 \subset K_2$ of neat compact open subgroups of $G(\mathbb{A}_f)$, we have a natural morphism of algebraic varieties

$$\mathrm{Sh}_{K_1}(G,X)_{\mathbb{C}} \to \mathrm{Sh}_{K_2}(G,X)_{\mathbb{C}}.$$

Therefore, varying K, we get an inverse system of algebraic varieties

$$(\mathrm{Sh}_K(G,X)_{\mathbb{C}})_K$$

and we write the scheme-theoretic limit of this system as $\mathrm{Sh}(G,X)_{\mathbb{C}}$. On the system there is a natural action of $G(\mathbb{A}_f)$ given by

$$\cdot g : \mathrm{Sh}_K(G,X)(\mathbb{C}) \to \mathrm{Sh}_{g^{-1}Kg}(G,X)(\mathbb{C}) : [x,a]_K \mapsto [x,ag]_{g^{-1}Kg},$$

where we use $[\cdot,\cdot]_K$ to denote a double coset belonging to $\mathrm{Sh}_K(G,X)(\mathbb{C})$. By the theorem of Borel, this action is algebraic. Therefore, for any given $g \in G(\mathbb{A}_f)$, it induces an algebraic correspondence

$$\mathrm{Sh}_K(G,X)_{\mathbb{C}} \leftarrow \mathrm{Sh}_{K\cap gKg^{-1}}(G,X)_{\mathbb{C}} \xrightarrow{\cdot g} \mathrm{Sh}_{g^{-1}Kg\cap K}(G,X)_{\mathbb{C}} \to \mathrm{Sh}_K(G,X)_{\mathbb{C}},$$

where the outer maps are the natural projections. We refer to this correspondence as a Hecke correspondence.

Finally, if we have a morphism

$$f : (G_1, X_1) \to (G_2, X_2)$$

of Shimura data and two compact open subgroups $K_1 \subset G_1(\mathbb{A}_f)$ and $K_2 \subset G_2(\mathbb{A}_f)$ such that $f(K_1) \subset K_2$, then we obtain a morphism

$$\mathrm{Sh}_{K_1}(G_1, X_1)(\mathbb{C}) \to \mathrm{Sh}_{K_2}(G_2, X_2)(\mathbb{C}),$$

which, again by the theorem of Borel is a regular map

$$\mathrm{Sh}_{K_1}(G_1, X_1)_{\mathbb{C}} \to \mathrm{Sh}_{K_2}(G_2, X_2)_{\mathbb{C}}.$$

We refer to the images of such maps as Shimura subvarieties. We also obtain an induced morphism

$$\mathrm{Sh}(G_1, X_1)_{\mathbb{C}} \to \mathrm{Sh}(G_2, X_2)_{\mathbb{C}}$$

of the limits, by which we mean an inverse system of regular maps, compatible with the action of $G(\mathbb{A}_f)$.

2.16 Special subvarieties

Special subvarieties constitute the smallest class of irreducible algebraic subvarieties containing the connected components of Shimura subvarieties and the irreducible components of their images under Hecke correspondences. The precise definition is the following:

Definition 2.9. *Let $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ be a Shimura variety. A closed irreducible subvariety Z is called special if there exists a morphism of Shimura data*

$$(G', X') \to (G, X)$$

and $g \in G(\mathbb{A}_f)$ such that Z is an irreducible component of the image of

$$\mathrm{Sh}(G', X')_{\mathbb{C}} \to \mathrm{Sh}(G, X)_{\mathbb{C}} \xrightarrow{\cdot g} \mathrm{Sh}(G, X)_{\mathbb{C}} \to \mathrm{Sh}_K(G, X)_{\mathbb{C}}.$$

The situation is analogous to the case of Abelian varieties, where the special subvarieties are the Abelian subvarieties and their translates under torsion points.

By definition, if we let $K' \subset G(\mathbb{A}_f)$ be a compact open subgroup contained in K and consider the natural morphism of Shimura varieties

$$\pi : \mathrm{Sh}_{K'}(G, X)_{\mathbb{C}} \to \mathrm{Sh}_K(G, X)_{\mathbb{C}}$$

- If Z is a special subvariety of $\mathrm{Sh}_{K'}(G, X)_{\mathbb{C}}$, then $\pi(Z)$ is a special subvariety of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$.
- If Z is a special subvariety of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$, then any irreducible component of $\pi^{-1}Z$ is a special subvariety of $\mathrm{Sh}_{K'}(G, X)_{\mathbb{C}}$.

2.17 Special points

The natural definition of a special point is the following:

Definition 2.10. *A special point in* $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ *is a special subvariety of dimension zero.*

However, we can characterise special points in a more concrete manner: consider a special point $[h, g]_K \in \mathrm{Sh}_K(G, X)(\mathbb{C})$. Let $M := \mathrm{MT}(h)$ be the Mumford-Tate group of h i.e. the smallest algebraic subgroup H of G (defined over $\mathbb{Q}$) such that $h : \mathbb{S} \to G_{\mathbb{R}}$ factors through $H_{\mathbb{R}}$ and let X_M denote the orbit $M(\mathbb{R}) \cdot h$ inside X. Then (M, X_M) is a Shimura subdatum of (G, X) and, if we let X_M^+ be the connected component $M(\mathbb{R})^+ \cdot h$ of X_M, then the image of $X_M^+ \times \{g\}$ in $\mathrm{Sh}_K(G, X)(\mathbb{C})$ defines the smallest special subvariety containing $[h, g]_K$. Therefore, X_M must be zero dimensional and so M must be commutative. It is a general fact that any subgroup of G defined over $\mathbb{Q}$ and containing $h(\mathbb{S})$ is reductive. Therefore, M is a torus.

On the other hand if T is a torus in G and $h \in X$ factors through $T_{\mathbb{R}}$ then $[h, g]_K \in \mathrm{Sh}_K(G, X)(\mathbb{C})$ is clearly a special point for any $g \in G(\mathbb{A}_f)$. Therefore, we may define a special point as any point $[h, g]_K \in \mathrm{Sh}_K(G, X)(\mathbb{C})$ such that $\mathrm{MT}(h)$ is a torus. Of course, the choice of h is only well-defined up to conjugation by an element of $G(\mathbb{Q})$, but this doesn't affect the property of $\mathrm{MT}(h)$ being a torus.

2.18 Canonical model

Now we would like to define a model for $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ that is canonical in a sense we will make precise. As we have seen, $\mathrm{Sh}_K(G, X)(\mathbb{C})$ is often a moduli space for Abelian varieties and the main theorem of complex multiplication gives us a description of how Galois groups act on sets of CM-Abelian varieties. Therefore, we would like the Galois action on $\mathrm{Sh}_K(G, X)(\mathbb{C})$ to agree with this description, whenever it applies. In order to achieve this, the canonical model will satisfy a generalised version of this description given in terms of Deligne's group-theoretic (G, X) language.

Recall that a model over a number field E for a complex algebraic variety V is a variety V_0 defined over E with an isomorphism $\phi : V_{0,\mathbb{C}} \to V$, though we will follow convention and omit any mention of this isomorphism. First we define the field of definition $E := E(G, X)$ of the canonical model. It is referred to as the reflex field and, as we will see, it does not depend on K. This independence is one reason for having several connected components in the definition of a Shimura variety. We refer the reader to [Mil04], §12.

For a subfield k of $\mathbb{C}$, we write $\mathcal{C}(k)$ for the set of $G(k)$-conjugacy classes of cocharacters of G_k defined over k i.e.

$$\mathcal{C}(k) = G(k)\backslash \mathrm{Hom}(\mathbb{G}_{m,k}, G_k).$$

Any homomorphism $k \to k'$ induces a map $\mathcal{C}(k) \to \mathcal{C}(k')$, so $\mathrm{Aut}(k'/k)$ acts on $\mathcal{C}(k')$.

For $h \in X$, we obtain a cocharacter

$$\mu_h : \mathbb{G}_{m,\mathbb{C}} \xrightarrow{z \mapsto (z,1)} \mathbb{G}_{m,\mathbb{C}}^2 \cong \mathbb{S}_{\mathbb{C}} \xrightarrow{h_{\mathbb{C}}} G_{\mathbb{C}}$$

of $G_{\mathbb{C}}$ and so the $G(\mathbb{R})$-conjugacy class X of h maps to an element $c(X) \in \mathcal{C}(\mathbb{C})$. The reflex field E is then the fixed field of the stabiliser of $c(X)$ in $\mathrm{Aut}(\mathbb{C})$. By what follows, we will see that E is a number field.

Suppose that

$$[h, g]_K \in \mathrm{Sh}_K(G, X)(\mathbb{C})$$

is a special point i.e. $M := \mathrm{MT}(h)$ is a torus. Therefore, since all cocharacters of M are defined over $\overline{\mathbb{Q}}$ and μ_h factors through $M_{\mathbb{C}}$, μ_h is defined over a finite extension E_h of $\mathbb{Q}$. Note that E_h does not depend on the choice of h. By [Mil04], Remark 12.3 (b), E is contained in E_h.

For any $t \in M(E_h)$, the element

$$\prod_{\sigma : E_h \to \overline{\mathbb{Q}}} \sigma(t)$$

is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and so belongs to $M(\mathbb{Q})$. The so-called reciprocity morphism is defined by

$$r_h : \mathbb{A}_{E_h,f}^{*} \to M(\mathbb{A}_f) : a \mapsto \prod_{\sigma : E_h \to \overline{\mathbb{Q}}} \sigma(\mu_h(a)).$$

Finally, recall the (surjective) Artin map

$$\mathrm{Art}_{E_h} : \mathbb{A}_{E_h}^* \to \mathrm{Gal}(E_h^{\mathrm{ab}}/E_h)$$

from class field theory and let $\mathrm{Art}_{E_h}^{-1}$ denote its reciprocal.

Definition 2.11. *We say that a model of* $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ *over* E *is canonical if every special point* $[h, g]_K$ *in* $\mathrm{Sh}_K(G, X)(\mathbb{C})$ *has coordinates in* E_h^{ab} *and*

$$\sigma[h, g]_K = [h, r_h(s_f)g]_K,$$

for any $\sigma \in \mathrm{Gal}(E_h^{\mathrm{ab}}/E_h)$ *and* $s = (s_\infty, s_f) \in \mathbb{A}_{E_h}^*$ *such that* $\mathrm{Art}_{E_h}^{-1}(s) = \sigma$*.*

By [Mil04], Theorem 13.7, if a canonical model exists, it is unique up to unique isomorphism. The difficult theorem is that canonical models actually exist. For a discussion, see [Mil04], §14.

A model of $\mathrm{Sh}(G, X)_{\mathbb{C}}$ over E is an inverse system of varieties over E, endowed with a right action of $G(\mathbb{A}_f)$, which over $\mathbb{C}$ is isomorphic to $\mathrm{Sh}(G, X)_{\mathbb{C}}$ with its $G(\mathbb{A}_f)$ action. Such a system is canonical if each component is canonical in the previous sense.

By [Mil04], Theorem 13.7 (b), if for all compact open subgroups K of $G(\mathbb{A}_f)$, $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ has a canonical model, then so does $\mathrm{Sh}(G, X)_{\mathbb{C}}$ and it is unique up to unique isomorphism. In particular, by [Mil04], Theorem 13.6, the action of $G(\mathbb{A}_f)$ is defined over E. By [Mil04], Remark 13.8, if $(G', X') \to (G, X)$ is a morphism of Shimura data and $\mathrm{Sh}(G', X')_{\mathbb{C}}$ and $\mathrm{Sh}(G, X)_{\mathbb{C}}$ have canonical models, then the induced morphism

$$\mathrm{Sh}(G', X')_{\mathbb{C}} \to \mathrm{Sh}(G, X)_{\mathbb{C}}$$

is defined over $E(G', X') \cdot E(G, X)$.

3 The Pila-Zannier strategy

A connected component of a Shimura variety arises as a quotient $\Gamma\backslash D$, where D is a certain type of complex manifold called a Hermitian symmetric domain, and Γ is a certain type of discrete subgroup of $\mathrm{Hol}(D)^+$ called a congruence subgroup.

Let S denote such a component. By [KUY13], §3, there exists a semi-algebraic fundamental domain $\mathcal{F} \subset D$ for the action of Γ. By [KUY13], Theorem 1.2, when the uniformisation map

$$\pi : D \to S$$

is restricted to $\mathcal{F}$, one obtains a function definable in the o-minimal structure $\mathbb{R}_{\mathrm{an,exp}}$. From these observations, the André-Oort conjecture becomes amenable to tools from o-minimality.

The purpose of this section is to explain the so-called Pila-Zannier strategy for proving the André-Oort conjecture. This strategy first arose in a proof of the Manin-Mumford conjecture [PZ08] and was first adapted to Shimura varieties by Pila [Pil09a]. We will follow the outline given by Ullmo [Ull13] for $\mathcal{A}_6^r$, where $\mathcal{A}_g$ is the moduli space for principally polarised Abelian varieties of dimension g.

The first step is to show that, if Y is an irreducible Hodge generic subvariety of S, then the union of all positive-dimensional special subvarieties contained in Y is not Zariski dense in Y. The second step is to show that all but finitely many special points in Y lie on a positive-dimensional special subvariety contained in Y.

Both steps require the hyperbolic Ax-Lindemann-Weierstrass conjecture, a geometric statement, itself amenable to proof via o-minimality, which was first proven in the cocompact case by Ullmo and Yafaev [UY14], by Pila and Tsimerman for $\mathcal{A}_g$ [PT14], and finally by Klingler, Ullmo and Yafaev in the general case [KUY13].

Ullmo demonstrates the first step in his article [Ull13]. Therefore, we focus on the second step. The strategy will be to compare lower bounds for the size of Galois orbits of special points with upper bounds for the heights of their pre-images in the fundamental domain. One concludes by applying the Pila-Wilkie counting theorem [PW06], which states that the number of algebraic points of degree at most k and height at most T, in the complement of all connected positive-dimensional semi-algebraic subsets of a set X, definable in an o-minimal structure, is $\ll_{\epsilon,k,X} T^{\epsilon}$.

3.1 Reductions

Let (G, X) be a Shimura datum and let K be a compact open subgroup of $G(\mathbb{A}_f)$. Let Σ be a set of special points in $\mathrm{Sh}_K(G, X)(\mathbb{C})$ and let Y denote an irreducible component of the Zariski closure of $\cup_{s\in\Sigma} s$ in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$.

Let $[h, g]_K \in Y$ denote a point such that $M := \mathrm{MT}(h)$ is maximal among such groups. Note that the maximality is independent of the choice of h. We say that such a point is Hodge generic in Y. Let $X_M := M(\mathbb{R}) \cdot h$. Then, by [EY03], Proposition 2.1, Y is contained in the image of the morphisms

$$\mathrm{Sh}_{K_M}(M, X_M)_{\mathbb{C}} \to \mathrm{Sh}_{gKg^{-1}}(G, X)_{\mathbb{C}} \xrightarrow{\cdot g} \mathrm{Sh}_K(G, X)_{\mathbb{C}},$$

where $K_M := M(\mathbb{A}_f) \cap gKg^{-1}$. Denote by f their composition and let Y_M be an irreducible component of $f^{-1}Y$. Then Y is a special subvariety of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ if and only if Y_M is a special subvariety of $\mathrm{Sh}_{K_M}(M,X_M)_{\mathbb{C}}$. Furthermore, Y_M is Hodge generic in $\mathrm{Sh}_{K_M}(M,X_M)_{\mathbb{C}}$. Therefore, we may assume that Y is Hodge generic in $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$.

Let $(G^{\mathrm{ad}},X^{\mathrm{ad}})$ be the adjoint Shimura datum associated to (G,X) and let K^{ad} be a compact open subgroup of $G^{\mathrm{ad}}(\mathbb{A}_f)$ containing the image of K. Then Y is a special subvariety of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ if and only if its image Y^{ad} in $\mathrm{Sh}_{K^{\mathrm{ad}}}(G^{\mathrm{ad}},X^{\mathrm{ad}})_{\mathbb{C}}$ is a special subvariety. Furthermore, if Y is Hodge generic in $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$, then Y^{ad} is Hodge generic in $\mathrm{Sh}_{K^{\mathrm{ad}}}(G^{\mathrm{ad}},X^{\mathrm{ad}})_{\mathbb{C}}$. Therefore, we may assume that G is semisimple of adjoint type.

Recall that the irreducible components of the image of a special subvariety under a Hecke correspondence are again special subvarieties. Therefore, if we fix a connected component X^+ of X, we may assume that Y is contained in the image $S:=\Gamma\backslash X^+$ of $X^+\times\{1\}$ in $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$, where $\Gamma:=G(\mathbb{Q})_+\cap K$ and $G(\mathbb{Q})_+$ is the stabiliser of X^+ in $G(\mathbb{Q})$. We denote a point in S as $[h]$ for some $h\in X^+$.

3.2 Galois orbits

The first ingredient is a lower bound for the size of the Galois orbit of a special point. By the definition of special subvarieties, the choice of K is irrelevant in the André-Oort conjecture. Thus, we may assume that K is neat and a product of compact open subgroups K_p in $G(\mathbb{Q}_p)$.

Now let $[h]\in S$ be a special point. Recall that $M:=\mathrm{MT}(h)$ is a torus and let L denote its splitting field, by which we mean the smallest field over which M becomes isomorphic to a product of the multiplicative group. Note that this is a finite Galois extension of $\mathbb{Q}$ containing E_h and is independent of the choice of h.

Let K_M denote the compact open subgroup $M(\mathbb{A}_f)\cap K$ of $M(\mathbb{A}_f)$, which is equal to the product of the $M(\mathbb{Q}_p)\cap K_p$. Let K_M^m be the maximal compact open subgroup of $M(\mathbb{A}_f)$, which is unique since M is a torus, and equal to the product of the maximal compact open subgroups $K_{M,p}^m$ of $M(\mathbb{Q}_p)$. Note that $K_{M,p} = K_{M,p}^m$ for almost all primes p. The following is a natural generalisation of [EMO01], Problem 14, posed by Edixhoven for $\mathcal{A}_g$:

Conjecture 3.1. *There exist positive constants c_1, B_1 and μ_1 such that, for any special point $[h] \in S$,*

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/L)\cdot[h]| > c_1 B_1^{i(M)}[K_M^m : K_M]\Delta_L^{\mu_1},$$

where $i(M)$ is the number of places such that $K_{M,p} \neq K_{M,p}^m$ and Δ_L is the absolute value of the discriminant of L.

Note that, although the groups K_H^m and K_M depend on the choice of h, they are well-defined up to conjugation by an element of Γ and, hence, the index $[K_M^m : K_M]$ is well-defined. By [UYb], Théorème 6.1, this bound is known to hold under the GRH for CM fields and, by [Tsi12], Theorem 1.1, it holds unconditionally in the case of $\mathcal{A}_g$, for g at most 6.

3.3 Realisations

We refer to a point $h \in X^+$ as a pre-special point if $[h] \in S$ is a special point. The second ingredient in the Pila-Zannier strategy is an upper bound for the height of a pre-special point in a fundamental domain $\mathcal{F}$ of X^+ with respect to Γ. As opposed to the case of an Abelian variety, this is a non-trivial issue.

For a sensible notion of height, we must first choose a realisation $\mathcal{X}$ of X^+. By this we mean an analytic subset of a complex quasi-projective variety $\widetilde{\mathcal{X}}$, with a transitive holomorphic action of $G(\mathbb{R})^+$ on $\mathcal{X}$ such that, for any $x_0 \in \mathcal{X}$, the orbit map

$$G(\mathbb{R})^+ \to \mathcal{X} : g \mapsto g \cdot x_0$$

is semi-algebraic and identifies $\mathcal{X}$ with $G(\mathbb{R})^+/K_\infty$, where K_∞ is a maximal compact subgroup of $G(\mathbb{R})^+$ (recall that G is semisimple and adjoint). A morphism of realisations is then a $G(\mathbb{R})^+$-equivariant biholomorphism. By [Ull13], Lemme 2.1, any realisation has a canonical semi-algebraic structure and any morphism of realisations is semi-algebraic. Therefore, X^+ has a canonical semi-algebraic structure.

A subset $Z \subset \mathcal{X}$ is called an irreducible algebraic subvariety of $\mathcal{X}$ if Z is an irreducible component of the analytic set $\mathcal{X} \cap \widetilde{Z}$, where $\widetilde{Z}$ is an algebraic subset of $\widetilde{\mathcal{X}}$. By [Ull13], Lemme 2.1, $\mathcal{X} \cap \widetilde{Z}$ has finitely many analytic components and they are semi-algebraic. Also note that, by [KUY13], Corollary B.1, this notion is independent of our choice of $\mathcal{X}$. In particular, we have a well defined notion of an irreducible algebraic subvariety of X^+.

3.4 Heights

For the remainder of this article, we will fix as our realisation the so-called Borel embedding of X^+ in its compact dual $X^\vee$. We refer to [UY11], 3.3 for the following definitions:

For a point $h \in X^+$, let

$$\mu_h : \mathbb{G}_{m,\mathbb{C}} \xrightarrow{z \mapsto (z,1)} \mathbb{G}_{m,\mathbb{C}}^2 \cong \mathbb{S}_\mathbb{C} \xrightarrow{h_\mathbb{C}} G_\mathbb{C}$$

be the corresponding cocharacter and let M_X be the $G(\mathbb{C})$-conjugacy class of μ_h. Let V be a faithful representation of G on a finite dimensional $\mathbb{Q}$-vector space so that, for each point $h \in X^+$, we obtain a Hodge structure V_h and a Hodge filtration

$$F_h := \{\cdots \supset F_h^p \supset F_h^{p+1} \supset \cdots\},\ F_h^p := \oplus_{r \geq p} V_h^{r,s}.$$

Fix a point $h_0 \in X^+$ and let P be the parabolic subgroup of $G(\mathbb{C})$ stabilising F_{h_0}. We define $X^\vee$ to be the complex projective variety $G(\mathbb{C})/P$, which is naturally a subvariety of the flag variety $\Theta_{\mathbb{C}} := \mathrm{GL}(V_{\mathbb{C}})/Q$, where Q is the parabolic subgroup of $\mathrm{GL}(V_{\mathbb{C}})$ stabilising F_{h_0}. Therefore, we have a surjective map from M_X to $X^\vee$ sending μ_h to F_h.

The Borel embedding $X \hookrightarrow X^\vee$ is the map $h \mapsto F_h$. It is injective since, by [Mil04], §2, (18), the Hodge filtration determines the Hodge decomposition. In other words, the maximal compact subgroup K_∞ of $G(\mathbb{R})^+$ constituting the stabiliser of h_0 is equal to $G(\mathbb{R})^+ \cap P$.

However, $\Theta_{\mathbb{C}}$ has a natural model Θ over $\mathbb{Q}$ such that, for any extension L of $\mathbb{Q}$, a point of $\Theta(L)$ corresponds to a filtration defined over L. By definition, $X^\vee$ is defined over the reflex field $E := E(G, X)$ and a special point $h \in X^+$ is defined over the field of definition E_h of μ_h.

Therefore, since a pre-special point $h \in X^+$ has algebraic coordinates, we are allowed to talk about its (multiplicative) height $H(h)$, as defined in [BG06], Definition 1.5.4. The following is a natural generalisation of [PT13], Theorem 3.1, due to Tsimerman:

Conjecture 3.2. *There exist positive constants c_2, B_2, μ_2 and μ_3 such that,* *for any pre-special point $h \in \mathcal{F}$,*

$$H(h) < c_2 B_2^{i(M)} [K_M^m : K_M]^{\mu_2} \Delta_L^{\mu_3}.$$

Remark 3.3. *Let $h \in X^+$ be a pre-special point and let L be the splitting field of $M := \mathrm{MT}(h)$. The dimension d of M is at most the dimension of a maximal torus of G and the Galois action on the character group of M is given by a homomorphism*

$$\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{GL}_d(\mathbb{Z}).$$

Since, by a classical result of Minkowski, the number of isomorphism classes of finite groups contained in $\mathrm{GL}_d(\mathbb{Z})$ is finite, the degree of L (and therefore E_h) is bounded by a positive constant depending only on G.

3.5 Definability

In order to apply the Pila-Wilkie counting theorem, one requires the following theorem:

Theorem 3.4. *The restriction $\pi_{|\mathcal{F}}$ of the uniformisation map*

$$\pi : X^+ \to S$$

is definable in $\mathbb{R}_{\mathrm{an,exp}}$.

This theorem was first proved for restricted theta functions by Peterzil and Starchenko [PS13]. In particular, this addressed the case of $\mathcal{A}_g$. It is known for general Shimura varieties due to the work of Klingler, Ullmo and Yafaev [KUY13].

3.6 Ax-Lindemann-Weierstrass

The final ingredient is the hyperbolic Ax-Lindemann-Weierstrass conjecture. In order to state the conjecture, we require the notion of a weakly special subvariety:

Definition 3.5. *A variety V in S is weakly special if the (analytic) connected components of $\pi^{-1}V$ are algebraic in X^+.*

This definition is actually the characterisation [UY11], Theorem 1.2 of the original definition [UY11], Definition 2.1. However, given some familiarity with Shimura varieties, the proof is fairly straightforward and this characterisation is precisely what we need. The term weakly special is motivated by the fact that all special subvarieties are weakly special whereas, as explained in [Moo98a], weakly special subvarieties are special subvarieties if and only if they contain a special point.

Theorem 3.6. *Let Z be an algebraic subvariety of S. Maximal, irreducible, algebraic subvarieties of $\pi^{-1}Z$ are precisely the irreducible components of the preimages of maximal, weakly special subvarieties contained in Z.*

This theorem is due to Klingler, Ullmo and Yafaev [KUY13]. It was first proven for compact Shimura varieties by Ullmo and Yafaev [UY14] and for $\mathcal{A}_g$ by Pila and Tsimerman [PT14].

3.7 Pila-Wilkie

Let $A \subset \mathbb{R}^m$ be a definable set in an o-minimal structure and let A^{alg} be the union of all connected positive dimensional semi-algebraic subsets contained in A. Recall the Pila-Wilkie counting theorem, first proved for rational points in [PW06] and later for algebraic points in [Pil09b]:

Theorem 3.7. *For every $\epsilon > 0$ and $k \in \mathbb{N}$, there exists a positive constant c, depending only on A, k and ϵ, such that, for any real number $T \geq 1$, the number of points lying on $A \setminus A^{\text{alg}}$, whose coordinates in $\mathbb{R}^m$ are algebraic of degree at most k and of multiplicative height at most T, is at most cT^{ϵ}.*

In this thesis, the o-minimal structure will be $\mathbb{R}_{\text{an,exp}}$ and definable will always mean definable in $\mathbb{R}_{\text{an,exp}}$.

3.8 Final reduction

The final reduction is the following result due to Ullmo, appearing as Theorem 4.1 in [Ull13]:

Theorem 3.8. *Let Z be a Hodge generic subvariety of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$, strictly contained in S. Suppose that, if S is a product $S_1 \times S_2$ of connected components of Shimura varieties, then Z is not of the form $S_1 \times Z'$, for a subvariety Z' of S_2. Then the union of all positive-dimensional weakly special subvarieties of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ contained in Z is not Zariski dense in Z.*

We apply the theorem to Y noting that the assumption in the theorem is no loss of generality: if necessary, we simply replace S by S_2 and Y by Y'. Thus, we may assume that the union of all positive-dimensional special subvarieties of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ contained in Y is not Zariski dense in Y.

Therefore, if we are able to show that all but a finite number of special points in Y lie on a positive-dimensional special subvariety of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ contained in Y, then the theorem implies that $Y = S$.

3.9 Implementation

By Theorem 3.4, $\pi_{|\mathcal{F}}$ is definable and so

$$\widetilde{Y} := \pi^{-1}Y \cap \mathcal{F}$$

is a definable set. By assumption, Y contains a dense set of special points and so is defined over a finite extension F of E.

Consider a pre-special point $h \in \widetilde{Y}$ and let L denote the splitting field of $M := \mathrm{MT}(h)$. The Galois orbit $\mathrm{Gal}(\overline{\mathbb{Q}}/LF) \cdot [h]$ is contained in Y and, if Conjecture 3.1 holds, then

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/LF) \cdot [h]| > c_1' B_1^{i(M)} [K_M^m : K_M] \Delta_L^{\mu_1},$$

where $c_1' := c_1/[F : E]$. On the other hand, let

$$[h, m]_K \in \mathrm{Sh}_K(G, X)(\mathbb{C})$$

denote an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/LF) \cdot [h]$, where $m \in M(\mathbb{A}_f)$ is given by the explicit description of the Galois action. Since $[h, m]_K \in S$, m is equal to qk, for some $q \in G(\mathbb{Q})_+$ and $k \in K$. Denote by h' the point of $\widetilde{Y}$ such that $[h'] = [h, m]_K$. Then, up to conjugation by an element of Γ,

$$M' := \mathrm{MT}(q^{-1} \cdot h) = q^{-1} M q$$

is equal to $\mathrm{MT}(h')$ and

$$K_{M'}^m / K_{M'} = q^{-1} K_M^m q / q^{-1} M(\mathbb{A}_f) q \cap K.$$

Conjugation by q yields a bijection between this quotient and

$$K_M^m / M(\mathbb{A}_f) \cap qKq^{-1},$$

which has cardinality $[K_M^m : K_M]$ since $q = mk^{-1}$.

Hence, if Conjecture 3.2 holds, then

$$H(h') < c_2 B_2^{i(M)} [K_M^m : K_M]^{\mu_2} \Delta_L^{\mu_3}.$$

Therefore, since by Remark 3.3 all pre-special points in X^+ have algebraic co-ordinates of bounded degree, Theorem 3.7 implies that, for any $\epsilon > 0$, there exists a constant c, depending only on $\widetilde{Y}$ and ϵ, such that there are at most

$$c(B_2^{i(M)}[K_M^m : K_M]\Delta_L)^{\epsilon}$$

pre-special points on $\widetilde{Y} \setminus \widetilde{Y}^{\text{alg}}$ belonging to $\text{Gal}(\overline{\mathbb{Q}}/LF) \cdot [h]$.

Consequently, we may choose ϵ sufficiently small such that, if either $B_2^{i(M)}[K_M^m : K_M]$ or Δ_L is large enough, then there exists a point in $\text{Gal}(\overline{\mathbb{Q}}/LF)\cdot$ $[h]$ such that the corresponding point $h' \in \widetilde{Y}$ belongs to a connected positive-dimensional semi-algebraic set contained in $\widetilde{Y}$. Therefore, by [KUY13], Lemma B.2, h' belongs to an irreducible algebraic subvariety of X^+ contained in $\widetilde{Y}$ and so, by Theorem 3.6, there exists a weakly special subvariety V contained in Y such that $[h'] \in V$. Therefore, V is a special subvariety of positive dimension and $[h]$ belongs to a special subvariety contained in Y.

Therefore, on Y, in the complement of all positive-dimensional special subvarieties contained in Y, the quantities $B_2^{i(M)}[K_M^m : K_M]$ and Δ_L corresponding to special points are bounded. By [UYa], Proposition 3.21, the set of tori equal to the Mumford-Tate group of a pre-special point such that $[K_M^m : K_M]$ and Δ_L are bounded lie in only finitely many Γ-conjugacy classes. In particular, such pre-special points lie above only finitely many points in S.

4 Hilbert modular surfaces

The purpose of this section is to prove the following special case of the André-Oort conjecture via the Pila-Zannier strategy. This represents joint work with Andrei Yafaev. For background on Hilbert modular surfaces we refer to [Edi01] and [vdG87].

Theorem 4.1. *Let S be a Hilbert modular surface and let $C \subset S$ be an irreducible algebraic curve containing an infinite set of special points. Then C is a special subvariety of S.*

Let F be a real quadratic field, $\mathcal{O}_F$ its ring of integers and $\Gamma := \mathrm{SL}_2(\mathcal{O}_F)$. By a Hilbert modular surface we mean $S := \Gamma\backslash\mathbb{H}^2$. This is a connected component of the Shimura variety $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ defined by the Shimura datum $(G,X) := (\mathrm{Res}_{F/\mathbb{Q}}\mathrm{GL}_{2,F}, \mathbb{H}^{\pm 2})$ and $K = \mathrm{GL}_2(\hat{\mathcal{O}}_F)$. One can also consider quotients of $\mathbb{H}\times\mathbb{H}$ by other congruence subgroups of $\mathrm{SL}_2(\mathcal{O}_F)$. However, the André-Oort conjecture for such quotients is equivalent to the one for S. Furthermore, since a subvariety is special if and only if irreducible components of its images by Hecke correspondences are special, the statement holds for a curve contained in any component of $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$.

The Shimura variety $\mathrm{Sh}_K(G,X)_{\mathbb{C}}$ is a coarse moduli space for pairs (A,i) where A is an Abelian surface and $i\colon \mathcal{O}_F \to \mathrm{End}(A)$ is a homomorphism. It admits a canonical model over $\mathbb{Q}$ and S is defined over a certain explicit Abelian extension. Let $\pi\colon \mathbb{H}^2 \longrightarrow S$ be the uniformisation map. We choose a certain fundamental set $\mathcal{F} \subset \mathbb{H}^2$ (actually a certain part thereof) for the action of Γ.

Let C be a curve in S containing an infinite set of special points. In particular, C is defined over a number field. We let $\mathcal{Z} := \pi^{-1}C \cap \mathcal{F}$ and we denote by $\mathcal{Z}^{alg}$ the algebraic part of $\mathcal{Z}$ i.e. the union of all connected positive-dimensional semi-algebraic subsets contained in $\mathcal{Z}$, where $\mathbb{H} \times \mathbb{H}$ is viewed as a subset of $\mathbb{R}^4$.

Suppose that C is not special. The theorem of Peterzil and Starchenko [PS13] shows that $\mathcal{Z}$ is definable in the o-minimal structure $\mathbb{R}_{\mathrm{an,exp}}$ whereas, as explained in Section 4.2, $\mathcal{Z}^{alg}$ contains no pre-special points. Therefore, by the Pila-Wilkie counting theorem, the number of pre-special points on $\mathcal{Z}$ up to a height T is $\ll_\epsilon T^\epsilon$ for any $\epsilon > 0$.

For a special point x of S, we let (A_x, i_x) be the corresponding pair as above. The ring $\mathrm{End}_{\mathcal{O}_F}(A_x)$ of endomorphisms commuting with the action of $\mathcal{O}_F$ is an order in a totally imaginary quadratic extension of F. We let $d_x := |\mathrm{disc}(\mathrm{End}_{\mathcal{O}_F}(A_x))|$. In Section 4.1 we show that the height of a pre-special point in $\mathcal{F}$ is bounded by a power of its discriminant. Hence, Pila-Wilkie implies that the size of the Galois orbit of the special point x is $\ll_\epsilon d_x^\epsilon$ where $\epsilon > 0$ can be chosen arbitrary small. This contradicts a result of Edixhoven who showed that the size of the Galois orbit is $\gg d_x^{1/8}$. It seems very likely that the methods of this section generalise to the mixed case i.e. the analogue of the André-Oort conjecture for the universal Abelian scheme over a Hilbert modular surface. To generalise the result to the case of Hilbert modular varieties of higher dimension, one needs unconditional lower bounds for the Galois orbits of special points in terms of a positive power of the discriminant.

4.1 Bounds on the heights of special points

In this section, we give upper bounds on the heights of coordinates of pre-special points contained in a certain fundamental set in terms of their discriminant. For an element α of F, we denote by α' the image of α by the non-trivial automorphism of F. Recall, a point $z = (z_1, z_2)$ of $\mathbb{H}^2$ is called pre-special if $\pi(z)$ is a special point of S.

Let $z = (z_1, z_2)$ be a pre-special point in $\mathbb{H}^2$. Then z is fixed by a certain semisimple element of $\mathrm{SL}_2(F)$. From this it immediately follows that z_1 satisfies an equation $az_1^2 + bz_1 + c = 0$ with $a, b, c \in \mathcal{O}_F$ and z_2 satisfies $a'z_2^2 + b'z_2 + c' = 0$. The field $K = F(z_1)$ is an imaginary quadratic extension of F.

We follow [vdGU82], Section 1.1. Consider the embedding $\mathcal{L}_z \colon F \times F \longrightarrow \mathbb{C}^2$ sending (α, β) to $(\alpha z_1 + \beta, \alpha' z_2 + \beta')$ and giving rise to the complex torus

$$A_z = \mathbb{C}^2 / \mathcal{L}_z(\mathcal{O}_F \oplus \mathcal{I}),$$

where $\mathcal{I}$ is an invertible rank one $\mathcal{O}_F$-module contained in $\mathcal{O}_F^\vee$, the $\mathbb{Z}$-dual of $\mathcal{O}_F$ with respect to the trace. The action of $\mathcal{O}_F$ on A_z is given by $m(a) \colon (\zeta_1, \zeta_2) \longrightarrow (a\zeta_1, a'\zeta_2)$. In [vdGU82], Section 1.1, it is shown that A_z is a polarised Abelian variety. By [vdG87], Section I.7, Corollary 7.3, the Abelian variety corresponding to a point x of S is $A_z = \mathbb{C}^2/\mathcal{L}_z(\mathcal{O}_F \oplus \mathcal{O}_F)$, where $z \in \pi^{-1}(x)$. Denoting $\Lambda_z := \mathcal{L}_z(\mathcal{O}_F \oplus \mathcal{O}_F)$, we have

$$\mathrm{End}_{\mathcal{O}_F}(A_z) = \{k \in K : k\Lambda_z \subset \Lambda_z\}$$

The ring $\mathrm{End}_{\mathcal{O}_F}(A_z)$ is an order in K containing $\mathcal{O}_F$.

Lemma 4.2. *The relative discriminant ideal*

$$\mathrm{disc}_{K/F}(\mathrm{End}_{\mathcal{O}_F}(A_z))$$

is generated by the $b^2 - 4ac$ *(with* $a, b, c \in \mathcal{O}_F$*) such that* $az_1^2 + bz_1 + c = 0$.

Proof. Let R be $\mathrm{End}_{\mathcal{O}_F}(A_z)$ and let I be the ideal in $\mathcal{O}_F$ generated by the b^2-4ac (with $a, b, c \in \mathcal{O}_F$) such that $az_1^2+bz_1+c = 0$. For any such equation, R contains az_1 and hence $\mathrm{disc}_{K/F}(R)$ contains I.

To prove the other inclusion, fix a prime ideal P of $\mathcal{O}_F$ and let $\mathcal{O}_{F_P}$ be the completion of $\mathcal{O}_F$ at P. We let M be a maximal ideal of $\mathcal{O}_K$ above P and K_M the completion of K with respect to the corresponding valuation. Let $az_1^2 + bz_1 + c = 0$ be an equation satisfied by z_1 with $v_P(abc)$ minimal where v_P denotes the P-adic valuation. It follows, in particular, that a, b and c are relatively prime in the ring $\mathcal{O}_{F_P}$. Then, the proof of [Cox89], Lemma 7.5 goes through and shows that the local order

$$\{k \in K_M : k(\Lambda_z \otimes \mathcal{O}_{F_P}) \subset \Lambda_z \otimes \mathcal{O}_{F_P}\}$$

is $\mathcal{O}_{F_P}[az_1]$. It follows that $\mathrm{disc}_{K/F}(R)O_{F_P}$ is generated by $b^2 - 4ac$ and is therefore contained in $I\mathcal{O}_{F_P}$. As this holds for all primes P, we conclude that $\mathrm{disc}_{K/F}(R) = I$ □

We write $z_i = x_i + iy_i$ and we redefine

$$H(z) := \max(H(x_1), H(x_2), H(y_1), H(y_2)).$$

Our aim is to give an upper bound for $H(z)$ in terms of a power of $d_z :=$ $|\mathrm{disc}(\mathrm{End}_{O_F}(A_z))|$, whenever z is in a fundamental set for Γ. Therefore, choose an equation $az_1^2 + bz_1 + c = 0$ where a, b, c are such that the norm $|N_{F/\mathbb{Q}}(b^2 - 4ac)|$ is minimal. The above discussion shows that

$$|N_{F/\mathbb{Q}}(\mathrm{disc}_{K/F}(\mathrm{End}_{O_F}(A_z)))| = |N_{F/\mathbb{Q}}(b^2 - 4ac)|.$$

In [Fre90], Chapter I, Proposition 2.11, it is proved that there exists a fundamental set (by which we are referring to a set containing a fundamental domain) for the action of $\Gamma = \mathrm{SL}_2(\mathcal{O}_F)$ of the form

$$\mathcal{K} \cup V_1 \cup \cdots \cup V_h,$$

where h is the class number of F, $\mathcal{K}$ is compact and the V_i are the so-called cusp sectors. Here V_1 is the cusp sector at infinity ∞. By definition, there is a constant $C > 0$ and $T > 0$ such that

$$V_1 = \{(z_1, z_2) \in \mathbb{H} \times \mathbb{H} : y_1 y_2 > C, |x_1| \leq T, |x_2| \leq T\}$$

Noticing that, on $\mathcal{K}$, y_i is bounded below and $|x_i|$ is bounded, we may and do (after possibly altering C and T), assume that $\mathcal{K} \subset V_1$. Furthermore, for $\epsilon \in \mathcal{O}_F^*$, the transformation $(z_1, z_2) \mapsto (\epsilon^2 z_1, \epsilon^{-2} z_2)$ is in Γ. We can therefore assume that (y_1, y_2) is in the fundamental set for the action $(y_1, y_2) \mapsto (\epsilon^2 y_1, \epsilon^{-2} y_2)$. We therefore have the inequalities

$$A^{-1} \leq \frac{y_i^2}{y_1 y_2} \leq A,$$

where A is a constant depending only on F. For reasons explained in Section 4.4, it is enough to consider the pre-special points in $\mathcal{K} \cup V_1$. Therefore, we consider pre-special points in the set

$$\mathcal{F} := \{(z_1, z_2) \in \mathbb{H}^2 : y_1 y_2 > C, A^{-1} \leq \frac{y_i^2}{y_1 y_2} \leq A, |x_1| \leq T, |x_2| \leq T\}.$$

Theorem 4.3. *There exists a real $c_1 > 0$ such that for any pre-special point $z = (z_1, z_2) \in \mathcal{F}$ we have,*

$$H(z) \leq c_1 {d_z}^{1/2}.$$

Remark 4.4. *The proof below generalises to the case of Hilbert modular varieties of arbitrary dimension.*

Proof. Let $D_1 = |b^2 - 4ac|$ and $D_2 = |b'^2 - 4a'c'|$. Therefore, we have

$$|N_{F/\mathbb{Q}}(\mathrm{disc}_{K/F}(\mathrm{End}_{O_F}(A_z)))| = D_1 D_2$$

and $d_z = D_1 D_2 \Delta_F^2$, where $\Delta_F = |\mathrm{disc}(O_F)|$.

Note that we have

$$|b| = 2|a||x_1| \leq 2T|a|, \ |b'| = 2|a'||x_2| \leq 2T|a'|.$$

Secondly, since $D_1 = 4a^2 y_1^2$ and $D_2 = 4a'^2 y_2^2$, we have

$$|a| \leq \sqrt{\frac{D_1}{4U}}, \ |a'| \leq \sqrt{\frac{D_2}{4U}},$$

where $U := A^{-1}C$.

We calculate the heights using [BG06], 1.6.5 and 1.6.6. We first examine the degree two case. If $|x_1| \geq 1$,

$$H(x_1) = |2a\frac{b}{2a}| = |b| \leq 2T|a| \leq \frac{T}{\sqrt{U}}\sqrt{D_1},$$

otherwise

$$H(x_1) = |2a| \leq \frac{1}{\sqrt{U}}\sqrt{D_1}.$$

If $|y_1| \geq 1$,

$$H(y_1)^2 \leq 4a^2 \frac{D_1}{4a^2} = D_1,$$

whereas, if $|y_1| < 1$,

$$H(y_1)^2 \leq 4a^2 \leq \frac{D_1}{U}.$$

The arguments for z_2 proceed identically.

Next we examine the degree four case, where we use the fact that if we have a minimal polynomial f over O_F, the minimal polynomial over $\mathbb{Z}$ will be the product of f and σf, where σ acts on the coefficients of f.

We have

$$H(x_1)^2 \leq |4aa' \frac{bb'}{4aa'}| = |bb'| \leq 4T^2|aa'| \leq T^2 \frac{\sqrt{D_1 D_2}}{U},$$

or

$$H(x_1)^2 \leq |4aa'| \leq \frac{\sqrt{D_1 D_2}}{U}.$$

Finally,

$$H(y_1)^4 \leq 16a^2a'^2 \leq \frac{D_1 D_2}{U^2},$$

or

$$H(y_1)^4 \leq 16a^2a'^2 \frac{D_1}{4a^2} = 4a'^2 D_1 \leq \frac{D_1 D_2}{U},$$

or

$$H(y_1)^4 \leq 16a^2a'^2 \frac{D_2}{4a'^2} = 4a^2 D_2 \leq \frac{D_1 D_2}{U},$$

or

$$H(y_1)^4 =\leq 16a^2a'^2\frac{D_1D_2}{16a^2a'^2} = D_1D_2.$$

The arguments for z_2 proceed identically.

□

4.2 Characterisation of special subvarieties

Let C be an irreducible algebraic curve in S and let $\mathcal{Z} := \pi^{-1}C$. Let (z_1, z_2) be a point of $\mathbb{H}^2$. Writing $z_1 = x + iy$ and $z_2 = u + iv$, we can view $\mathbb{H}^2$ as a subset of $\mathbb{R}^4$. A semi-algebraic subset of $\mathbb{H}^2 \subset \mathbb{R}^4$ is, by definition, the intersection of a semi-algebraic subset of $\mathbb{R}^4$ with $\mathbb{H}^2$. Following Pila, we define $\mathcal{Z}^{alg}$ to be the union of all connected positive-dimensional semi-algebraic subsets of $\mathcal{Z}$. We also define $\mathcal{Z}^{ca}$ to be the union of all connected components Y of $W \cap \mathbb{H}^2$ such that Y is contained in $\mathcal{Z}$, for any positive-dimensional irreducible complex algebraic subset W contained in $\mathbb{C}^2$. The argument of the proof of [Pil09a], Proposition 2.2 shows that

$$\mathcal{Z}^{alg} = \mathcal{Z}^{ca}.$$

Theorem 4.5. *If C is not special then $\mathcal{Z}^{alg}$ contains no special points.*

Proof. We consider $\mathcal{Z}^{ca} = \mathcal{Z}^{alg}$ instead. Suppose that $\mathcal{Z}^{ca}$ is not empty (otherwise there is nothing to prove). Let $\mathcal{Z}'$ be an analytic component of $\mathcal{Z}^{ca}$. As the dimension of $\mathcal{Z}$ is one, $\pi(\mathcal{Z}') = \pi(\mathcal{Z}) = C$. In particular $\pi(\mathcal{Z}')$ is an algebraic subvariety of S. By [UY11], Theorem 1.2, $\pi(\mathcal{Z}') = C$ is a weakly special subvariety of S. By [Moo98a], Theorem 4.3, a weakly special subvariety (or totally geodesic in Moonen's terminology) of a Shimura variety is special (or Hodge type) if and only if it contains a special point. Therefore, $\mathcal{Z}$ and, hence, $\mathcal{Z}^{alg}$ contains no pre-special points. $\square$

4.3 Definability

We refer to Section 3 of [Pil09a] and references contained therein for notions of o-minimal structures and definability. We just mention here that an o-minimal structure (over $\mathbb{R}$) is a sequence, over $n \in \mathbb{N}$, of collections of subsets of $\mathbb{R}^n$ which contain all semi-algebraic subsets, stable under the natural set-theoretic operations and satisfying certain geometric finiteness properties.

In what follows we consider the o-minimal structure $\mathbb{R}_{an,exp}$ which is generated by $\mathbb{R}_{an}$ and $\mathbb{R}_{exp}$. Here $\mathbb{R}_{an}$ is the structure afforded by the so-called globally subanalytic sets and $\mathbb{R}_{exp}$ is the structure consisting of the sets defined by the exponential. In this thesis, we use definable to mean definable in $\mathbb{R}_{an,exp}$. A function from $A \subset \mathbb{R}^n$ to $B \subset \mathbb{R}^m$ is said to be definable if its graph in $A \times B \subset \mathbb{R}^{n+m}$ is definable.

We will use the theorem of Peterzil-Starchenko [PS13], which we now describe in greater detail. We follow [PS13], Section 6.3. Let Sp_{2g} be the algebraic group (over $\mathbb{Q}$) of symplectic $2g \times 2g$ matrices with determinant one. The group $\mathrm{Sp}_{2g}(\mathbb{Z})$ acts on the Siegel upper half-space $\mathbb{H}_g$. There exists a semi-algebraic subset $\mathcal{F}_g \subset \mathbb{H}_g$, which contains finitely many representatives for each orbit of $\mathrm{Sp}_{2g}(\mathbb{Z})$ (hence $\mathcal{F}_g$ contains a fundamental domain). For $a, b \in \mathbb{R}^g$, let $\vartheta_{(a,b)}(z, \tau)$ be the corresponding theta function, where $\tau \in \mathbb{H}_g$ and z is in the fundamental domain of $\mathbb{C}^g$ with respect to the lattice defined by τ. A special case of the result of Peterzil and Starchenko (Theorem 6.5 of [PS13]) is the following:

Theorem 4.6. *For all $a, b \in \mathbb{R}^g$, $\vartheta_{a,b}(0,\tau)$ restricted to $\mathcal{F}_g$ is definable.*

As in the previous section, for a subset $\mathcal{Z} \subset \mathbb{R}^n$, the algebraic part $\mathcal{Z}^{alg}$ is defined as the union of all connected positive-dimensional semi-algebraic subsets of $\mathcal{Z}$. Following Pila, for $k \in \mathbb{N}$ and $T \geq 1$, we also denote

$$Z(k,T) := \{x = (x_1, ..., x_n) \in \mathcal{Z} : [\mathbb{Q}(x_i) : \mathbb{Q}] \leq k, \max_i H(x_i) \leq T\}$$

and $N_k(\mathcal{Z}, T) := |Z(k,T)|$. Therefore, the Pila-Wilkie counting theorem becomes the following:

Theorem 4.7. *Let $\mathcal{Z} \subset \mathbb{R}^n$ be a set definable in an o-minimal structure over $\mathbb{R}$, let $k \in \mathbb{N}$ and let $\epsilon > 0$. There exists $c(\mathcal{Z}, k, \epsilon)$ such that*

$$N_k(\mathcal{Z} \backslash \mathcal{Z}^{alg}, T) \leq c(\mathcal{Z}, k, \epsilon) T^{\epsilon}.$$

The consequence of these results is the following:

Theorem 4.8. *Let C be an irreducible algebraic curve contained in S. Let $\mathcal{F}$ be the set defined in Section 4.1 and suppose that $\mathcal{Z} := \pi^{-1}C \cap \mathcal{F}$ is positive dimensional. Then, for $k \in \mathbb{N}$ and $\epsilon > 0$, there exists $c(\mathcal{Z}, k, \epsilon)$ such that*

$$N_k(\mathcal{Z} \backslash \mathcal{Z}^{alg}, T) \leq c(\mathcal{Z}, k, \epsilon) T^{\epsilon}.$$

Proof. Let

$$S = \Gamma \backslash \mathbb{H}^2 \longrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathbb{H}_2$$

be the modular embedding (see [vdG87], Chapter IX, §1). This embedding is induced by an equivariant embedding $\phi \colon \mathbb{H}^2 \longrightarrow \mathbb{H}_2$. After, if necessary, replacing the set $\mathcal{F}_g$ by a finite union of its translations by some $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$

(this does not affect the conclusion of the Peterzil-Starchenko theorem), we assume that $\phi(\mathcal{F}) \subset \mathcal{F}_g$. The set $\mathcal{F}$ is definable since it is semi-algebraic.

The functions $\vartheta_{a,b}(0,\tau)$ restricted to $\mathbb{H}^2$ induce a Γ-equivariant holomorphic embedding of S into $\mathbb{P}^N(\mathbb{C})$ for some $N \in \mathbb{N}$. As C is an algebraic curve, its image in $\mathbb{P}^N(\mathbb{C})$ is given by a collection of polynomial equations in the $\vartheta_{(a,b)}(0,\tau)$ restricted to $\phi(\mathcal{F})$. It follows from the theorem of Peterzil and Starchenko that the set $\mathcal{Z}$ is definable. The conclusion now follows from the Pila-Wilkie counting theorem. □

4.4 Proof of the main result

Let C be a curve in S containing an infinite set Σ of special points. Suppose that the closure of C in the Baily-Borel compactification $\overline{S}$ of S contains a cusp P. After, if necessary, replacing C by a component of its image under a suitable Hecke correspondence (which does not affect the property of C being special), we assume that $P = \infty$.

Let $\mathcal{F}$ be the subset of $\mathbb{H} \times \mathbb{H}$ as in Section 4.1. Our assumption that $P = \infty$ implies that, after possibly replacing Σ by an infinite subset, the preimages of the points in Σ lie in $\mathcal{F}$.

Suppose that C is not special. Let $\mathcal{Z}^{alg}$ be the algebraic part (as defined in Section 4.2) of $\mathcal{Z} := \mathcal{F} \cap \pi^{-1}C$. Then $\mathcal{Z}^{alg}$ contains no pre-special points of $\mathbb{H} \times \mathbb{H}$ by Theorem 4.5.

Let z be a point in $\mathcal{F}$ such that $x := \pi(z) \in \Sigma$. We write d_x for the discriminant d_z and A_x for the isomorphism class of the Abelian variety A_z as in Section 4.1. Note that d_x and A_x depend only on x and not on the choice of z.

As special points are $\overline{\mathbb{Q}}$-valued, C is defined over $\overline{\mathbb{Q}}$ and we can choose a number field L such that C is defined and geometrically irreducible over L Hence for all $x \in \Sigma$, $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \cdot x$ is contained in C.

Let x be a point in Σ. By [Edi01], Theorem 6.2,

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/L) \cdot x| \geq c_2 d_x^{1/8},$$

for some absolute constant $c_2 > 0$. Furthermore, as the points of $\mathrm{Gal}(\overline{\mathbb{Q}}/L) \cdot x$ have the same discriminant d_x, for any $z \in \mathcal{Z}$ such that $\pi(z) \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) \cdot x$, we have

$$H(z) \leq c_1 d_x^{1/2},$$

by Theorem 4.3. On the other hand, consider the number of pre-special points on $\mathcal{Z}$ whose coordinates in $\mathbb{R}^4$ have height at most $c_1 d_x^{1/2}$. This is bounded above by $N_4(\mathcal{Z} \backslash \mathcal{Z}^{alg}, c_1 d_x^{1/2})$, which by Theorem 4.8 is at most $c_\epsilon c_1^\epsilon d_x^{\epsilon/2}$ for any $\epsilon > 0$, where c_ϵ depends only on $\mathcal{Z}$ and ϵ. It follows that

$$d_x^{\frac{2\epsilon-1}{8}} \leq \frac{c_\epsilon c_1^\epsilon}{c_2}$$

Notice, however, that d_x must tend to infinity as x ranges through Σ: indeed there are only finitely many orders of degree two over $\mathcal{O}_F$ with a given discriminant and for such an order R there are only finitely many special points x such that $\mathrm{End}_{\mathcal{O}_F}(A_x) = R$.

Therefore, choose any $0 < \epsilon < \frac{1}{2}$. Then the left hand side of the previous inequality goes to infinity as x ranges through Σ while the right hand side remains bounded, which is a contradiction. We conclude that C is a special subvariety.

5 Torsion in class groups of CM tori

Let T be an algebraic torus over $\mathbb{Q}$ such that $T(\mathbb{R})$ is compact. In this section, we give a lower bound under the GRH for the size of the class group of T modulo its n-torsion in terms of a small power of the discriminant of the splitting field of T. As a corollary, we obtain an upper bound on the n-torsion in that class group, generalising known results on the structure of class groups of CM fields.

This work is partly motivated by Zhang's "ϵ-conjecture" [Zha05], proposing that the size of n-torsion in the class groups of CM fields of fixed degree grows slower than any positive power of the discriminant:

Conjecture 5.1. *Fix a totally real number field F, a positive integer n and a positive number ϵ. Then, for any quadratic CM-extension L, and any order $\mathcal{O}$ of L containing the ring of integers of F, the n-torsion of the class group of $\mathcal{O}$ has the following bound:*

$$\#\mathrm{Pic}(\mathcal{O})[n] \leq C(\epsilon)\mathrm{disc}(\mathcal{O})^{\epsilon},$$

where $C(\epsilon)$ is a positive constant depending only on ϵ.

Recent results on torsion in the class groups of number fields, due to Ellenberg and Venkatesh, can be found in [EV07].

By CM tori we refer to the Mumford-Tate groups of pre-special points. Understanding n-torsion in the class groups of CM tori arises as a natural problem in not only the Pila-Zannier strategy for proving the André-Oort conjecture, but also in the methods of Klingler, Ullmo and Yafaev.

As we have seen, the Galois action on special points of Shimura varieties is given by the so-called reciprocity morphisms of CM tori. To give a lower bound for the size of Galois orbits, one needs to bound from below the size of the images of the induced maps on class groups. Lower bounds for the size of class groups modulo n-torsion yield estimates on these quantities (see [Tsi12] and [UYb] for further details). Our results are primarily of this form.

Note that the Mumford-Tate group of a pre-special point is an algebraic torus over $\mathbb{Q}$ whose real points are compact. Its splitting field is a CM field.

Let $\mathbb{A}_f$ denote the finite adèles over $\mathbb{Q}$. For an arbitrary algebraic torus M over $\mathbb{Q}$, we denote by K_M^m the maximal compact open subgroup of $M(\mathbb{A}_f)$. For any such torus we denote by h_M its class group i.e.

$$h_M = M(\mathbb{Q})\backslash M(\mathbb{A}_f)/K_M^m.$$

Given any $n \in \mathbb{N}$ we denote by $h_M[n]$ the n-torsion. For an arbitrary number field F, we denote by Δ_F the absolute value of the discriminant of F. We obtain the following bound:

Theorem 5.2. *Assume the GRH for CM fields. Let T be an algebraic torus over $\mathbb{Q}$ of dimension d such that $T(\mathbb{R})$ is compact and denote by L its splitting field. Then*

$$|h_T/h_T[n]| \gg_{\epsilon,d} \Delta_L^{\frac{c}{2n}+\epsilon},$$

for all $\epsilon > 0$, where c is a positive constant depending only on d.

By its splitting field we refer to the smallest field over which T becomes isomorphic to a product of copies of $\mathbb{G}_m$. Our method relies on the fact that T is isogenous to a product $T_1 \times \cdots \times T_s$ of simple tori. We fix surjective maps with connected kernels from $R := \mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_{m,L}$ to each of the T_i and take r to be their product composed with an isogeny to T. For a prime p

splitting in L, $R(\mathbb{Q}_p)$ is isomorphic to the cocharacter group of R tensored with $\mathbb{Q}_p^*$. We use the GRH to find 'small' split primes and take an arbitrary product of powers of uniformisers lying over these primes. We embed this element in $R^s(\mathbb{A}_f)$ and assume that it lies in the kernel of the map induced by r on class groups i.e. the image under r is an element $\pi k \in T(\mathbb{Q})K_T^m$. The element π gives us elements π_i in the $T_i(\mathbb{Q})$ and we show that L is generated over $\mathbb{Q}$ by the images of the π_i under a set of characters forming a basis for the character groups of the T_i. Scaling by the previous primes p raised to the absolute values of the aforementioned exponents, we may assume that the images of the π_i belong to $\mathcal{O}_L$. Hence, we may take a basis for L over $\mathbb{Q}$ in terms of these elements, whose $\mathbb{Z}$-span is an order in $\mathcal{O}_L$, yielding a relation between Δ_L and their absolute values. However, these absolute values are controlled by the primes found under the GRH, a uniform bound on the coordinates of characters, and the exponents. Since these primes are 'small' compared to Δ_L, we are able to bound the exponents from below. A group theoretic argument converts this into a lower bound for the size of the class group modulo n-torsion.

Our method relies crucially on the assumption that $T(\mathbb{R})$ is compact. However, note that, while the class group of a CM field L is the class group of the torus $R_L := \mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_m$ whose real points are not compact, this torus lies in an exact sequence

$$1 \to M \to R_L \to \mathbb{G}_m \to 1,$$

where M is a torus over $\mathbb{Q}$ whose real points are compact (its $\mathbb{Q}$-points are precisely the elements of L of norm 1). This exact sequence of tori induces a morphism of class groups

$$h_M \to h_{R_L}$$

whose kernel, by the proof of [Tsi12], Theorem 5.1, has order r bounded in terms of d only. It follows that the kernel of the map

$$h_M \to h_{R_L}/h_{R_L}[n]$$

is contained in $h_M[nr]$ and so the statement of Theorem 5.2 also applies to CM fields and, indeed, to the extension of any torus by one as in the statement of Theorem 5.2.

5.1 Corollary on n-torsion.

Before proceeding to the proof of Theorem 5.2 we obtain an upper bound on the size of n-torsion. All that is required is a simple upper bound on the class group of T. We have the following theorem.

Theorem 5.3. *Let T be an algebraic torus over $\mathbb{Q}$ with dimension d and splitting field L. Then, for all $\epsilon > 0$,*

$$|h_T| \ll_{\epsilon,d} \Delta_L^{\frac{s}{2}+\epsilon},$$

where s is the number of simple subtori of T.

Proof. The statement of [PR91], Proposition 2.1 is that T lies in an exact sequence

$$1 \to T \to R_L^s \to M \to 1,$$

where M is a $\mathbb{Q}$-torus. As before, the proof of [Tsi12], Theorem 5.1. explains that the induced map on class groups

$$h_T \to h_{R^s}$$

has kernel of size bounded in terms of d only. Note that the class group h_{R^s} is simply the s-fold direct product of the class group $Cl(L)$ of L. By [DKM10], (1), we have

$$|Cl(L)| \ll_{\epsilon, n_L} \Delta_L^{\frac{1}{2}+\epsilon},$$

where n_L is the degree of L over $\mathbb{Q}$. □

The combination of Theorems 5.3 and 5.2 yield the following bound on the size of n-torsion in the class group:

Theorem 5.4. *Assume the GRH for CM fields. Let T be an algebraic torus over $\mathbb{Q}$ of dimension d with splitting field L such that $T(\mathbb{R})$ is compact. Then, for all $\epsilon > 0$,*

$$|h_T[n]| \ll_{\epsilon, d} \Delta_L^{\frac{s}{2}-\frac{c}{2n}+\epsilon},$$

where c is a positive constant depending only on d and s is the number of simple subtori of T.

5.2 A group theoretic argument.

The proof of Theorem 5.2 will combine ideas of the two papers [AD03] and [Yaf06]. Following [AD03], for an arbitrary Abelian group G and $l \in \mathbb{N}$, let $\mathcal{M}_G(l)$ be the smallest integer A such that, for any l elements $g_1, ..., g_l \in$

G, not necessarily distinct, there exist $a_1, ..., a_l \in \mathbb{Z}$, not all zero, with $\sum_{i=1}^{l} |a_i| \leq A$, such that

$$g_1^{a_1} \cdots g_l^{a_l} = 1.$$

In what follows we will demonstrate that

$$\mathcal{M}_{h_T}(l) > \frac{c \log \Delta_L}{\log(l) + \log\log \Delta_L}, \tag{1}$$

for any $l \in \mathbb{N}$, provided Δ_L is greater than a constant depending only on d. Here we prove that inequality (1) implies Theorem 5.2.

Proof. We follow the proof of [AD03], Lemma 5.1. Let G be a finite Abelian group, set $l = |G|$, and take $g_1, ..., g_l \in G$. If $g_i = 1$ for some $i \in \{1, ..., l\}$, then we clearly have a non-trivial relation between the g_i and $A = 1$, A defined as above. Otherwise, an element of G appears twice amongst our g_i and there exist i and j such that $i \neq j$ and $g_i g_j^{-1} = 1$. Either way, we have a non-trivial relation with $A \leq 2$. Hence, we have shown that

$$\mathcal{M}_G(|G|) \leq 2.$$

Henceforth, let $G = h_T/h_T[n]$. Then, by [AD03], Lemma 5.1. (iii), we have

$$\mathcal{M}_{h_T}(|G|) \leq n\mathcal{M}_G(|G|)$$

and, therefore, by the preceding argument,

$$\mathcal{M}_{h_T}(|G|) \leq 2n.$$

Substituting $\mathcal{M}_{h_T}(|G|)$ into (1), we obtain the desired result

$$l = |h_T/h_T[n]| > \frac{\Delta_L^{\frac{c}{2n}}}{\log \Delta_L},$$

provided $\Delta_L > 2$. □

The remainder of this section is devoted to the proof of (1).

5.3 Covering T.

For an arbitrary algebraic torus M over $\mathbb{Q}$, we denote by $X^*(M)$ its character group i.e. the free $\mathbb{Z}$-module $\mathrm{Hom}(M_{\overline{\mathbb{Q}}}, \mathbb{G}_{m,\overline{\mathbb{Q}}})$ with the natural Galois action. The corresponding representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(X^*(M)),$$

has kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ for some finite Galois extension F, which we refer to as the splitting field of M.

We denote by $X_*(M)$ the group of cocharacters of M, by which we refer to the $\mathbb{Z}$-module $\mathrm{Hom}(\mathbb{G}_{m,\overline{\mathbb{Q}}}, M_{\overline{\mathbb{Q}}})$, again assuming the natural $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, also factoring through $\mathrm{Gal}(F/\mathbb{Q})$. There is a natural bilinear map

$$X_*(M) \times X^*(M) \to \mathbb{Z},$$

identifying $X_*(M)$ with the dual $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$-module of $X^*(M)$.

Recall that we have a semisimple category whose objects are algebraic tori and whose morphisms are the usual homomorphisms of algebraic tori (which form an Abelian group) tensored with $\mathbb{Q}$. Therefore, T is isogenous to a product of tori $T_1 \times \cdots \times T_s$, where the T_i are simple i.e. they contain no proper subtori. Each T_i splits over a Galois extension L_i and the compositum of these fields is L. Two algebraic tori are isogenous precisely when their character groups become isomorphic when tensored with $\mathbb{Q}$.

Consider the torus $\mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_{m,F}$, derived from the multiplicative group $\mathbb{G}_{m,F}$ over a number field F by restriction of scalars to $\mathbb{Q}$. Tori of this form, along with their finite direct products, are often called quasi-split. They are characterised by the property that their character groups are permutation modules with respect to their Galois action. For example, the character group of R_L is $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$. In this regard, these tori are the easiest to study. We will make use of their tractability via the following lemma:

Lemma 5.5. *Let M be a simple algebraic torus over $\mathbb{Q}$, split over a Galois field F. Then M can be covered by the quasi-split torus*

$$R_F := \mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_{m,F}.$$

That is, M can be put into an exact sequence

$$1 \to N \to R_F \to M \to 1,$$

where N is a $\mathbb{Q}$-torus.

Proof. The fact that M may be covered by some finite product R_F^s is [PR91], Proposition 2.2. However, since the Hom functor commutes with products, an element of

$$\mathrm{Hom}(R_F^s, M)$$

is a product of morphisms into M, each of which has an image constituting a subtorus of M. Since M is simple, we may assume that all but one of these images is trivial i.e. we may assume $s = 1$. □

In light of this, each T_i may be covered by a copy of R_L. Any such morphism of tori is equivalent to an injection of character groups

$$\xi : X^*(T_i) \hookrightarrow X^*(R_L).$$

We have proved the existence of such embeddings, but have not specified one precisely. We identify $X^*(R_L)$ with $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ and choose a basis by enumerating the elements of the Galois group. We denote this basis

$$\{\psi_1, ..., \psi_{n_L}\}.$$

We define an inner product on $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ by letting

$$\langle \psi_i, \psi_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j, \end{cases}$$

and extending $\mathbb{Z}$-bilinearly.

Consider one of the T_i. For a fixed embedding

$$\xi : X^*(T_i) \hookrightarrow X^*(R_L),$$

and a chosen basis

$$\{\chi_1, ..., \chi_{d_i}\}$$

of $X^*(T_i)$, where d_i denotes the dimension of T_i, let m_ξ denote

$$\max\{|\langle \chi_j, \psi_k \rangle|\} \in \mathbb{N},$$

for $j = 1, ..., d_i$ and $k = 1, ..., n_L$. For each T_i we choose an embedding of $X^*(T_i)$ into $X^*(R_L)$ and a basis such that m_ξ is minimal i.e. the coordinates of this basis have the smallest upper bound on their absolute values among all possible choices.

Thus, we have a collection of surjective maps of tori

$$R_L \to T_i.$$

We consider their direct product, yielding another surjection

$$R_L^s \to T_1 \times \cdots \times T_s.$$

Now, since T is isogenous to $T_1 \times \cdots \times T_s$, we may choose a surjection

$$\lambda : T_1 \times \cdots \times T_s \to T,$$

with kernel of smallest degree, which we will denote by n_λ.

We denote the composition of our product map with λ as

$$r : R_L^s \to T.$$

Lemma 5.6. *Consider the morphism*

$$f : R_L^s \to T_1 \times \cdots \times T_s,$$

the direct product of the previously defined surjections of R on to the T_i, followed by raising to the power n_λ. Then there exists a unique morphism,

$$g : T \to T_1 \times \cdots \times T_s,$$

such that $f = g \circ r$.

Proof. Let S be the kernel of r. By the universal property of quotients, any morphism from R_L^s vanishing on S factors uniquely through r. □

5.4 Uniform boundedness.

Firstly, we recall a standard property of integral matrix groups due to Minkowski.

Theorem 5.7. *For any $d \in \mathbb{N}$, the number of isomorphism classes of finite groups contained in $\mathrm{GL}_d(\mathbb{Z})$ is finite.*

We have fixed an algebraic torus T over $\mathbb{Q}$ of dimension d with splitting field L. In other words, for any choice of basis, we have a faithful representation

$$\rho : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{GL}_d(\mathbb{Z}).$$

Therefore, by the previous theorem, $n_L = |\mathrm{Gal}(L/\mathbb{Q})|$ is bounded in terms of d only.

Secondly, we refer to a standard result from the theory of integral representations of finite groups (see [Tsi12], Theorem 2.1).

Theorem 5.8. *Let H be a finite group and let $d \in \mathbb{N}$. Then the number of isomorphism classes of integral representations of H of dimension d is finite.*

Recall that we chose a surjection

$$\lambda : T_1 \times \cdots \times T_s \to T,$$

with kernel of smallest degree n_λ. Tori over $\mathbb{Q}$ of dimension d with splitting field L induce d-dimensional representations of the Galois group of L. By Theorem 5.7, there are only finitely many choices for this group. Therefore, by Theorem 5.8, only finitely many isomorphism classes of such tori exist. Therefore, n_λ is bounded in terms of d only.

Recall that we also constructed

$$f : R_L^s \to T_1 \times \cdots \times T_s,$$

via the composition of our original direct product of surjections with raising to the power n_λ. This corresponds to embeddings

$$X^*(T_i) \hookrightarrow X^*(R_L),$$

for each i. We have chosen a canonical basis for $X^*(R_L)$ and we choose the bases for the $X^*(T_i)$ to be the bases chosen in the previous section multiplied by n_λ. The previously stated results yield the following:

Lemma 5.9. *The coordinates of these bases for the $X^*(T_i)$, with respect to the chosen bases of the $X^*(R_L)$, are bounded in terms of d only.*

5.5 Uniformisers.

We have identified $X^*(R_L)$ with $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ and chosen a canonical basis $\{\psi_1, ..., \psi_{n_L}\}$ by enumerating the elements of the Galois group. The inner product on $X^*(R_L)$ satisfies the invariance property

$$\langle \sigma\psi, \psi' \rangle = \langle \psi, \sigma^{-1}\psi' \rangle,$$

for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and $\psi, \psi' \in X^*(R_L)$. Now, $X^*(R_L)$ is naturally isomorphic to its dual $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$-module $\mathrm{Hom}(X^*(R_L), \mathbb{Z})$, sending ψ_i to $\langle \psi_i, - \rangle$, which we denote φ_i, and extending $\mathbb{Z}$-linearly. Via our perfect pairing

$$X_*(R_L) \times X^*(R_L) \to \mathbb{Z},$$

we have an isomorphism of $X_*(R_L)$ with the dual of $X^*(R_L)$. We identify φ_i with its image in $X_*(R_L)$. Thus, we obtain a basis

$$\{\varphi_1, ..., \varphi_{n_L}\}$$

of $X_*(R_L)$, which is that obtained by an enumeration of the elements of $\mathrm{Gal}(L/\mathbb{Q})$.

Let p be a rational prime, completely split in L. The basis

$$\{\psi_1, ..., \psi_{n_L}\}$$

induces an isomorphism of $R_L(\mathbb{Q}_p)$ with

$$\prod \mathbb{Q}_p^* = X_*(R_L) \otimes \mathbb{Q}_p^*.$$

Let P be the element of $R_L(\mathbb{Q}_p)$ such that $\chi_1(P) = p$ and $\chi_i(P) = 1$ for $i = 2, ..., n_L$. In fact, P is a uniformiser corresponding to a place lying above p and the Galois orbit of its image under the above isomorphism corresponds to a complete set of uniformisers at the places lying above p.

Applying the valuation map

$$\upsilon_p : \mathbb{Q}_p^* \to \mathbb{Z}$$

to each factor, we have a morphism from $X_*(R_L) \otimes \mathbb{Q}_p^*$ to $X_*(R_L)$. Under this morphism, P is sent to the basis element φ_1 and the Galois orbit of P yields the complete set of basis elements.

Now let l be a natural number and let $p_1, ..., p_l$ be rational primes completely split in L. For each p_i, let P_i be the element of $R_L(\mathbb{Q}_{p_i})$ associated to p_i via the above construction. We embed each $R_L(\mathbb{Q}_{p_i})$ into

$$R_L(\mathbb{A}_f) = (\mathbb{A}_f \otimes L)^*$$

in the natural way. For integers $a_1, ..., a_l$, we consider the element

$$I = P_1^{a_1} \cdots P_l^{a_l}$$

belonging to $R_L(\mathbb{A}_f)$.

Recall that we have a surjective map of $\mathbb{Q}$-tori,

$$r : R_L^s \to T.$$

Following [UYb], we have an induced map on the corresponding class groups, which we denote

$$r_h : h_{R_L^s} \to h_T.$$

Let $H = h_{R_L^s} / \ker r_h$. We will show that

$$\mathcal{M}_H(l) > \frac{c \log \Delta_L}{\log(l) + \log\log \Delta_L},$$

for any $l \in \mathbb{N}$, provided Δ_L is greater than a uniform constant. Since H injects into h_T, it is an easy observation that $\mathcal{M}_{h_T}(l) \geq \mathcal{M}_H(l)$, for any $l \in \mathbb{N}$, thus yielding (1).

Henceforth, let I_i denote the embedding of I into the i^{th} factor of $R_L^s(\mathbb{A}_f)$. We denote by $\underline{I}$ the product of the I_i i.e. I embedded diagonally into $R_L^s(\mathbb{A}_f)$. Recall that, by Lemma 5.6, we have the following commutative diagram:

$$\begin{array}{ccccc} R_L^s(\mathbb{A}_f) & \longrightarrow & T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f) & \longrightarrow & T(\mathbb{A}_f) \\ & \searrow^{f} & & \swarrow^{g} & \\ & & T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f) & & \end{array}$$

with r being the composite homomorphism from $R_L^s(\mathbb{A}_f)$ to $T(\mathbb{A}_f)$.

Assume that $\underline{I}$ belongs to the kernel of r_h i.e.

$$r(\underline{I}) = \pi k \in T(\mathbb{Q})K_T^m,$$

where this product is unique up to an element of $T(\mathbb{Q}) \cap K_T^m$, which by [Yaf06], Theorem 2.5 is a finite group of order bounded in terms of the dimension of T only. Now, $f(\underline{I}) = g(\pi k)$, but f is a product of morphisms from $R_L(\mathbb{A}_f)$ into the $T_i(\mathbb{A}_f)$, so we write $f(\underline{I})$ as

$$(f_1(I), ..., f_s(I)).$$

As g is a morphism into $T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f)$, we write $g(\pi k)$ as

$$(g_1(\pi k), ..., g_s(\pi k)).$$

Therefore, we have

$$f_i(I) = \pi_i k_i \in T_i(\mathbb{Q})K_{T_i}^m,$$

for $i = 1, ..., s$, where $\pi_i = g_i(\pi)$ and $k_i = g_i(k)$.

Now, recall the bases for the $X^*(T_i)$ embedded in $X^*(R_L)$ via the maps induced by the f_i. We denote their elements as $\chi_{i,j}$, where $i = 1, ..., s$ and $j = 1, ..., d_i$. Furthermore, let

$$\pi_{i,j} = \chi_{i,j}(\pi_i).$$

The following lemma is a generalisation of [Yaf06], Lemma 2.13:

Lemma 5.10. *The field L' generated over $\mathbb{Q}$ by the $\pi_{i,j}$ is L.*

Proof. Clearly $L' \subseteq L$, so let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and assume that σ acts trivially on L'. We need to show that σ is trivial. We have a faithful representation of $\mathrm{Gal}(L/\mathbb{Q})$ on the product of the $X_*(T_i)$ and, thus, it is equivalent to show that σ acts trivially on each $X_*(T_i) \otimes \mathbb{Q}$.

Recall our surjective maps of tori from R_L to the T_i, which we denoted f_i. After tensoring our cocharacter modules with $\mathbb{Q}$ we retrieve short exact sequences

$$0 \to \mathbb{Q} \otimes \Delta_i \to \mathbb{Q} \otimes \Gamma \to \mathbb{Q} \otimes X_*(T_i) \to 0,$$

where $\Gamma = \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ and the Δ_i are Γ-submodules of $X_*(R_L) = \Gamma$. The Δ_i correspond to the kernels of our surjections, which we denote N_i. We will show that σ acts trivially on the

$$\mathbb{Q} \otimes (X_*(R_L)/X_*(N_i)).$$

We will consider in turn the elements I_i. Since f is a product of the maps f_i, we will consider the I_i as belonging to $R_L(\mathbb{A}_f)$ mapping to $T_i(\mathbb{A}_f)$. The elements under scrutiny here are the $\pi_i \in T_i(\mathbb{Q})$, which are diagonally embedded in $T_i(\mathbb{A}_f)$. Therefore, we relabel p_1, P_1 and a_1 as p, P and a, respectively, and project from $R_L(\mathbb{A}_f)$ to $R_L(\mathbb{Q}_p)$ i.e. we turn our attention from I_i to its image $P^a \in R(\mathbb{Q}_p)$, mapping under f_i to $\pi_i k_{i,p}$, where $k_{i,p}$ is the p-component of k_i.

Since p splits each T_i, we also have

$$T_i(\mathbb{Q}_p) = X_*(T_i) \otimes \mathbb{Q}_p^*,$$

sending $x \in T_i(\mathbb{Q}_p)$ to

$$(\chi_{i,1}(x), ..., \chi_{i,d_i}(x)),$$

where we tacitly assume a choice

$$\{\mu_{i,1}, ..., \mu_{i,d_i}\}$$

of the natural dual basis to our character basis already chosen, as described earlier for R_L. The valuation $\upsilon_p : \mathbb{Q}_p^* \to \mathbb{Z}$ evaluates each factor, inducing an isomorphism between $T_i(\mathbb{Q}_p)/K^m_{T_i,p}$ and $X_*(T_i)$, where $K^m_{T_i,p}$ is the maximal compact open subgroup of $T_i(\mathbb{Q}_p)$.

We have the following commutative diagrams

$$\begin{array}{ccc} R_L(\mathbb{Q}_p) & \longrightarrow & X_*(R_L) \\ \big\downarrow & & \big\downarrow \\ T_i(\mathbb{Q}_p)/K^m_{T_i,p} & \longrightarrow & X_*(T_i), \end{array}$$

where the bottom arrow is the isomorphism just mentioned and the top arrow is the corresponding surjection for $R_L(\mathbb{Q}_p)$ described earlier. The righthand arrow is the map of cocharacters induced by f_i and the left arrow is f_i composed with factoring out by $K^m_{T,p}$.

The element P^a is mapped to the class of π_i in $T_i(\mathbb{Q}_p)/K^m_{T_i,p}$, which is mapped to

$$(\upsilon_p(\chi_{i,1}(\pi_i)), ..., \upsilon_p(\chi_{i,d_i}(\pi_i))) \in X_*(T_i).$$

On the other hand, P^a is mapped to

$$(\upsilon_p(\psi_1(P^a)), ..., \upsilon_p(\psi_{n_L}(P^a))) \in X_*(R_L),$$

which is $a\varphi_1$. In this form, the action of a $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ is clear, sending this image to

$$(\upsilon_p((\tau^{-1}\psi_1)(P^a)), ..., \upsilon_p((\tau^{-1}\psi_{n_L})(P^a))).$$

Note that, since $\mathrm{Gal}(L/\mathbb{Q})$ permutes the characters, the Galois orbit of the image of P^a comprises precisely the elements $a\varphi_i$, which constitute a basis for $X_*(R_L) \otimes \mathbb{Q}$.

We claim that the image of this orbit in $X_*(T_i)$ consists of the elements

$$(\upsilon_p((\tau^{-1}\chi_{i,1})(\pi_i)), ..., \upsilon_p((\tau^{-1}\chi_{i,d_i})(\pi_i))) \in X_*(T_i). \qquad (2)$$

To see this, let $\tau\mu_{i,j}$ be denoted by

$$\sum_{k=1}^{d_i} n_{j,k}^{i,\tau} \mu_{i,k}.$$

Thus, the image of

$$\sum_{j=1}^{d_i} \chi_{i,j}(\pi_i)\mu_{i,j} \in X_*(T_i) \otimes \mathbb{Q}_p^*$$

under $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ will be

$$\sum_{k=1}^{d_i} \sum_{j=1}^{d_i} n_{j,k}^{i,\tau} \chi_{i,j}(\pi_i)\mu_{i,k}.$$

The k^{th} coefficient here is equal to $(\tau^{-1}\chi_{i,k})(\pi_i)$ if we have $n_{k,j}^{i,\tau^{-1}} = n_{j,k}^{i,\tau}$ for all $j, k = 1, ..., d_i$, but this is simply the Galois invariance of the inner product we previously placed on $X^*(R_L)$.

Now, since σ fixes each $\pi_{i,j}$ and the characters $\chi_{i,j}$ are a basis, σ clearly fixes each of the elements of $X_*(T_i)$ depicted in (2). Thus, by our exact sequence, σ fixes the Galois orbit of the image of P^a in

$$\mathbb{Q} \otimes (X_*(R_L)/X_*(N_i)).$$

Since these elements span the above space, the claim follows.

$\square$

Remark 5.11. *It is worth noting that any element in $R_L^s(\mathbb{A}_f)$ with a nonzero valuation at a place lying above a split prime in each of the s factors produces generators for L via this argument.*

5.6 Small split primes.

The remainder of the proof follows the concluding pages of [UYb].

We have $I = P_1^{a_1} \cdots P_l^{a_l} \in R_L(\mathbb{A}_f)$ embedded diagonally into $R_L^s(\mathbb{A}_f)$. We denote this element $\underline{I}$. The image of $\underline{I}$ in $T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f)$ under f is

$$f(\underline{I}) = (\pi_1 k_1, ..., \pi_s k_s) \in T_1(\mathbb{Q})K_{T_1}^m \times \cdots \times T_s(\mathbb{Q})K_{T_s}^m.$$

We consider the images $\pi_{i,j}$ of the π_i under the elements $\chi_{i,j}$ of the character bases. Due to Lemma 5.9, we have a bound B, say, on the absolute values of the coordinates of these basis elements with respect to the chosen basis for $X^*(R_L)$. This bound depends only on d. We replace the $\pi_{i,j}$ by $(p_1^{|a_1|} \cdots p_l^{|a_l|})^B \pi_{i,j}$, which therefore belong to $\mathcal{O}_L$.

By virtue of Lemma 5.10, we may form a primitive element

$$\alpha = \sum_{i,j} a_{i,j} \pi_{i,j}$$

for the field L, where the $a_{i,j}$ are integers with absolute value bounded by some constant B' depending only on d. We take the $\mathbb{Q}$-basis $\{1, \alpha, \alpha^2, ..., \alpha^{n_L-1}\}$ for L. Consequently, $\mathbb{Z}[1, \alpha, \alpha^2, ..., \alpha^{n_L-1}]$ is an order in $\mathcal{O}_L$. We denote the absolute value of its discriminant as Δ'_L. Therefore,

$$\Delta'_L \geq \Delta_L.$$

On the other hand, Δ'_L is the square of the determinant of the matrix

$$(\tau_i(\alpha^j))_{i,j},$$

where the τ_i range over the elements of $\mathrm{Gal}(L/\mathbb{Q})$ and $0 \leq j \leq n_L - 1$. An inequality of Hadamard then states that, given an upper bound C on the values of

$$|\tau_i(\alpha^j)|,$$

we have

$$\Delta'_L \leq n_L^{n_L} C^{2n_L} \leq c_1 C^{2n_L},$$

where $c_1 > 0$ is a constant depending only on d.

The splitting field L of T is a Galois CM-field. For a character χ, we denote by $\overline{\chi}$ the image of χ under the automorphism of L induced by complex conjugation on $\mathbb{C}$. It is at this point that we use the fact that $T(\mathbb{R})$ is compact and is, therefore, a product of circles (see [Vos98], Section 10.1). This implies that $\chi_{i,j}\overline{\chi_{i,j}}$ is the trivial character for every i and j (writing the group law multiplicatively).

Thus, for each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$,

$$|\tau(\pi_{i,j})| = (p_1^{|a_1|} \cdots p_l^{|a_l|})^B$$

and, therefore, by the preceding discussion,

$$|\tau_i(\alpha^j)| \leq (dB'(p_1^{|a_1|} \cdots p_l^{|a_l|}))^{B(n_L-1)}.$$

Hence, our calculation yields

$$c_1^{-1}\Delta_L \leq (dB'(p_1^{|a_1|} \cdots p_l^{|a_l|}))^{2Bn_L(n_L-1)}.$$

It remains to find the p_i for any given l. We require the following corollary of a special case of the effective Chebotarev Density Theorem, a proof of which can be found in [AD03].

Theorem 5.12. *Let F be any number field. Assume the GRH holds for the Dedekind zeta function of F. Let $\pi_F(x)$ denote the number of rational primes p completely split in F such that $p \leq x$. There exist positive absolute constants c_2 and c_3 that are effectively calculable such that, for all $x \geq c_2(\log \Delta_F)^2(\log\log \Delta_F)^4$,*

$$\pi_F(x) \geq c_3 \frac{x}{\log x}.$$

We assume the GRH for CM fields. Let l be any natural number. We require at least l primes completely split in L, so let

$$x = c_4 l \log l + c_1(\log \Delta_L)^2(\log\log \Delta_L)^4 > 1,$$

where c_4 is a positive absolute constant, such that

$$c_3 \frac{x}{\log x} \geq l.$$

It is uniform since

$$\frac{x}{\log x} \geq \frac{c_4 l \log l}{\log c_4 + 2\log l},$$

and so our requirement is satisfied when, for example, $\frac{c_3 c_4}{\log c_4 + 2} \geq 1$.

Thus, by Theorem 5.12, we are able to find l primes $p_1, ..., p_l$ completely split in L such that $p_i \leq x$. Subsequently, we return to our inequality

$$c_1^{-1}\Delta_L \leq (dB'(p_1^{|a_1|} \cdots p_l^{|a_l|}))^{2Bn_L(n_L-1)},$$

taking the p_i to be those just found. As before, we let

$$A = \sum_{i=1}^{l} |a_i|,$$

yielding

$$\log(D^{-1}\Delta_L) \leq 2ABn_L(n_L - 1)\log x,$$

provided $\Delta_L > D$, where $D = c_1(dB')^{2Bn_L(n_L-1)}$. Now, there exists a positive absolute constant c_5 such that

$$\log x \leq c_5(\log l + \log\log\Delta_L),$$

provided Δ_L exceeds a positive absolute constant. Combining these two inequalities yields a lower bound for A, which implies (1).

□

Remark 5.13. *The constant c given in the statement of Theorem 5.2 can be taken to be $\frac{1-\epsilon}{2Bn_L(n_L-1)}$ for any $0 < \epsilon < 1$.*

6 André-Oort for a product of modular curves

We now turn our attention towards the strategy of Edixhoven, which was eventually generalised by Klingler, Ullmo and Yafaev to a full proof of the André-Oort conjecture under the GRH for CM fields.

In this section, we give a short proof under the GRH of the André-Oort conjecture for products of modular curves, using only simple Galois-theoretic and geometric arguments. This will serve as a prototype for our strategy to prove the full conjecture under the GRH without using ergodic theory. We also demonstrate a short proof of the Manin-Mumford conjecture for Abelian varieties using similar arguments.

Therefore, we will prove the following theorem:

Theorem 6.1. *Assume the GRH for imaginary quadratic fields. Let S be a product of modular curves and let Σ be a set of special points in S. Every irreducible component of the Zariski closure of $\cup_{s\in\Sigma}s$ in S is a special subvariety.*

Note that S always admits a morphism π to the Shimura variety arising as the quotient $\mathrm{SL}_2^n(\mathbb{Z})\backslash\mathbb{H}^n$ and an irreducible subvariety Z of S is special if and only if $\pi(Z)$ is special. Therefore, we will assume S is the Shimura variety arising from $\mathrm{SL}_2^n(\mathbb{Z})\backslash\mathbb{H}^n$, which we identify with $\mathbb{C}^n$. Special subvarieties of $\mathbb{C}^n$ have the following description (see [UY09], Definition 2.1):

Definition 6.2. *Let $I = \{1, ..., n\}$. A closed irreducible subvariety Z of $\mathbb{C}^n$ is called special (of type $\Omega = \Omega_Z$) if I has a partition $\Omega = (I_1, ..., I_t)$, with $|I_i| = n_i$, such that Z is a product of subvarieties Z_i of $\mathbb{C}^{n_i}$, each of one of the following forms:*

- *I_i is a one element set and Z_i is a CM point.*

- *Z_i is the image of $\mathbb{H}$ in $\mathbb{C}^{n_i}$ under the map sending τ in $\mathbb{H}$ to the image of $(g_s \cdot \tau)_{s \in I_i}$ in $\mathbb{C}^{n_i}$ for elements $g_s \in \mathrm{GL}_2(\mathbb{Q})^+$.*

Given a special subvariety Z of type Ω, we define $c(\Omega)$ to be the number of CM factors. A special subvariety Z is called strongly special if $c(\Omega) = 0$.

The strategy of this paper will be to consider an irreducible subvariety X in $\mathbb{C}^n$ containing a Zariski dense set Σ of special subvarieties. After, if necessary, replacing Σ by a Zariski dense subset, we may assume that $c(\Omega_Z)$ is constant as Z ranges through Σ. Hence, we denote its value $c(\Sigma)$. Under the GRH, using Galois-theoretic and geometric arguments, Ullmo and Yafaev show in [UY09] that, if $c(\Sigma) > 0$, then X contains a Zariski dense set Σ' with $c(\Sigma') = 0$. Therefore, we consider sets of strongly special subvarieties. These are dealt with in [CU05] via ergodic theory. In this section, we show that the irreducible components of the Zariski closure of a set of strongly special subvarieties are special using only simple geometric arguments.

The André-Oort conjecture for products of modular curves was also tackled via relatively elementary methods by Edixhoven in [Edi05]. However, his method relied intrinsically on the properties of products of modular curves. The motivation for this work was to develop a strategy that would apply to a general Shimura variety and, furthermore, to support the exposition of this strategy.

Given a set of strongly special subvarieties Σ, we consider an irreducible component X of the Zariski closure of $\cup_{Z \in \Sigma} Z$. The idea of the proof is to intersect X with its image under a suitable Hecke correspondence and reiterate this procedure, each time with an irreducible component of the previous intersection. By comparing lower bounds for the degrees of strongly special subvarieties with the degrees of Hecke correspondences, we arrive at a nonproper intersection. For each Z in Σ, we produce a Z' strictly containing Z and repeat the argument.

6.1 Degrees of strongly special subvarieties

For some $n \in \mathbb{N}$, consider the image of $\mathbb{H}$ in $\mathbb{C}^n$ under the map described in Definition 6.2 for some $g_1, ..., g_n \in \mathrm{GL}_2(\mathbb{Q})^+$. For simplicity we may assume that g_1 is the identity. This image is the modular curve $\Gamma'\backslash\mathbb{H}$ embedded in $\mathbb{C}^n$, with $\Gamma' := \Gamma \cap g_2^{-1}\Gamma g_2 \cap ... \cap g_n^{-1}\Gamma g_n$, where $\Gamma := \mathrm{SL}_2(\mathbb{Z})$.

By [KY], Proposition 5.3.2., the projection

$$\pi : \Gamma'\backslash\mathbb{H} \to \Gamma\backslash\mathbb{H},$$

extends to a morphism

$$\overline{\pi} : \overline{\Gamma'\backslash\mathbb{H}} \to \overline{\Gamma\backslash\mathbb{H}}$$

of the Baily-Borel compactifications, such that the inverse image $\overline{\pi}^* L_\Gamma$ of the Baily-Borel line bundle on $\overline{\Gamma\backslash\mathbb{H}}$ is $L_{\Gamma'}$, the Baily-Borel line bundle on $\overline{\Gamma'\backslash\mathbb{H}}$, which is the restriction of the Baily-Borel line bundle on $(\mathbb{P}^1_{\mathbb{C}})^n$. Therefore, by the projection formula (see citeKY, §1), we have

$$\deg_{L_{(\mathbb{P}^1_{\mathbb{C}})^n}} \overline{\Gamma'\backslash\mathbb{H}} = \deg \overline{\pi} \cdot \ \deg_{L_\Gamma} \overline{\Gamma\backslash\mathbb{H}},$$

which is bounded below by the index $[\Gamma : \Gamma']$ multiplied by an absolute positive constant.

Consider the closures $\overline{\Gamma} = \mathrm{SL}_2(\hat{\mathbb{Z}})$ and $\overline{\Gamma'}$ of Γ and Γ' in $\mathrm{SL}_2(\hat{\mathbb{Z}})$, respectively. We have $[\Gamma : \Gamma'] \geq [\overline{\Gamma} : \overline{\Gamma'}]$, which is equal to

$$\prod_p \left[\mathrm{SL}_2(\mathbb{Z}_p) : (\mathrm{SL}_2(\mathbb{Z}_p) \cap g_2^{-1}\mathrm{SL}_2(\mathbb{Z}_p)g_2 \cap ... \cap g_n^{-1}\mathrm{SL}_2(\mathbb{Z}_p)g_n)\right],$$

noting that, for almost all p, $g_i \in \mathrm{GL}_2(\mathbb{Z}_p)$ for all $i = 2, ..., n$ i.e. the above indices at these primes are equal to one. Now suppose that $g_i \notin \mathrm{GL}_2(\mathbb{Z}_p)$ for some $i \in \{2, ..., n\}$ and a prime p. Considering Smith normal forms, it is possible to write $g_i = \gamma D \gamma'$, where $\gamma, \gamma' \in \mathrm{GL}_2(\mathbb{Z}_p)$ and D is a diagonal matrix of the form $\mathrm{diag}(p^n, p^{-n})$, for some $n \in \mathbb{N}$. Then

$$\mathrm{SL}_2(\mathbb{Z}_p) \cap g_2^{-1}\mathrm{SL}_2(\mathbb{Z}_p)g_2 \cap ... \cap g_n^{-1}\mathrm{SL}_2(\mathbb{Z}_p)g_n$$

is contained in the subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ whose lower left entry belongs to $p\mathbb{Z}_p$. The index of this subgroup can be calculated as in [Mil12], p81 and is bounded below by p.

Therefore, from the above remarks, we conclude that the degree of $\Gamma' \backslash \mathbb{H}$ with respect to the Baily-Borel line bundle on $(\mathbb{P}^1_{\mathbb{C}})^n$ is bounded below by the product of primes p such that $g_i \notin \mathrm{GL}_2(\mathbb{Z}_p)$ for some $i \in \{2, ..., n\}$.

Henceforth, when we refer to the degree of a subvariety of $\mathbb{C}^n$, we will omit reference to the Baily-Borel line bundle.

6.2 Choosing a suitable Hecke correspondence

We are considering the Shimura variety $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ defined by the Shimura datum

$$(G, X) := (\mathrm{GL}_2^n, (\mathbb{H}^{\pm})^n)$$

and $K := \mathrm{GL}_2^n(\hat{\mathbb{Z}})$, a compact open subgroup of $\mathrm{GL}_2^n(\mathbb{A}_f)$. Consider GL_2 embedded into GL_2^n via the map

$$\varphi : x \mapsto (x, g_2 x g_2^{-1}, ..., g_n x g_n^{-1}),$$

for $g_2, ..., g_n \in \mathrm{GL}_2(\mathbb{Q})^+$. We denote its image by H and we write X_H^+ for its connected component $H(\mathbb{R})^+ \cdot (i, g_2 i, ..., g_n i) \subset \mathbb{H}^n$. Let Z be the image of $X_H^+ \times \{1\}$ in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$. This is the image of $\mathbb{H}$ described in the previous section.

Lemma 6.3. *For any $\alpha \in H(\mathbb{A}_f)$, Z is contained in its image under the Hecke correspondence T_{α^2}.*

Proof. Let $\overline{(x, 1)} \in Z$ i.e. $x \in X_H^+$. Let $\tau \in \mathrm{GL}_2(\mathbb{A}_f)$ be such that $\alpha = \varphi(\tau)$. A point $\overline{(h, g)} \in \mathrm{Sh}_K(G, X)_{\mathbb{C}}$ depends only on g modulo $(\mathbb{A}_f^*)^n = (\mathbb{Q}^* \cdot \hat{\mathbb{Z}}^*)^n$ since these factors are killed in the double coset defining the Shimura variety. Hence, we consider the image of τ^2 under the natural map

$$\pi : \mathrm{GL}_2 \to \mathrm{PGL}_2,$$

which is surjective on adélic points since the kernel $\mathbb{G}_m$ is connected. Consider the simply connected covering

$$\rho : \mathrm{SL}_2 \to \mathrm{PGL}_2.$$

Its kernel is isomorphic to μ_2. Therefore, there exists a $\upsilon \in \mathrm{SL}_2(\mathbb{A}_f)$ such that $\rho(\upsilon) = \pi(\tau^2)$. By strong approximation applied to SL_2, $\upsilon = qk$, with $q \in \mathrm{SL}_2(\mathbb{Q})$ and k belonging to the compact open subgroup

$$\bigcap_{i=1}^{n} g_i^{-1} \mathrm{SL}_2(\hat{\mathbb{Z}}) g_i \subset \mathrm{SL}_2(\mathbb{A}_f),$$

where we define $g_1 := \mathrm{id}$. Note that π restricted to SL_2 coincides with ρ, since ρ is the universal cover. Now, $\varphi(q)$ belongs to $H(\mathbb{Q})^+$. Hence, $\varphi(q) \cdot x$ belongs to X_H^+. Therefore, consider $\overline{(\varphi(q) \cdot x, \varphi(\tau^2))} \in T_{\alpha^2}(Z)$. By the previous discussion, this equals $\overline{(\varphi(q) \cdot x, \varphi(qk))} = \overline{(x, \varphi(k))}$. However, since $\varphi(k) \in \mathrm{GL}_2^n(\hat{\mathbb{Z}})$, this point is $\overline{(x, 1)}$. □

Choose a prime p such that $g_i \in \mathrm{GL}_2(\mathbb{Z}_p)$ for all $i = 2, ..., n$ and consider the element

$$P := \begin{pmatrix} 1 & 0 \\ 0 & p^{-2} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+$$

Let $\alpha \in H(\mathbb{Q}_p)$ be the image of P in $\mathrm{GL}_2^n(\mathbb{Q}_p)$ under φ. Since the g_i belong to $\mathrm{GL}_2(\mathbb{Z}_p)$ for all $i = 2, ..., n$, the double coset $K\alpha K$ equals $K\beta K$, where β is P diagonally embedded into $\mathrm{GL}_2^n(\mathbb{Q}_p)$.

Recall that, by [EY03], Theorem 6.1, the connected components of the correspondence T_β on $\mathbb{C}^n$ are the T_{β_i} induced by $\mathrm{GL}_2^n(\mathbb{Q})^+$ acting on $\mathbb{H}^n$ such that

$$\mathrm{GL}_2^n(\mathbb{Q})^+ \cap K\beta K = \coprod_i \Gamma^n \beta_i^{-1} \Gamma^n.$$

Note, however, that $\mathrm{GL}_2^n(\mathbb{Q})^+ \cap K\beta K = \Gamma^n \beta \Gamma^n$. Hence, the correspondence T_β is irreducible and equal to the standard Hecke correspondence T_{p^2} on $\mathbb{C}^n$. Combining this observation with Lemma 6.3, we obtain the following result:

Lemma 6.4. *Let Z be the image of $\mathbb{H}$ in $\mathbb{C}^n$ as defined above. Choose a prime p such that $g_i \in \mathrm{GL}_2(\mathbb{Z}_p)$ for all $i = 2, ..., n$. Then Z is contained in its image under the Hecke correspondence T_{p^2} on $\mathbb{C}^n$ given by P^{-1}.*

6.3 Proof of the main result

Recall the situation in the statement of Theorem 6.1. By [UY09] we may assume that $c(\Sigma) = 0$ i.e. Σ is a set of strongly special subvarieties. The GRH will not be used in this case. Using [EY03], Proposition 2.1, we may assume that S arises as the product of n copies of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

Denote by X an irreducible component of the Zariski closure of $\cup_{s\in\Sigma}s$ in S. Consider a special subvariety $Z \subset X \subset \mathbb{C}^n$. Given our description of strongly special subvarieties we write $Z = Z_1 \times \cdots \times Z_t$, where each Z_i is the image of $\mathbb{H}$ in $\mathbb{C}^{n_i}$ given by some $g_{i_2}, ..., g_{i_{n_i}} \in \mathrm{GL}_2(\mathbb{Q})^+$. Therefore, by the arguments in Section 6.1, the degree of Z is bounded below by the product of all primes p such that not all $g_{i_j} \in \mathrm{GL}_2(\mathbb{Z}_p)$ for $i = 1, ..., t$ and $j = 2, ..., n_i$. We denote this product $M_Z \in \mathbb{N}$. By Lemma 6.4, for any prime p not dividing M_Z, we have $Z \subset T_{p^2}(Z)$,

By [Edi05], Section 3, we may assume that X is a hypersurface all of whose projections to any $n-1$ factors of $\mathbb{C}^n$ are dominant. Under this assumption, by [UY09], Proposition 3.1, if $n \geq 3$, $T_{p^2}(X)$ is irreducible for any p greater than $\deg X$ and 13. If $n = 2$, Z is either a modular curve or $\mathbb{C}^2$, in which case X is a modular curve or $\mathbb{C}^2$ and we are done.

Consider first the case that X contains a Zariski dense subset Σ' such that M_Z is bounded for all Z in Σ' i.e. the elements g_{i_j} defining a given Z must belong to $\mathrm{GL}_2(\mathbb{Z}_p)$ for all but a fixed and finite set of primes whose product we denote M. For any prime p not dividing M, every Z in Σ' is contained in its image under T_{p^2}. Hence, Σ' belongs to $X \cap T_{p^2}(X)$. This is a closed set and so $X \subset T_{p^2}(X)$. However, since $T_{p^2}(X)$ is irreducible (provided p is larger than $\deg X$ and 13), we must have equality. By [Edi05], Lemma 4.4, for any point $z \in \mathbb{C}^n$, the T_{p^2}-orbit $\cup_{i \geq 0} T^i_{p^2}(z)$ is dense in $\mathbb{C}^n$ for the archimedean topology. Thus, $X = \mathbb{C}^n$ and we are done.

Therefore, we assume that X contains no such Zariski dense subset. Hence, we may assume that M_Z is larger than any predetermined constant for all Z in Σ. We consider an arbitrary Z. By a theorem of Chebyshev, there exist positive absolute constants c_1 and c_2 such that the number of primes $\pi(x)$ less than a given real number $x \geq 2$ is bounded below by $c_1 \frac{x}{\log x}$ and above by $c_2 \frac{x}{\log x}$. Therefore, for any fixed $0 < \delta_1 < 1$ and $\epsilon > 0$,

$$\pi\left(M_Z^{\delta_1}\right) \gg \frac{M_Z^{\delta_1}}{\log M_Z^{\delta_1}} \gg M_Z^{\delta_1 - \epsilon}.$$

It is an obvious fact that the number of primes $\omega(M_Z)$ dividing M_Z satisfies

$$\omega(M_Z) \leq \frac{\log M_Z}{\log 2} \ll M_Z^{\epsilon}.$$

Therefore, for M_Z larger than a constant depending only on X, we can find a prime p_1 not dividing M_Z, smaller than $M_Z^{\delta_1}$ and larger than $\max\{13, \deg X\}$. The last condition implies that $T_{p_1^2}(X)$ is irreducible. Therefore, the intersection of X and $T_{p_1^2}(X)$ is either proper or $X = T_{p_1^2}(X)$. If $X = T_{p_1^2}(X)$ then we are done, as explained above.

Therefore, we assume that the intersection is proper. For the prime p_1, $Z \subset T_{p_1^2}(Z)$, which implies $Z \subset X \cap T_{p_1^2}(X)$. We relabel X as X_1 and let X_2 be an irreducible component of the intersection containing Z. Notice that, by Bezout's theorem ([RU09], Lemme 3.4), the degree of $X_2 \subset X_1 \cap T_{p_1^2}(X_1)$ is bounded above by $(\deg X_1)^2 \cdot \deg T_{p_1^2}$, where

$$\deg T_{p_1^2} = |\Gamma : \Gamma_0(p_1^2)|^n = p_1^n (p_1 + 1)^n \ll p_1^{2n},$$

i.e. $\deg X_2 \ll p_1^{2+2n} \ll M_Z^{(2+2n)\delta_1}$.

So long as δ_1 and ϵ are small enough, we can fix $0 < \delta_2 < 1$ such that $(2+2n)\delta_1 + 2\epsilon < \delta_2$. We have

$$\pi\left(M_Z^{(2+2n)\delta_1}\right) \ll \frac{M_Z^{(2+2n)\delta_1}}{\log M_Z^{(2+2n)\delta_1}} \ll M_Z^{(2+2n)\delta_1+\epsilon}$$

and

$$\pi\left(M_Z^{\delta_2}\right) \gg \frac{M_Z^{\delta_2}}{\log M_Z^{\delta_2}} \gg M_Z^{\delta_2-\epsilon}.$$

Therefore, for M_Z larger than a constant depending only on X, we can a find a prime p_2 not dividing M_Z, smaller than $M_Z^{\delta_2}$ and larger than $\max\{3, \deg X_2\}$. The first condition implies that $Z \subset X_2 \cap T_{p_2^2}(X_2)$. The last condition implies that if this intersection is not proper i.e. $X_2 \subset T_{p_2^2}(X_2)$, then X_2 is special by [Edi05], Theorem 4.1. It can only be strongly special since it contains Z. It is also of higher dimension than Z by comparing degrees. Hence, we replace Z in Σ with X_2.

Therefore, assume that the intersection is proper. We perform the above construction recursively, with suitable δ_k, assuming M_Z is large enough, thus obtaining subvarieties X_k and primes p_k. If at some point we have $X_k \subset T_{p_k^2}(X_k)$, X_k is a strongly special subvariety containing Z. If this inclusion does not occur at any of the previous stages, after a finite number of steps bounded by $\dim X_1$, we end up in the following situation:

- $\dim(X_k) = \dim(Z) + 1$
- $\deg(X_k) \ll M_Z^{(2+2n)\delta_{k-1}}$
- $\deg Z > M_Z$
- $Z \subset X_k$

- $p_k < M_Z^{\delta_k}$
- p_k not divinding M_Z
- $p_k > \deg(X_k)$

Therefore, we have $Z \subset X_k \cap T_{p_k^2}(X_k)$. By comparing the degrees of Z and $X_k \cap T_{p_k^2}(X_k)$, the intersection cannot be proper. Hence, X_k is contained in $T_{p_k^2}(X_k)$ and is therefore strongly special.

We perform this procedure on all of the Z, replacing them in Σ by strongly special subvarieties of higher dimension. Reiterating the above argument, we eventually conclude that X must be special.

6.4 Manin-Mumford

We conclude this section by remarking that the techniques exhibited above apply, in a simpler way, to the Manin-Mumford conjecture for Abelian varieties.

Theorem 6.5. *(***Manin-Mumford)** *Let K be a number field, A/K an Abelian variety over K and V/K a geometrically irreducible subvariety of A. If $V(\overline{K})$ contains a Zariski dense set of torsion points then V is the translate of an Abelian subvariety by a torsion point.*

Many proofs of this theorem exist. Ratazzi and Ullmo have recently given a proof combining Galois-theoretic and ergodic methods. We refer to their paper [RU09] for more details. Here we replace the ergodic theory in their proof with an elementary geometric argument. In this setting, special subvarieties are the translates of Abelian subvarieties by torsion points.

Proof. Let $(\Sigma_n)_{n\in\mathbb{N}}$ be a sequence of special subvarieties, the union of which is Zariski dense in V. For each $n \in \mathbb{N}$ we choose a representation

$$\Sigma_n = A_n + \xi_n,$$

where $A_n \subset A$ is an Abelian subvariety and ξ_n is a torsion point in the Abelian subvariety A'_n such that $A = A_n + A'_n$ and $A_n \cap A'_n$ is finite of uniformly bounded order (see [RU09], Proposition 2.1). Let d_n denote the order of the torsion point ξ_n.

Whether or not the sequence $(d_n)_{n\in\mathbb{N}}$ is bounded is independent of the choice of the ξ_n ([RU09], Remarque 3.1). In the case that the sequence $(d_n)_{n\in\mathbb{N}}$ is unbounded, Section 3.2 of [RU09] demonstrates that each Σ_n is contained in a special subvariety Σ'_n of higher dimension (the arguments here are Galois-theoretic, similar to the Shimura case, but are not dependent on the GRH). Therefore, we replace $(\Sigma_n)_{n\in\mathbb{N}}$ with $(\Sigma'_n)_{n\in\mathbb{N}}$ and reiterate this argument unless, at some point, we obtain a sequence $(\Sigma_n)_{n\in\mathbb{N}}$ with $(d_n)_{n\in\mathbb{N}}$ bounded.

In this case, since the set of torsion points of bounded order is finite, we may suppose that each Σ_n is of the form $A_n + \xi$, for a fixed torsion point ξ. However, since V is special if and only if $V - \xi$ is special, we may assume that $\Sigma_n = A_n$ for all $n \in \mathbb{N}$.

We denote by $[m]$ the multiplication by $m \in \mathbb{N}$ map on A and choose one of the A_n. Consider the intersection $V \cap [m]V$. Either it is proper or $[m]V = V$, in which case V is special by [RU09], Lemme 3.2. Notice that, by Bezout's theorem, the degree of $V \cap [m]V$ is bounded above by $\deg V \cdot \deg [m]V$

where, by [RU09], Lemme 3.1,

$$\deg[m]V \leq m^{2\dim V} \cdot \deg V.$$

It is a classical fact that an Abelian variety contains only finitely many Abelian subvarieties of bounded degree. Therefore, we may assume that the A_n have degree exceeding any uniform constant. Therefore, by comparing degrees, if $\dim V = \dim A_n + 1$ and $\deg A_n > m^{2\dim V} \cdot (\deg V)^2$, we must have $V = [m]V$.

If the intersection is proper we choose an irreducible component W of the intersection containing A_n. Therefore, A_n is contained in the intersection $W \cap [m]W$. Either this intersection is proper or $W = [m]W$ and W is special, in which case we replace A_n in $(\Sigma_n)_{n\in\mathbb{N}}$ by W, a special subvariety of higher dimension. Again, comparing degrees, if $\dim W = \dim A_n + 1$ and $\deg A_n > m^{8\dim V} \cdot (\deg V)^4$, we must have $W = [m]W$.

Otherwise, if $W \cap [m]W$ is a proper intersection, we take an irreducible component containing A_n and repeat the argument in the previous paragraph. After a finite number of steps, bounded by $\dim V$, we will have found a special subvariety strictly containing A_n. We perform this procedure on all of the A_n, replacing them by special subvarieties of V of higher dimension. Reiterating the above arguments at most $\dim V - 1$ times, we conclude that V must be special.

□

7 Degrees of strongly special subvarieties

In this final section we generalise the strategy of the previous section to give a new proof under the GRH of the André-Oort conjecture. That is, we generalise the strategy pioneered by Edixhoven, and implemented by Klingler and Yafaev, to all special subvarieties. Thus, we remove ergodic theory from the proof of Klingler, Ullmo and Yafaev and replace it with tools from algebraic geometry. Our key ingredient is a lower bound for the degrees of strongly special subvarieties coming from Prasad's volume formula for S-arithmetic quotients of semisimple groups. For ease of notation we make the following convention:

Definition 7.1. *Given a set Σ of special subvarieties of a Shimura variety S, we denote by $\mathbf{\Sigma}$ the subset $\cup_{V\in\Sigma}V$ of S.*

Recall the André-Oort conjecture:

Conjecture 7.2. (André-Oort) *Let S be a Shimura variety and let Σ be a set of special points in S. Every irreducible component of the Zariski closure of $\mathbf{\Sigma}$ in S is a special subvariety.*

As indicated, this work is complementary to the article [KY], in which Klingler and Yafaev consider the above conjecture with Σ replaced by a set of special subvarieties, rather than just points. Via extra machinery developed by Ullmo and Yafaev [UYa], the authors prove the conjecture, assuming the GRH, by repeatedly replacing the elements of Σ with higher dimensional special subvarieties. They rely on a lower bound, obtained by Ullmo and Yafaev, on the degree of the Galois orbit of a special subvariety. As one ranges through the elements of Σ, this bound is either bounded from above or tends to infinity. In the case that it tends to infinity, the authors are able to proceed using their generalisation of a method pioneered by Edixhoven that compares Galois orbits and Hecke correspondences. Though technical, the proof relies on the simple geometric idea exhibited above.

In the case that the lower bound is bounded for all elements in Σ, Klingler and Yafaev appeal to a result by Ullmo and Yafaev [UYa], generalising the equidistribution of strongly special subvarieties demonstrated by Clozel and Ullmo [CU05]. Our motivation was to remove this element of the proof, thus eliminating the dependency on the extremely deep and complicated theorems of Ratner. In this section, we achieve this aim, thus reproving the following theorem of Clozel and Ullmo:

Theorem 7.3. *Let Z be a subvariety of a Shimura variety S. There exists a finite set $\{V_1, ..., V_k\}$ of positive-dimensional strongly special subvarieties $V_i \subset Z$ such that, if $V \subset Z$ is a positive-dimensional strongly special subvariety, then $V \subset V_i$ for some $i \in \{1, ..., k\}$.*

Therefore, under the GRH, we are able to prove the André-Oort conjecture solely via the geometric strategy of Edixhoven. In fact, the case dealt with here is less technical and does not depend on the GRH. We employ similar tools from algebraic geometry and the theory of reductive groups over local fields. The main ingredient is the following lower bound for the degrees of strongly special subvarieties. We refer the reader to Section 7.1, 7.2, 7.3 and 7.5 for the relevant definitions and explanations.

Theorem 7.4. *Let (G, X) be a Shimura datum such that $G = G^{\mathrm{ad}}$ and fix a* *connected component X^+ of X. Fix a faithful representation*

$$\rho : G \hookrightarrow \mathrm{GL}_n$$

and let K be a neat compact open subgroup of $G(\mathbb{A}_f)$ such that K is the product of compact open subgroups $K_p \subset G(\mathbb{Q}_p)$. There exist positive constants c and δ such that, if V is a strongly special subvariety of $S_K(G,X)$, defined by (H, X_H), then

$$\deg_{\mathcal{L}_K} V > c \cdot \Pi(H, K_H)^{\delta}.$$

This bound replaces the lower bound on the degrees of Galois orbits used in [KY]. Otherwise, the strategy is largely similar, though somewhat simplified in this case since we will not need an analogue of [KY], Lemma 9.2.3. Given a strongly special subvariety V, contained in an irreducible subvariety Z, one obtains a lower bound for the degree of V in terms of a product of 'bad' primes (see Theorem 7.4). One then obtains a 'good' prime p, small compared to the degree of V, such that there exists a 'suitable' Hecke correspondence T at p satisfying $V \subset T(V)$. Thus, V is contained in $Z \cap T(Z)$. However, if the dimension of Z is only one greater than that of V, comparing their degrees leads one to realise that the intersection $Z \cap T(Z)$ cannot be proper. Therefore, since Z is irreducible, it must be contained in $T(Z)$. In this case, a geometric argument implies that there exists a strongly special subvariety $V' \subset Z$ such that $V \subsetneq V'$. On the other hand, if the intersection $Z \cap T(Z)$ is proper, one chooses an irreducible component containing V and repeats the above procedure.

This result represents the full generalisation of the strategy tested in the previous section for removing ergodic theory from the proof of the André-

Oort conjecture. However, we also hope that the bounds presented here will lead to useful developments in the wider world of the Zilber-Pink conjectures.

7.1 Generalities

Unless stated otherwise, all varieties (except for linear algebraic groups) will be defined over $\mathbb{C}$ and identified with their set of $\mathbb{C}$-points. We will denote by $\mathbb{A}_f$ the ring of finite (rational) adéles and by $\hat{\mathbb{Z}}$ the product of $\mathbb{Z}_p$ over all primes p.

For any algebraic group G, we will denote by G^{ad} the quotient of G by its centre. If G is defined over $\mathbb{Q}_p$ and ρ is a faithful representation, we will consider G as a subgroup of $\mathrm{GL}_{n,\mathbb{Q}_p}$. For such a subgroup, we will denote by $G_{\mathbb{Z}_p}$ the Zariski closure of G in $\mathrm{GL}_{n,\mathbb{Z}_p}$. We will say that G is unramified if it is quasi-split and splits over an unramified extension of $\mathbb{Q}_p$. If G and ρ are defined over $\mathbb{Q}$, then the previous definitions make sense for $G_{\mathbb{Q}_p}$ and $\rho_{\mathbb{Q}_p}$ for any prime p. A subgroup $K_p \subset G(\mathbb{Q}_p)$ is called hyperspecial if there exists a smooth reductive group scheme $\mathbf{G}$ over $\mathbb{Z}_p$ such that $\mathbf{G}_{\mathbb{Q}_p} = G_{\mathbb{Q}_p}$ and $\mathbf{G}(\mathbb{Z}_p) = K_p$ (see [BT84], 4.6). By a reductive group scheme, we mean a group scheme with reductive fibres.

Given an algebraic torus T over a field k and a representation

$$\rho : T \hookrightarrow \mathrm{GL}_{n,k},$$

let l/k be a Galois extension such that T_l splits. One obtains a decomposition $l^n = \oplus_\chi V_\chi$, summing over characters $\chi : T_l \to \mathbb{G}_{m,l}$ of T, where V_χ is the l-subspace on which T_l acts via χ. We refer to those characters χ such that $V_\chi \neq \{0\}$ as the characters intervening in l^n. The characters of T form a free $\mathbb{Z}$-module $X^*(T)$ equipped with an action of $\mathrm{Gal}(l/k)$. After choosing a basis for $X^*(T)$, one may refer to the coordinates of a character $\chi \in X^*(T)$.

Let X be a complete irreducible variety and let $\mathcal{L}$ be a line bundle on X with topological first Chern class

$$c_1(\mathcal{L}) \in H^2(X, \mathbb{Z}).$$

Given an irreducible subvariety V of X, we define the degree of V with respect to $\mathcal{L}$, as in [KY], 5.1, by

$$\deg_{\mathcal{L}} V := c_1(\mathcal{L})^{\dim V} \cap [V] \in H_0(X, \mathbb{Z}) = \mathbb{Z},$$

where $[V] \in H_{2\dim V}(X, \mathbb{Z})$ denotes the fundamental class of V and $\cap$ denotes the cap product between $H^{2\dim V}(X, \mathbb{Z})$ and $H_{2\dim V}(X, \mathbb{Z})$. We will also put

$$\int_V c_1(\mathcal{L})^{\dim V} := \deg_{\mathcal{L}} V.$$

When the variety X is a disjoint union of irreducible components X_i, the function $\deg_{\mathcal{L}}$ is defined as the sum $\sum_i \deg_{\mathcal{L}|X_i}$.

7.2 Reductions

Consider a Shimura datum (G, X), a connected component X^+ of X, and a compact open subgroup K of $G(\mathbb{A}_f)$. From now on, we will simply write $\mathrm{Sh}_K(G, X)$ for the corresponding Shimura variety and its $\mathbb{C}$-points. We will denote by $S_K(G, X)$ the image of $X^+ \times \{1\}$ in $\mathrm{Sh}_K(G, X)$. Recall that the André-Oort conjecture is equivalent for all choices of K. We may also assume that $G = G^{\mathrm{ad}}$.

We will write $\overline{\mathrm{Sh}_K(G, X)}$ for the Baily-Borel compactification of $\mathrm{Sh}_K(G, X)$ (as defined in [KY], Proposition 5.3.1) and $\mathcal{L}_K$ for the corresponding ample line bundle (as defined in [KY] Proposition 5.3.2). For an irreducible subvariety V of $\mathrm{Sh}_K(G,X)$ we will denote by $\overline{V}$ the Zariski closure of V in $\overline{\mathrm{Sh}_K(G,X)}$. We will write $\deg_{\mathcal{L}_K} V$ for $\deg_{\mathcal{L}_K} \overline{V}$.

Let $\alpha \in G(\mathbb{A}_f)$ and let T_α be the associated Hecke correspondence on $\mathrm{Sh}_K(G,X)$. Recall that, by the definition of a special subvariety, V is special if and only if one (or, equivalently, all) of the irreducible components of $T_\alpha(V)$ is (are) special. In particular, in order to prove the André-Oort conjecture, it suffices to consider sets of special subvarieties Σ such that the Zariski closure of $\mathbf{\Sigma}$ in $\mathrm{Sh}_K(G,X)$ is irreducible and contained in $S_K(G,X)$.

We will often have an inclusion of Shimura data $(G_1,X_1) \subset (G_2,X_2)$ and a compact open subgroup $K_1 := K_2 \cap G_1(\mathbb{A}_f)$ of $G_1(\mathbb{A}_f)$, where K_2 is a compact open subgroup of $G_2(\mathbb{A}_f)$. We obtain a morphism

$$\phi : \mathrm{Sh}_{K_1}(G_1,X_1) \to \mathrm{Sh}_{K_2}(G_2,X_2)$$

and, by [UYa], Lemma 2.2, if K_2 is neat, ϕ is generically injective. In this case, we will use the same symbol for a subvariety of $\mathrm{Sh}_{K_1}(G_1,X_1)$ and its image in $\mathrm{Sh}_{K_2}(G_2,X_2)$.

7.3 Choosing a measure

Consider a special subvariety V of $S_K(G,X)$. By [UYa], Lemma 2.1, there exists a Shimura subdatum (H,X_H) of (G,X) and a connected component X_H^+ of X_H contained in X^+ such that H is the generic Mumford-Tate group on X_H and V is the image of $X_H^+ \times \{1\}$ in $\mathrm{Sh}_K(G,X)$. We will denote by K_H the intersection $K \cap H(\mathbb{A}_f)$ and by Γ_H the intersection $H(\mathbb{Q})_+ \cap K_H$, where $H(\mathbb{Q})_+$ is the stabiliser of X_H^+ in $H(\mathbb{Q})$. Thus, V is the image of $\Gamma_H \backslash X_H^+$ in

$\mathrm{Sh}_K(G,X)$. We refer to (H,X_H) as the Shimura datum defining V and we say that V is strongly special if the image of H in G^{ad} is semisimple.

The space X_H^+ is isomorphic to $H^{\mathrm{ad}}(\mathbb{R})^+/K_\infty$, where K_∞ is a maximal compact subgroup of $H^{\mathrm{ad}}(\mathbb{R})^+$. Let $\mathfrak{h}$ denote the Lie algebra of $H^{\mathrm{ad}}(\mathbb{R})^+$ and let $\mathfrak{h}^*$ denote the dual of $\mathfrak{h}$. Any real non-zero left-invariant differential form ω of maximal degree r on $H^{\mathrm{ad}}(\mathbb{R})^+$ corresponds to an element of $\bigwedge^r \mathfrak{h}^*$.

Since $\mathfrak{h}$ admits a Cartan decomposition $\mathfrak{k}\oplus\mathfrak{p}$, where $\mathfrak{k}$ is the Lie algebra of K_∞ and $\mathfrak{p}$ is the tangent space of X_H^+ at the point K_∞, we can write $\omega=\omega_{\mathfrak{k}}\wedge\omega_{\mathfrak{p}}$, where $\omega_{\mathfrak{k}}$ and $\omega_{\mathfrak{p}}$ correspond to real multilinear forms on $\mathfrak{k}$ and $\mathfrak{p}$, respectively. In this paper, we will always choose $\omega_{\mathfrak{k}}$ so that, with respect to the measure it determines, the volume of K_∞ is one.

Consider the unique (up to isomorphism) $\mathbb{R}$-anisotropic form H^c of H^{ad} i.e. the real algebraic group H^c isomorphic to H^{ad} over $\mathbb{C}$ such that $H^c(\mathbb{R})$ is compact. Then $H^c(\mathbb{R})$ is a connected maximal compact subgroup of $H^c(\mathbb{C})$ containing a copy of K_∞ and the quotient $\check{X}_H := H^c(\mathbb{R})/K_\infty$ is called the compact dual of X_H^+. It contains X_H^+ as an open subset.

Considering multilinear forms on the complexification $\mathfrak{h}_{\mathbb{C}} := \mathfrak{h}\otimes\mathbb{C}$, ω extends $\mathbb{C}$-linearly to a complex, left-invariant differential form $\omega_{\mathbb{C}}$ on $H^{\mathrm{ad}}(\mathbb{C})$. As in [Mum77], Proportionality Theorem 3.2, the Lie algebra of $H^c(\mathbb{R})$ inside $\mathfrak{h}_{\mathbb{C}}$ is equal to $\mathfrak{k}\oplus i\mathfrak{p}$. We will always choose $\omega_{\mathfrak{p}}$ so that, with respect to the measure determined by $\omega_{\mathbb{C}}$, the volume of $H^c(\mathbb{R})$ or, equivalently, any maximal compact subgroup of $H^{\mathrm{ad}}(\mathbb{C})$, is one. Therefore, the volume of $\check{X}_H$ is also one.

We will denote by μ the Haar measure on $H^{\mathrm{ad}}(\mathbb{R})^+$ determined by ω. We will also denote by μ the volume measure on X_H^+ determined by $\omega_{\mathfrak{p}}$. When we consider the volume measures induced on arithmetic quotients of either $H^{\mathrm{ad}}(\mathbb{R})^+$ or X_H^+ we will again use μ.

7.4 Degrees of strongly special subvarieties

In order to prove Theorem 7.4, we will need the following theorem, relating the degree of a special subvariety to its volume:

Theorem 7.5. *Let (G, X) be a Shimura datum, X^+ a connected component of X, and K a neat compact open subgroup of $G(\mathbb{A}_f)$. There exists a constant c_1 such that, if V is a special subvariety of $S_K(G, X)$, defined by (H, X_H), then*

$$\deg_{\mathcal{L}_K} V > c_1 \cdot \mu(\Gamma_H \backslash X_H^+).$$

By a constant we will always mean a positive real number.

Proof. By [KY], Corollary 5.3.10,

$$\deg_{\mathcal{L}_K} V \geq \deg_{\mathcal{L}_{K_H}} V$$

and, for the remainder of this proof, V will refer to the connected component $\Gamma_H \backslash X_H^+$ of $\mathrm{Sh}_{K_H}(H, X_H)$.

Consider a smooth compactification $\overline{V}^{\mathrm{sm}}$ of V, thus providing a canonical birational map

$$\pi : \overline{V}^{\mathrm{sm}} \to \overline{V},$$

as in the proof of [Mum77], Proposition 3.4 (b). By [KY], Proposition 5.3.2 (1), the exterior product $\Omega^{\dim X_H}$ of the cotangent bundle Ω on X_H descends to $\mathrm{Sh}_{K_H}(H, X_H)$ and extends uniquely to an ample line bundle on $\overline{V}$ (this is the restriction of $\mathcal{L}_{K_H}$). By [Mum77], Proposition 3.4 (b), the pullback $\pi^*\mathcal{L}_{K_H}$ of $\mathcal{L}_{K_H}$ to $\overline{V}^{\mathrm{sm}}$ is the unique extension $\overline{E}$ of [Mum77], Main Theorem 3.1. Of course, $\Omega^{\dim X_H}$ is the restriction of the exterior product $\check{\Omega}^{\dim X_H}$ of the cotangent bundle $\check{\Omega}$ on the compact dual $\check{X}_H$. By [Mum77], Proportionality Theorem 3.2, we have

$$\deg_{\pi^*\mathcal{L}_{K_H}} \overline{V}^{\mathrm{sm}} = (-1)^{\dim X_H} \cdot \mu(\Gamma_H \backslash X_H^+) \cdot \int_{\check{X}_H} c_1(\check{\Omega}^{\dim X_H})^{\dim X_H}.$$

However, since π is birational, the projection formula (see [KY], 5.1) implies that

$$\deg_{\pi^*\mathcal{L}_{K_H}} \overline{V}^{\mathrm{sm}} = \deg_{\mathcal{L}_{K_H}} V.$$

Furthermore, up to isomorphism, the number of Hermitian symmetric spaces corresponding to Shimura subdata of (G, X) is finite. Therefore,

$$(-1)^{\dim X_H} \cdot \int_{\check{X}_H^+} c_1(\check{\Omega}^{\dim X_H})^{\dim X_H},$$

may assume only finitely many positive values.

□

7.5 Volumes of strongly special subvarieties

Now we prove a lower bound for the volume of a strongly special subvariety, concluding the proof of Theorem 7.4. First, however, suppose that G is a reductive group over $\mathbb{Q}$ and L is a finite Galois extension over which G is split. Since almost all places of L are unramified over $\mathbb{Q}$, it follows that $G_{\mathbb{Q}_p}$ is split over an unramified extension for almost all primes p. Furthermore, by

[Spr79], Lemma 4.9 (ii), $G_{\mathbb{Q}_p}$ is quasi-split for almost all primes p. Therefore, we let $\Sigma(G)$ denote the finite set of primes p such that $G_{\mathbb{Q}_p}$ is not unramified.

Now suppose that K is a compact open subgroup of $G(\mathbb{A}_f)$, equal to a product of compact open subgroups $K_p \subset G(\mathbb{Q}_p)$, and fix a faithful representation $G \hookrightarrow \mathrm{GL}_n$. By [KY], 4.1.5, $K_p = G_{\mathbb{Z}_p}(\mathbb{Z}_p)$ for almost all primes p. Thus, by [Tit79], 3.9.1, K_p is hyperspecial for almost all p. Therefore, we let $\Sigma(K)$ denote the finite set of primes p such that K_p is not hyperspecial. Finally, we let $\Sigma(G,K)$ denote the set of primes belonging to either $\Sigma(G)$ or $\Sigma(K)$ and we let $\Pi(G,K)$ denote their product.

Theorem 7.6. *Let (G,X) be a Shimura datum such that $G = G^{\mathrm{ad}}$ and let X^+ be a connected component of X. Fix a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_n$ and let K be a neat compact open subgroup of $G(\mathbb{A}_f)$, equal to a product of compact open subgroups $K_p \subset G(\mathbb{Q}_p)$. There exist positive constants c_2 and δ such that, if V is a strongly special subvariety of $S_K(G,X)$, defined by (H,X_H), then*

$$\mu(\Gamma_H \backslash X_H^+) > c_2 \cdot \Pi(H,K_H)^{\delta}.$$

In the situation described in the theorem, we will use the term uniform to mean depending only on (G,X), K and ρ.

Note that, since K_H is neat, Γ_H injects into $H^{\mathrm{ad}}(\mathbb{R})^+$ and so acts freely on X_H^+. Let $\mathrm{ad} : H \to H^{\mathrm{ad}}$ denote the natural map. Since K_∞ has volume one with respect to the measure determined by $\omega_{\mathfrak{k}}$, we have

$$\mu(\Gamma_H \backslash X_H^+) = \mu(\mathrm{ad}(\Gamma_H) \backslash H^{\mathrm{ad}}(\mathbb{R})^+).$$

Since H is semisimple, we have a central isogeny $\pi : \widetilde{H} \to H$, where $\widetilde{H}$ is simply connected and whose centre we denote $Z_{\widetilde{H}}$. We denote by $Z \subset Z_{\widetilde{H}}$

the kernel of π. Note that, by [Mar91], Proposition 1.4.5, the maximal split tori (resp. parabolic subgroups) of $\widetilde{H}$ are in bijection via this morphism with the maximal split tori (resp. parabolic subgroups) of H. Therefore, $\Sigma(\widetilde{H}) = \Sigma(H)$.

Since π is finite, and therefore proper, $\widetilde{K}_H := \pi_{\mathbb{A}_f}^{-1}(K_H)$ is a compact open subgroup of $\widetilde{H}(\mathbb{A}_f)$ and we let $\widetilde{\Gamma}_H := \widetilde{H}(\mathbb{Q}) \cap \widetilde{K}_H$, which is equal to $\pi^{-1}(\Gamma_H)$. Since K_H is necessarily a product of compact open subgroups $K_{H,p} \subset H(\mathbb{Q}_p)$, $\widetilde{K}_H$ is also a product of compact open subgroups $\widetilde{K}_{H,p} \subset \widetilde{H}(\mathbb{Q}_p)$. Let $K^m_{\widetilde{H}}$ be a maximal compact open subgroup of $\widetilde{H}(\mathbb{A}_f)$ containing $\widetilde{K}_H$ and let $\Gamma^m_{\widetilde{H}} := \widetilde{H}(\mathbb{Q}) \cap K^m_{\widetilde{H}}$. Again $K^m_{\widetilde{H}}$ is a product of maximal compact open subgroups $K^m_{\widetilde{H},p} \subset \widetilde{H}(\mathbb{Q}_p)$.

By [Mil04], Theorem 5.2, $\widetilde{H}(\mathbb{R})$ is connected and so acts on $H^{\mathrm{ad}}(\mathbb{R})^+$ through $\mathrm{ad} \circ \pi$. Therefore, we have two finite projections

$$\mathrm{ad}(\Gamma_H)\backslash H^{\mathrm{ad}}(\mathbb{R})^+ \leftarrow \mathrm{ad} \circ \pi(\widetilde{\Gamma}_H)\backslash H^{\mathrm{ad}}(\mathbb{R})^+ \rightarrow \mathrm{ad} \circ \pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+$$

yielding the equality

$$\mu(\mathrm{ad}(\Gamma_H)\backslash H^{\mathrm{ad}}(\mathbb{R})^+) = \frac{[\mathrm{ad} \circ \pi(\Gamma^m_{\widetilde{H}}) : \mathrm{ad} \circ \pi(\widetilde{\Gamma}_H)]}{[\mathrm{ad}(\Gamma_H) : \mathrm{ad} \circ \pi(\widetilde{\Gamma}_H)]} \cdot \mu(\mathrm{ad} \circ \pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+).$$

Lemma 7.7. *There exists a uniform constant c_3 such that the index*

$$[\mathrm{ad} \circ \pi(\Gamma^m_{\widetilde{H}}) : \mathrm{ad} \circ \pi(\widetilde{\Gamma}_H)]$$

is greater than $c_3[K^m_{\widetilde{H}} : \widetilde{K}_H]$.

Proof. Consider the surjective map

$$\Gamma^m_{\widetilde{H}} \rightarrow \mathrm{ad} \circ \pi(\Gamma^m_{\widetilde{H}})/\mathrm{ad} \circ \pi(\widetilde{\Gamma}_H).$$

Since $\widetilde{\Gamma}_H = \pi^{-1}(\Gamma_H)$, the kernel is equal to

$$(\mathrm{ad} \circ \pi)^{-1}(\mathrm{ad} \circ \pi(\pi^{-1}(\Gamma_H))) \cap \Gamma^m_{\widetilde{H}},$$

which is readily seen to be $Z_{\widetilde{H}}(\mathbb{Q}) \cdot \pi^{-1}(\Gamma_H)$. Since the order of $Z_{\widetilde{H}}$ is uniformly bounded by the proof of [UYa], Lemma 2.4, we turn our attention to the index $[\Gamma^m_{\widetilde{H}} : \widetilde{\Gamma}_H]$. Write

$$K^m_{\widetilde{H}} = \coprod_{i=1}^{n} k_i \widetilde{K}_H,$$

where $k_i \in K^m_{\widetilde{H}}$. By strong approximation (as in [Mil04], Theorem 4.16), applied to $\widetilde{H}$, each k_i can be written as $q_i k_i'$, where $q_i \in \widetilde{H}(\mathbb{Q})$ and $k_i' \in \widetilde{K}_H$. Therefore, in the above, we may replace k_i with q_i. Intersecting both sides with $\widetilde{H}(\mathbb{Q})$ we obtain

$$\Gamma^m_{\widetilde{H}} = \coprod_{i=1}^{n} q_i \widetilde{\Gamma}_H,$$

and so $q_i \in \Gamma^m_{\widetilde{H}}$. □

Lemma 7.8. *There exist uniform constants c_4 and C such that*

$$[\mathrm{ad}(\Gamma_H) : \mathrm{ad} \circ \pi(\widetilde{\Gamma}_H)] < c_4 C^{|\Sigma(H,K_H)|}.$$

Proof. Consider the surjective map

$$\Gamma_H \to \mathrm{ad}(\Gamma_H)/\mathrm{ad} \circ \pi(\widetilde{\Gamma}_H).$$

The kernel is equal to

$$\mathrm{ad}^{-1}(\mathrm{ad} \circ \pi(\widetilde{\Gamma}_H)) \cap \Gamma_H,$$

which is readily seen to be

$$(\pi(\widetilde{\Gamma}_H)\cdot Z_H(\mathbb{Q}))\cap\Gamma_H=\pi(\widetilde{\Gamma}_H)\cdot(Z_H(\mathbb{Q})\cap\Gamma_H)=\pi(\widetilde{\Gamma}_H),$$

where Z_H is the centre of H (using the fact that Γ_H is neat). Therefore, we turn our attention to the index $[\Gamma_H:\pi(\widetilde{\Gamma}_H)]$.

Recall that Galois cohomology yields an exact sequence

$$\widetilde{H}(\mathbb{Q})\to H(\mathbb{Q})\to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),Z(\overline{\mathbb{Q}})).$$

Therefore, the quotient $\pi(\widetilde{\Gamma}_H)\backslash\Gamma_H$ embeds as a subgroup of the Abelian group $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),Z(\overline{\mathbb{Q}}))$. On the other hand, $\pi(\widetilde{\Gamma}_H)\backslash\Gamma_H$ embeds into

$$\pi(\widetilde{K}_H)\backslash K_H=\prod_p\pi(\widetilde{K}_{H,p})\backslash K_{H,p}$$

and, again, Galois cohomology tells us that

$$\pi(\widetilde{K}_{H,p})\backslash K_{H,p}\hookrightarrow H^1(\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p),Z(\overline{\mathbb{Q}_p})).$$

However, now consider a prime p such that $H_{\mathbb{Q}_p}$ is unramified and $K_{H,p}$ is hyperspecial. Since $\widetilde{H}_{\mathbb{Q}_p}$ is also unramified, $\widetilde{H}(\mathbb{Q}_p)$ also possesses hyperspecial subgroups by [Tit79], 3.8.2. Therefore, by [Tit79], 3.8.1, there exist smooth reductive group schemes $\widetilde{\mathbf{H}}$ and $\mathbf{H}$ over $\mathbb{Z}_p$, the generic fibres of which are $\widetilde{H}_{\mathbb{Q}_p}$ and $H_{\mathbb{Q}_p}$, such that $K_{H,p}=\mathbf{H}(\mathbb{Z}_p)$ and $\widetilde{\mathbf{H}}(\mathbb{Z}_p)$ is a hyperspecial subgroup of $\widetilde{H}(\mathbb{Q}_p)$. By [Vas12], Lemma 2.3.1, the central isogeny $\pi_{\mathbb{Q}_p}$ extends uniquely to a central isogeny $\pi_{\mathbb{Z}_p}:\widetilde{\mathbf{H}}\to\mathbf{H}$. Therefore, the kernel $\mathbf{Z}$ of $\pi_{\mathbb{Z}_p}$ is a finite group scheme of multiplicative type such that $\mathbf{Z}_{\mathbb{Q}_p}=Z_{\mathbb{Q}_p}$. Over a finite Galois extension F of $\mathbb{Q}$, Z_F is isomorphic to a product of roots of unity, whose orders we denote $n_1,...,n_r$. Therefore, by [DG63], Exposé X, Lemme 4.1, if p is coprime to the n_i, $\mathbf{Z}_{\mathbb{F}_p}$ is smooth.

Therefore, by [PR91], Lemma 6.5, for any prime $p \notin \Sigma(H, K_H)$ and coprime to the n_i, we have an exact sequence

$$\widetilde{\mathbf{H}}(\mathbb{Z}_p) \to \mathbf{H}(\mathbb{Z}_p) \to H^1(\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/\mathbb{Q}_p), \mathbf{Z}(\mathbb{Z}_p^{\mathrm{un}})),$$

where $\mathbb{Q}_p^{\mathrm{un}}$ is the maximal unramified extension of $\mathbb{Q}_p$ and $\mathbb{Z}_p^{\mathrm{un}}$ is its ring of integers. However, since $\widetilde{K}_{H,p}$ clearly contains $\widetilde{\mathbf{H}}(\mathbb{Z}_p)$ and, by [Tit79], 3.8.2, $\widetilde{\mathbf{H}}(\mathbb{Z}_p)$ is maximal among compact subgroups of $\widetilde{H}(\mathbb{Q}_p)$, we have $\widetilde{\mathbf{H}}(\mathbb{Z}_p) = \widetilde{K}_{H,p}$.

The degree $[F : \mathbb{Q}]$ is bounded by the degree of the splitting field of any torus containing Z, which we have seen is uniformly bounded. By the proof of [UYa], Lemma 2.4, the order of Z is also bounded by a uniform constant and so the same can be said of $|H^1(\mathrm{Gal}(F/\mathbb{Q}), Z(F))|$. Therefore, we may consider the image of $\pi(\widetilde{\Gamma}_H)\backslash\Gamma_H$ in $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/F), Z(\overline{\mathbb{Q}}))$, whose image in $H^1(\mathrm{Gal}(\overline{\mathbb{Q}_p}/F_v), Z(\overline{\mathbb{Q}_p}))$ is contained in $H^1(\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/F_v), \mathbf{Z}(\mathbb{Z}_p^{\mathrm{un}}))$ for all places v of F lying above a prime $p \notin \Sigma(H, K_H)$ coprime to the n_i.

We identify the three previous cohomology groups with the groups

$$\prod_{i=1}^{r} (F^*)^{n_i}\backslash F^*, \ \prod_{i=1}^{r} (F_v^*)^{n_i}\backslash F_v^* \text{ and } \prod_{i=1}^{r} (\mathcal{O}_{F_v}^*)^{n_i}\backslash \mathcal{O}_{F_v}^*$$

and choose a uniformiser $\xi_v \in F$ at each place v lying above a prime $p \in \Sigma(H, K_H)$ or dividing one of the n_i. Therefore, the image of

$$\pi(\widetilde{\Gamma}_H)\backslash\Gamma_H \to \prod_{i=1}^{r} (F^*)^{n_i}\backslash F^*$$

is contained in the subgroup generated by $\mathcal{O}_F^*$ and the ξ_v. Now, $\mathcal{O}_F^*$ is a finitely generated Abelian group whose rank and torsion subgroup are uniformly bounded and, since the n_i are bounded by the order of Z, we are done.

□

We now appeal to Prasad's formula.

Lemma 7.9. *There exist uniform constants c_5 and δ_1 such that*

$$\mu(\mathrm{ad}\circ\pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+) > c_5 \cdot \Pi(\widetilde{H}, K^m_{\widetilde{H}})^{\delta_1}.$$

Proof. Let $\widetilde{\omega} := \frac{1}{|Z_{\widetilde{H}}|}\omega^*$, where ω^* is the pullback of ω to $\widetilde{H}(\mathbb{R})$. Denote by $\widetilde{\mu}$ the measure determined by $\widetilde{\omega}$ on $\widetilde{H}(\mathbb{R})$ and its arithmetic quotients. By [Mil04], Proposition 5.1, $\widetilde{H}(\mathbb{R}) \to H^{\mathrm{ad}}(\mathbb{R})^+$ is surjective. On the other hand, the kernel of the map

$$\Gamma^m_{\widetilde{H}}\backslash\widetilde{H}(\mathbb{R}) \to \mathrm{ad}\circ\pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+$$

is $\Gamma^m_{\widetilde{H}} \cap Z_{\widetilde{H}}(\mathbb{R})\backslash Z_{\widetilde{H}}(\mathbb{R})$. It follows from the proof of [UYa], Lemma 2.4 that

$$\frac{\mu(\mathrm{ad}\circ\pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+)}{\widetilde{\mu}(\Gamma^m_{\widetilde{H}}\backslash\widetilde{H}(\mathbb{R}))}$$

is greater than a uniform constant.

Since $\widetilde{H}$ is simply connected, it is a direct product $H_1 \times \cdots \times H_s$ of quasi-simple, simply connected subgroups. We can write $\widetilde{\omega} = \omega_1 \wedge \cdots \wedge \omega_s$, where ω_i is a real non-zero left-invariant differential form of maximal degree on $H_i(\mathbb{R})$. Since $\mathrm{ad}\circ\pi$ is surjective, degree $|Z_{\widetilde{H}}|$ and proper, the preimage of a maximal compact subgroup of $H^{\mathrm{ad}}(\mathbb{C})$ is a maximal compact subgroup of $\widetilde{H}(\mathbb{C})$, whose volume with respect to the measure determined by $\widetilde{\omega}_{\mathbb{C}}$ is one. The ω_i are, therefore, determined up to multiplication by a non-zero multiplicative constant. We choose this constant so that the volume of any maximal compact subgroup of $H_i(\mathbb{C})$ is also one. We denote the measures determined on the $H_i(\mathbb{R})$ by μ_i. Since $K^m_{\widetilde{H}}$ is maximal, it is a product of maximal compact open subgroups $K^m_{H_i} \subset H_i(\mathbb{A}_f)$, each a product of maximal compact open subgroups $K^m_{H_i,p} \subset H_i(\mathbb{Q}_p)$. Hence,

$$\widetilde{\mu}(\Gamma^m_{\widetilde{H}} \backslash \widetilde{H}(\mathbb{R})) = \prod_{i=1}^{s} \mu_i(\Gamma^m_{H_i} \backslash H_i(\mathbb{R})),$$

where $\Gamma^m_{H_i} := H_i(\mathbb{Q}) \cap K^m_{H_i}$.

By [Vas07], 3.3, each H_i is of the form $\mathrm{Res}_{K_i/\mathbb{Q}} H'_i$, where K_i is a totally real number field and H'_i is a simply connected absolutely quasi-simple group. Now,

$$H_i(\mathbb{Q}_p) = \mathrm{Res}_{K_i/\mathbb{Q}} H'_i(\mathbb{Q}_p) = H'_i(K_i \otimes_{\mathbb{Q}} \mathbb{Q}_p) = \prod_{v|p} H'_i(K_{i,v}),$$

where the product runs over the places v of K_i lying above p and $K_{i,v}$ is the completion of K_i with respect to the valuation determined by v. Thus, $K^m_{H_i,p}$ is a product of maximal compact open subgroups $K^m_{H'_i,v} \subset H'_i(K_{i,v})$.

Since $H_i(\mathbb{R}) = \prod_{v|\infty} H'_i(K_{i,v})$, we can write $\omega_i = \wedge_{v|\infty} \omega_{i,v}$, where $\omega_{i,v}$ is a real non-zero left-invariant differential form of maximal degree on $H'_i(K_{i,v})$. We choose the $\omega_{i,v}$ so that the volume of any maximal compact subgroup of $H'_i(\mathbb{C})$ is one. Note that, by [Pra89], 3.5, for each archimedean place v of K_i, the Haar measure $\mu_{i,v}$ determined by $\omega_{i,v}$ on $H'_i(\mathbb{R})$ is precisely that defined in loc. cit. 3.6. Therefore, by loc. cit. Theorem 3.7, $\mu_i(\Gamma^m_{H_i} \backslash H_i(\mathbb{R}))$ is equal to

$$D_{K_i}^{\frac{1}{2}\dim H'_i} \cdot |N_{K_i/\mathbb{Q}}(\Delta_{L_i/K_i})|^{\frac{s_i}{2}} \cdot \left(\prod_{j=1}^{r_i} \frac{m_{i,j}!}{(2\pi)^{m_{i,j}+1}} \right)^{[K_i:\mathbb{Q}]} \cdot \tau_{K_i}(H'_i) \cdot \xi_i,$$

where

- D_{K_i} is the absolute value of $\mathrm{disc}(K_i)$.

- L_i is the splitting field of the quasi-split inner form $\mathcal{H}_i$ of H_i'.
- $N_{K_i/\mathbb{Q}}$ is the norm on K_i.
- Δ_{L_i/K_i} is the relative discriminant of L_i over K_i.
- s_i is the integer defined in [Pra89], 0.4.
- r_i is the absolute rank of $\mathcal{H}_i$.
- The $m_{i,j}$ are the exponents of the simple, simply connected, compact, real-analytic Lie group of the same type as $\mathcal{H}_i$.
- $\tau_{K_i}(H_i') = 1$ is the Tamagawa number of H_i' (see [Pra89], 3.3).
- ξ_i is the product, over all finite places v of K_i, of local factors $\xi_{i,v}$.

Note first that $\dim H_i'$, s_i, r_i, the $m_{i,j}$ and $[K_i : \mathbb{Q}]$ are all positive integers, with the possible exception of s_i when $L_i = K_i$, in which case it becomes irrelevant. It is also worth noting that they are all uniformly bounded.

Recall that Δ_{L_i/K_i} is an ideal in $\mathcal{O}_{K_i}$ with the property that the prime ideals dividing it are precisely those that ramify in $\mathcal{O}_{L_i}$ i.e. those places v of K_i such that $\mathcal{H}_{i,K_{i,v}}$ does not split over an unramified extension of $K_{i,v}$. Its norm $N_{K_i/\mathbb{Q}}(\Delta_{L_i/K_i})$ is divisible by precisely those primes p such that there exists v lying above p and dividing Δ_{L_i/K_i}.

By [Pra89], 2.10, $\xi_{i,v} > 1$ for all non-archimedean places v of K_i. Furthermore, if $H'_{i,K_{i,v}}$ is not quasi-split, $K^m_{H_i',v}$ is not special, or $H'_{i,K_{i,v}}$ splits over an unramified extension of $K_{i,v}$ and $K^m_{H_i',v}$ is not hyperspecial, then

$$\xi_{i,v} \geq q_{i,v}^{r_{i,v}+1} \cdot (q_{i,v} + 1)^{-1},$$

where $q_{i,v}$ is the cardinality of the residue field $k_{i,v}$ of $K_{i,v}$ and $r_{i,v} \geq 1$ is the rank of $\mathcal{H}_{i,K_{i,v}}$ over the maximal unramified extension of $K_{i,v}$. Therefore, let Σ_i be the set of primes p such that, for some place v of K_i lying above p, either $H'_{i,K_{i,v}}$ is not quasi-split, $H'_{i,K_{i,v}}$ does not split over an unramified extension of $K_{i,v}$, or $K^m_{H'_i,v}$ is not a hyperspecial subgroup of $H'_i(K_{i,v})$. Then there exist uniform constants c_6 and δ_2 such that

$$\mu_i(\Gamma^m_{H_i}\backslash H_i(\mathbb{R})) > c_6 D_{K_i}^{\frac{1}{2}\dim H'_i} \cdot \prod_{p\in\Sigma_i} p^{\delta_2}.$$

However, recall that

$$H_{i,\mathbb{Q}_p} = \prod_{v|p} \mathrm{Res}_{K_{i,v}/\mathbb{Q}_p} H'_{i,K_{i,v}}.$$

Therefore, by [BT65], 6.19, the set $\Sigma(H_i)$ is contained in the union of Σ_i and the set of primes p dividing D_{K_i}. On the other hand, suppose that $K^m_{H'_i,v}$ is a hyperspecial subgroup of $H'_i(K_{i,v})$ for each place v of K_i lying above a prime p. For each such subgroup, there exists a smooth group scheme $\mathbf{H}'_{i,\mathcal{O}_{K_{i,v}}}$ over $\mathcal{O}_{K_{i,v}}$, with generic fibre $H'_{i,K_{i,v}}$, such that $\mathbf{H}'_{i,k_{i,v}}$ is reductive and $\mathbf{H}'_{i,\mathcal{O}_{k_{i,v}}}(\mathcal{O}_{K_{i,v}})$ is equal to $K^m_{H'_i,v}$. Let

$$\mathbf{H}_{i,\mathbb{Z}_p} := \prod_{v|p} \mathrm{Res}_{\mathcal{O}_{K_{i,v}}/\mathbb{Z}_p} \mathbf{H}'_{i,\mathcal{O}_{K_{i,v}}}.$$

Then, the generic fibre of $\mathbf{H}_{i,\mathbb{Z}_p}$ is $H_{i,\mathbb{Q}_p}$ and $\mathbf{H}_{i,\mathbb{Z}_p}(\mathbb{Z}_p) = K^m_{H_i,p}$. Furthermore, if p does not divide D_{K_i}, then

$$\mathbf{H}_{i,\mathbb{F}_p} = \prod_{v|p} \mathrm{Res}_{\mathcal{O}_{K_{i,v}}\otimes_{\mathbb{Z}_p}\mathbb{F}_p/\mathbb{F}_p} \mathbf{H}'_{i,\mathcal{O}_{K_{i,v}}\otimes_{\mathbb{Z}_p}\mathbb{F}_p} = \prod_{v|p} \mathrm{Res}_{k_{i,v}/\mathbb{F}_p} \mathbf{H}'_{i,k_{i,v}}$$

is a reductive group over $\mathbb{F}_p$. Therefore, the set $\Sigma(K^m_{H_i})$ is also contained in the union of Σ_i and the set of primes p dividing D_{K_i}, from which we conclude there exists a uniform constant δ_3 such that

$$\mu_i(\Gamma^m_{H_i}\backslash H_i(\mathbb{R})) > c_6 \cdot \Pi(H_i, K^m_{H_i})^{\delta_3}.$$

However, the union of the $\Sigma(H_i)$ is equal to $\Sigma(H)$ and the union of the $\Sigma(K^m_{H_i})$ is equal to $\Sigma(K^m_{\widetilde{H}})$.

□

We will require the following lemma in the proof of Lemma 7.11 and also to obtain suitable Hecke correspondences:

Lemma 7.10. *Let T be a maximal torus of $H_{\mathbb{Q}_p}$. There exists a basis of $X^*(T)$ such that the coordinates of the characters of T intervening in $\overline{\mathbb{Q}}_p^n$ are bounded in absolute value by a uniform constant.*

Proof. By [CU06], Proposition 2.1, since H is the generic Mumford-Tate group on X_H, there exists a dense set of special points X'_H in X_H such that, for $x \in X'_H$, the Mumford-Tate group $\mathrm{MT}(x)$ of x is a maximal torus in H. Choose an $x \in X'_H$ and let $M := \mathrm{MT}(x)$. Denote by L the splitting field of M and by R_L the torus $\mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_{m,L}$.

The reciprocity morphism $r_x : R_L \to M$ corresponding to x is surjective and induces an embedding

$$X^*(M) \hookrightarrow X^*(R_L).$$

Enumerate the elements $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, thereby producing a basis $\mathcal{B} := \{b_\sigma\}$ of $X^*(R_L)$. By [Yaf06], Section 2, with respect to this basis, the characters of M intervening in $\overline{\mathbb{Q}}^n$ have coordinates bounded in absolute value by a uniform constant.

Since any two maximal tori of $H_{\overline{\mathbb{Q}}_p}$ are conjugate by an element of $H(\overline{\mathbb{Q}}_p)$, we may conjugate $r_{x,\overline{\mathbb{Q}}_p}$ by an element of $H(\overline{\mathbb{Q}}_p)$ to obtain a surjective morphism $r'_{x,\overline{\mathbb{Q}}_p} : R_{L,\overline{\mathbb{Q}}_p} \to T_{\overline{\mathbb{Q}}_p}$. Thus, we obtain an embedding

$$X^*(T_{\overline{\mathbb{Q}}_p}) \hookrightarrow X^*(R_{L,\overline{\mathbb{Q}}_p})$$

such that, with respect to the basis $\mathcal{B}$, the coordinates of the characters of T intervening in $\overline{\mathbb{Q}}_p^n$ are uniformly bounded in absolute value. Since our representation was faithful, these characters generate $X^*(T_{\overline{\mathbb{Q}}_p})$ and so there are only finitely many possibilities for this submodule of $X^*(R_{L,\overline{\mathbb{Q}}_p})$. For each such possibility, choose a basis for $X^*(T_{\overline{\mathbb{Q}}_p})$ and consider the maximum of the absolute values of the coordinates of the characters intervening in $\overline{\mathbb{Q}}_p^n$ with respect to these bases.

□

Lemma 7.11. *There exist uniform constants c_7 and c_8 such that, for any $p \notin \Sigma(\widetilde{H}, K^m_{\widetilde{H}})$ greater than c_7, such that $\widetilde{K}_{H,p} \subsetneq K^m_{\widetilde{H},p}$,*

$$[K^m_{\widetilde{H},p} : \widetilde{K}_{H,p}] > c_8 p.$$

Proof. We will imitate the proof of [UYa], Proposition 3.15. Since $K^m_{\widetilde{H},p}$ is hyperspecial and $H_{\mathbb{Q}_p}$ is unramified, there exist smooth reductive group schemes $\widetilde{\mathbf{H}}$ and $\mathbf{H}$ over $\mathbb{Z}_p$, the generic fibres of which are $\widetilde{H}_{\mathbb{Q}_p}$ and $H_{\mathbb{Q}_p}$, such that $K^m_{\widetilde{H},p} = \widetilde{\mathbf{H}}(\mathbb{Z}_p)$. By [Vas12], Lemma 2.3.1, the central isogeny $\pi_{\mathbb{Q}_p}$ extends uniquely to a central isogeny $\pi_{\mathbb{Z}_p} : \widetilde{\mathbf{H}} \to \mathbf{H}$ and we denote the kernel $\mathbf{Z}$.

The map

$$\widetilde{K}_{H,p} \backslash \widetilde{\mathbf{H}}(\mathbb{Z}_p) \to K_{H,p} \backslash \mathbf{H}(\mathbb{Z}_p)$$

is injective. However, recall from the proof of Lemma 7.8 that the cokernel is no larger than $H^1(\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/\mathbb{Q}_p), \mathbf{Z}(\mathbb{Z}_p^{\mathrm{un}}))$. Furthermore, if F is the splitting field of Z and v is a place of F lying above p, the kernel of the restriction map to $H^1(\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/F_v), \mathbf{Z}(\mathbb{Z}_p^{\mathrm{un}}))$ is uniformly bounded. However, as we have seen, $H^1(\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/F_v), \mathbf{Z}(\mathbb{Z}_p^{\mathrm{un}}))$ is itself uniformly bounded. Therefore, it suffices to show there exist uniform constants c_7 and c_8 such that $[\mathbf{H}(\mathbb{Z}_p) : K_{H,p}] > c_8 p$, whenever $p > c_7$.

Let $\mathbf{T}$ be a maximal torus of $\mathbf{H}$. The group $(K_{H,p} \cap \mathbf{T}(\mathbb{Z}_p))\backslash\mathbf{T}(\mathbb{Z}_p)$ is a subset of $K_{H,p}\backslash\mathbf{H}(\mathbb{Z}_p)$ and so a lower bound for the size of this group would suffice. Let T denote the generic fibre of $\mathbf{T}$ and note that, by [Tit79], 3.8.2, the hyperspecial subgroup $\mathbf{T}(\mathbb{Z}_p)$ is the maximal compact subgroup of $T(\mathbb{Q}_p)$. Therefore, if $K_p = G_{\mathbb{Z}_p}(\mathbb{Z}_p)$, a condition satisfied for all primes p greater than a uniform constant, $T_{\mathbb{Z}_p}$ is only a torus if

$$K_{T,p} := \mathrm{GL}_n(\mathbb{Z}_p) \cap T(\mathbb{Q}_p) = K_{H,p} \cap T(\mathbb{Q}_p) = K_{H,p} \cap \mathbf{T}(\mathbb{Z}_p)$$

is equal to $\mathbf{T}(\mathbb{Z}_p)$.

We claim that it is possible to choose $\mathbf{T}$ such that $T_{\mathbb{Z}_p}$ is not a torus. In particular, since, by [DG63], Exposé XXII, Section 8, every semisimple element of $\mathbf{H}$ is contained in a maximal torus, we are claiming that $\mathbf{H}(\mathbb{Z}_p)\setminus K_{H,p}$ contains a semisimple element. To see this, note that, by [DG63], Exposé XXII, Corollaire 1.10, the functor of maximal tori of $\mathbf{H}$ is representable by $\mathbf{H}/\mathbf{N}$, where $\mathbf{N}$ is the normaliser of a maximal torus in $\mathbf{H}$. By the paragraph following [DG63], Exposé XXII, Lemme 4.5, and by [DG63], Exposé XXI, Proposition 5.9, the universal maximal torus $\underline{\mathbf{T}}$ of $\mathbf{H}$ (see [DG63], Exposé XXII, Section 8) has the same dimension as $\mathbf{H}$. However, the morphism $u : \underline{\mathbf{T}} \to \mathbf{H}$ is quasi-finite. Hence, by [DG63], Exposé XXII, Proposition

8.1, the semisimple elements of $\mathbf{H}$ constitute a constructible set of dimension $\dim \mathbf{H}$, which therefore contains a Zariski open set. On the other hand, $\mathbf{H}(\mathbb{Z}_p) \setminus K_{H,p}$ is open in $\mathbf{H}(\mathbb{Z}_p)$ for the p-adic topology and so the claim follows.

By [PR91], 3.3, p134, every maximal compact subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$ is conjugate to $\mathrm{GL}_n(\mathbb{Z}_p)$ by an element of $\mathrm{GL}_n(\mathbb{Q}_p)$. Hence, there exists a $g \in \mathrm{GL}_n(\mathbb{Q}_p)$ such that

$$\mathbf{T}(\mathbb{Z}_p) = g\mathrm{GL}_n(\mathbb{Z}_p)g^{-1} \cap T(\mathbb{Q}_p).$$

We let T_0 denote $g^{-1}Tg$. Hence, $\mathrm{GL}_n(\mathbb{Z}_p) \cap T_0(\mathbb{Q}_p)$ is a maximal compact open subgroup $K^m_{T_0,p}$ of $T_0(\mathbb{Q}_p)$ and, since $K_{T,p} = \mathrm{GL}_n(\mathbb{Z}_p) \cap T(\mathbb{Q}_p)$, conjugation by g^{-1} establishes a bijection

$$K_{T,p} \backslash \mathbf{T}(\mathbb{Z}_p) \leftrightarrow (g^{-1}\mathrm{GL}_n(\mathbb{Z}_p)g \cap T_0(\mathbb{Q}_p)) \backslash K^m_{T_0,p}.$$

The latter index is the size of the orbit $K^m_{T_0,p} \cdot g^{-1}\mathbb{Z}_p^n$ in the space of lattices of $\mathbb{Q}_p^n$. Note that $K^m_{T_0,p} = T_{0,\mathbb{Z}_p}(\mathbb{Z}_p)$. Since T splits over an unramified extension of $\mathbb{Q}_p$, so too does T_0 and so, by [Tit79], 3.8.2, $K^m_{T_0,p}$ is a hyperspecial subgroup. Therefore, $T_{0,\mathbb{Z}_p}$ is a torus.

By [DG63], Exposé X, Lemme 4.1, there is a canonical isomorphism

$$X^*(T_{0,\overline{\mathbb{Q}}_p}) \cong X^*(T_{0,\overline{\mathbb{F}}_p})$$

identifying the characters intervening in $\overline{\mathbb{Q}}_p^n$ and $\overline{\mathbb{F}}_p^n$. Thus, with respect to the image of the basis obtained using Lemma 7.10, the coordinates of the characters of $T_{0,\mathbb{F}_p}$ intervening in $\overline{\mathbb{F}}_p^n$ are bounded in absolute value by a uniform constant.

Therefore, by [EY03], Lemma 4.4.1, for all subspaces W of $\overline{\mathbb{F}}_p^n$, the group of connected components of the stabiliser of W in $T_{0,\overline{\mathbb{F}}_p}$ is of order bounded by a uniform constant. Since $T_{\mathbb{Z}_p}$ is not a torus, $T_{0,\mathbb{Z}_p}$ does not fix the lattice $g^{-1}\mathbb{Z}_p^n$ in the sense of [EY03], Section 3.3. Therefore, [EY03], Proposition 4.3.9 implies that there exists a uniform constant c_8 such that the size of the orbit $T_{0,\mathbb{Z}_p}(\mathbb{Z}_p) \cdot g^{-1}\mathbb{Z}_p^n$ is greater than $c_8 p$.

□

Lemma 7.12. *There exists a uniform constant c_9 such that, if $p \notin \Sigma(\widetilde{H}, \widetilde{K}_H)$ is a prime greater than c_9, then $p \notin \Sigma(H, K_H)$.*

Proof. Since $H_{\mathbb{Q}_p}$ is unramified and $\widetilde{K}_{H,p}$ is hyperspecial, there exist smooth reductive group schemes $\widetilde{\mathbf{H}}$ and $\mathbf{H}$ over $\mathbb{Z}_p$, the generic fibres of which are $\widetilde{H}_{\mathbb{Q}_p}$ and $H_{\mathbb{Q}_p}$, such that $\widetilde{K}_{H,p} = \widetilde{\mathbf{H}}(\mathbb{Z}_p)$. By [Vas12], Lemma 2.3.1, the central isogeny $\pi_{\mathbb{Q}_p}$ extends uniquely to a central isogeny $\pi_{\mathbb{Z}_p} : \widetilde{\mathbf{H}} \to \mathbf{H}$.

Let $K_{H,p}^m$ be a maximal compact open subgroup containing $K_{H,p}$. Therefore, $K_{H,p}^m$ contains the image of $\widetilde{K}_{H,p}$. Since, by [Tit79], 3.8.2, $\widetilde{K}_{H,p}$ is maximal, [Oh01], Proposition 3.3 implies that $K_{H,p}^m = \mathbf{H}(\mathbb{Z}_p)$.

Since $\widetilde{K}_{H,p} = \widetilde{\mathbf{H}}(\mathbb{Z}_p)$, the map

$$\widetilde{\mathbf{H}}(\mathbb{Z}_p) \to K_{H,p} \backslash \mathbf{H}(\mathbb{Z}_p)$$

is trivial and we have seen that the cokernel is uniformly bounded. On the other hand, the proof of Lemma 7.11 shows that, if p is greater than a uniform constant and $K_{H,p} \subsetneq \mathbf{H}(\mathbb{Z}_p)$, then $[\mathbf{H}(\mathbb{Z}_p) : K_{H,p}]$ is at least a uniform constant times p. □

Proof. (Theorem 7.6) Recall that

$$\mu(\Gamma_H\backslash X_H^+) = \frac{[\mathrm{ad}\circ\pi(\Gamma^m_{\widetilde{H}}) : \mathrm{ad}\circ\pi(\widetilde{\Gamma}_H)]}{[\mathrm{ad}(\Gamma_H) : \mathrm{ad}\circ\pi(\widetilde{\Gamma}_H)]}\cdot\mu(\mathrm{ad}\circ\pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+).$$

Therefore, by Lemma 7.7 and 7.8, we have

$$\mu(\Gamma_H\backslash X_H^+) > c_3c_4^{-1}C^{-|\Sigma(H,K_H)|}\cdot[K^m_{\widetilde{H}} : \widetilde{K}_H]\cdot\mu(\mathrm{ad}\circ\pi(\Gamma^m_{\widetilde{H}})\backslash H^{\mathrm{ad}}(\mathbb{R})^+),$$

so, by Lemma 7.9,

$$\mu(\Gamma\backslash X_H^+) > c_3c_4^{-1}c_5C^{-|\Sigma(H,K_H)|}\cdot[K^m_{\widetilde{H}} : \widetilde{K}_H]\cdot\Pi(\widetilde{H},K^m_{\widetilde{H}})^{\delta_1}.$$

Lemma 7.11 implies that there exist uniform constants c_{10} and δ_4 such that

$$\mu(\Gamma\backslash X_H^+) > c_{10}C^{-|\Sigma(H,K_H)|}\cdot\Pi(\widetilde{H},\widetilde{K}_H)^{\delta_4}.$$

Therefore, the result follows from Lemma 7.12.

□

Proof. (Theorem 7.4) Follows from Theorem 7.5 and Theorem 7.6. □

7.6 Choosing a suitable Hecke correspondence

In this section, we prove an analogue of [KY], Theorem 8.1, demonstrating the existence of suitable Hecke correspondences. Recall that, if (G,X) is a Shimura datum, G^{ad} decomposes into a product of simple factors, which we denote G_i. Thus, X^{ad} decomposes into a product of factors X_i and, if X^+ is a connected component of X, then it decomposes into a product of factors X_i^+. If the image K^{ad} of K in $G^{\mathrm{ad}}(\mathbb{A}_f)$ is equal to a product of compact open subgroups $K_i\subset G_i(\mathbb{A}_f)$, then $S_{K^{\mathrm{ad}}}(G^{\mathrm{ad}},X^{\mathrm{ad}})$ is equal to the product of the $S_{K_i}(G_i,X_i)$. If K is a compact open subgroup of $G(\mathbb{A}_f)$ we will use the notation K^p to denote the product $\prod_{l\neq p}K_l$.

Theorem 7.13. *Let (G', X') be a Shimura datum such that $G' = G'^{\mathrm{ad}}$, let K' be a neat compact open subgroup of $G'(\mathbb{A}_f)$, equal to a product of compact open subgroups $K'_p \subset G'(\mathbb{Q}_p)$, and fix a faithful representation*

$$\rho : G' \hookrightarrow \mathrm{GL}_n.$$

There exist positive integers k and f such that, if V is a strongly special subvariety of $S_{K'}(G', X')$, defined by (H, X_H), $p \notin \Sigma(H, K_H)$ is a prime such that $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and (G, X) is a Shimura subdatum of (G', X') such that V is contained in $S_K(G, X)$, where $K := K' \cap G(\mathbb{A}_f)$, then there exist a compact open subgroup

$$I_p \subset K_p := K'_p \cap G(\mathbb{Q}_p)$$

and an element $\alpha \in G(\mathbb{Q}_p)$ such that

- $[K_p : I_p] \leq p^f$.
- *If $I \subset K$ is the compact open subgroup $K^p I_p \subset G(\mathbb{A}_f)$,*

  $$\tau : \mathrm{Sh}_I(G, X) \to \mathrm{Sh}_K(G, X)$$

  is the natural morphism, and $\widetilde{V} \subset S_I(G, X)_{\mathbb{C}}$ is an irreducible component of $\tau^{-1}(V)$, then $\widetilde{V} \subset T_\alpha(\widetilde{V})$.
- *For every $k_1, k_2 \in I_p$, the image of $k_1 \alpha k_2$ generates an unbounded subgroup of $G_i(\mathbb{Q}_p)$ for each i.*
- $[I_p : I_p \cap \alpha I_p \alpha^{-1}] < p^k$.

In the situation described in the theorem, we will use the term uniform to mean depending only on (G', X'), K' and ρ. Firstly, we will deal with the matter of including a strongly special subvariety in its image under a Hecke correspondence:

Lemma 7.14. *There exists a uniform integer A such that, for any $\alpha \in H(\mathbb{A}_f)$,*

$$V \subset T_{\alpha^A}(V).$$

Proof. By definition, V is the image of $X_H^+ \times \{1\}$ in $\mathrm{Sh}_K(G, X)$. Thus, consider a point $\overline{(x, 1)} \in V$ with $x \in X_H^+$. Let

$$\pi : \widetilde{H} \to H$$

be the simply connected covering, whose degree we denote d, and consider an $\alpha \in H(\mathbb{A}_f)$. Therefore, for any positive integer A divisible by d, there exists a $\beta \in \widetilde{H}(\mathbb{A}_f)$ such that $\pi(\beta) = \alpha^A$. By strong approximation applied to $\widetilde{H}$, $\beta = qk$, where $q \in \widetilde{H}(\mathbb{Q})$ and $k \in \pi^{-1}(K)$. Note that, since π is proper, $\pi^{-1}(K)$ is a compact open subgroup of $\widetilde{H}(\mathbb{A}_f)$. Since $\widetilde{H}(\mathbb{R})$ is connected, $\pi(q) \in H(\mathbb{R})^+$ and $\pi(q) \cdot x \in X_H^+$.

Thus, consider the point

$$\overline{(\pi(q) \cdot x, \pi(\beta))} \in T_{\alpha^A}(V).$$

By the previous discussion, this is equal to $\overline{(x, 1)}$. Since, by [UYa], Lemma 2.4, d is bounded by a uniform integer D, setting $A = D!$ finishes the proof. □

In order to find suitable Hecke correspondences, we will also need the following two results on maximal split tori:

Lemma 7.15. *Let $p \notin \Sigma(H, K_H)$ be a prime such that $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$. Then there exists a maximal split torus $S \subset H_{\mathbb{Q}_p}$ such that $S_{\mathbb{Z}_p}$ is a torus.*

Proof. Since $p \notin \Sigma(H, K_H)$, there exists a smooth reductive group scheme $\mathbf{H}$ over $\mathbb{Z}_p$ such that $\mathbf{H}_{\mathbb{Q}_p} = H_{\mathbb{Q}_p}$ and $\mathbf{H}(\mathbb{Z}_p) = K_{H,p}$. Let $\mathbf{S}$ be a maximal split torus of $\mathbf{H}$ and let S denote its generic fibre. By [Tit79], 3.8.1, $S_{\mathbb{Z}_p}$ is a torus if and only if

$$S_{\mathbb{Z}_p}(\mathbb{Z}_p) := \mathrm{GL}_n(\mathbb{Z}_p) \cap S(\mathbb{Q}_p) = K_{H,p} \cap S(\mathbb{Q}_p)$$

is equal to $\mathbf{S}(\mathbb{Z}_p)$. However, since $K_{H,p} = \mathbf{H}(\mathbb{Z}_p)$, $S_{\mathbb{Z}_p}(\mathbb{Z}_p)$ contains $\mathbf{S}(\mathbb{Z}_p)$ and so, by [Tit79], 3.8.2., they are equal. □

Lemma 7.16. *Assume $H_{\mathbb{Q}_p}$ is quasi-split and let $S \subset H_{\mathbb{Q}_p}$ be a maximal split torus. There exists a basis of $X^*(S)$ such that the coordinates of the characters of S that intervene in $\mathbb{Q}_p^n$ are uniformly bounded in absolute value.*

Proof. Let $T \subset H_{\mathbb{Q}_p}$ be the centraliser of S in $H_{\mathbb{Q}_p}$. Since $H_{\mathbb{Q}_p}$ is quasi-split, T is a maximal torus of $H_{\mathbb{Q}_p}$. By [Wat79], 7.4, there exists an isogeny $T \to S \times A$, where A is the maximal anisotropic subtorus of T, and the degree d of this isogeny is bounded by $[L_T : \mathbb{Q}]^{\dim T}$, where L_T is the splitting field of T. Note that $\dim T$ is bounded by the absolute rank of G and, as we have seen, $[L_T : \mathbb{Q}]$ is bounded in terms of the dimension of T.

Consider the map of characters

$$\varphi : \chi \mapsto \chi_S + \chi_A : X^*(T) \to X^*(S) \oplus X^*(A)$$

induced by the inclusions $S \subset T$ and $A \subset T$. The characters of S intervening in $\mathbb{Q}_p^n$ are precisely the χ_S such that $\chi \in X^*(T)$ intervenes in $\overline{\mathbb{Q}}_p^n$.

Now consider the embedding

$$\phi : X^*(S) \oplus X^*(A) \hookrightarrow X^*(T)$$

induced by the above isogeny. By Lemma 7.10 there exists a basis $\{e_1, ...e_r\}$ of $X^*(T)$ such that the coordinates of the characters of T intervening in $\overline{\mathbb{Q}}_p^n$ are bounded in absolute value by a uniform constant B'. Given a character of T, its coordinates increase in absolute value by at most a factor of d under $\phi \circ \varphi$.

Thus, let $\{\chi_i\}$ be the characters of T intervening in $\overline{\mathbb{Q}}_p^n$ and let $\{\chi_{i,S}+\chi_{i,A}\}$ be their images in $X^*(S) \oplus X^*(A)$. Write the image of $\chi_{i,S} + \chi_{i,A}$ under ϕ as

$$\sum_{j=1}^{r} n_{i,j} e_j.$$

Hence, $|n_{i,j}| < B := dB'$ for all i and j and $n_{i,j} = n_{i,S,j} + n_{i,A,j}$, where

$$\sum_{j=1}^{r} n_{i,S,j} e_j \text{ and } \sum_{j=1}^{r} n_{i,A,j} e_j$$

are the images of the $\chi_{i,S}$ and $\chi_{i,A}$ under ϕ, respectively. Therefore, either $|n_{i,S,j}| < B$ for all i and j, or there exist i and j such that $|n_{i,S,j}| \geq B$, in which case $n_{i,S,j}$ and $n_{i,A,j}$ are of opposite signs.

Assume the latter, letting χ_i denote the corresponding character and letting $n_{i,S,j}$ denote the coefficient with absolute value at least B. Since our representation of T was defined over $\mathbb{Q}_p$, for each $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, $\tau\chi_i$ also intervenes. Since S is split, $\tau\chi_{i,S} = \chi_{i,S}$ for every $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Therefore, the image of $\tau\chi_i$ in $X^*(S) \oplus X^*(A)$ varies over $\chi_{i,S} + \tau\chi_{i,A}$ and, since A is anisotropic,

$$\sum_{\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \tau\chi_{i,A} = 0.$$

Thus, there exists a $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that the coefficient of e_j corresponding to the image of $\tau\chi_{i,A}$ under ϕ is of the opposite sign to $n_{i,A,j}$. But then this coefficient is of the same sign as $n_{i,S,j}$, which implies that the sum of these two coefficients has absolute value greater than or equal to B, which is a contradiction.

Therefore, with respect to the basis $\{e_1, ..., e_r\}$ of $X^*(T)$, the coordinates of the characters of S intervening in $\mathbb{Q}_p^n$ are bounded in absolute value by B. Since our representation is faithful, these characters generate $X^*(S)$ and so, as a submodule of $X^*(T)$, there are only finitely many possibilities for $X^*(S)$. For each such possibility, choose a basis and consider the maximum of the absolute values of the coordinates of the characters intervening in $\mathbb{Q}_p^n$. □

Proof. (Theorem 7.13)

By Lemma 7.15, since $p \notin \Sigma(H, K_H)$, we can find a non-trivial, maximal, split torus $S \subset H_{\mathbb{Q}_p}$ such that $S_{\mathbb{Z}_p}$ is a torus. Furthermore, by Lemma 7.16, there exists a basis of $X^*(S)$ such that the coordinates of the characters intervening in $\mathbb{Q}_p^n$ are uniformly bounded in absolute value. Let $\pi_i : G \to G_i$ denote the natural morphisms.

Lemma 7.17. *The images $\pi_i(S)$ are non-trivial split tori.*

Proof. Let $\pi : \widetilde{H} \to H$ denote the simply connected cover and let $\widetilde{S}$ denote a maximal split torus of $\widetilde{H}_{\mathbb{Q}_p}$ such that $\pi(\widetilde{S}) = S$. We can write $\widetilde{S}$ as a product of maximal split tori S_j in the quasi-simple factors H_j of $\widetilde{H}_{\mathbb{Q}_p}$. The map $\pi_{\mathbb{Q}_p}$ composed with the inclusion of $H_{\mathbb{Q}_p}$ in the product of the $\pi_i(H)_{\mathbb{Q}_p}$ is given by maps f_i each a product of morphisms $g_{i,j} : H_j \to \pi_i(H)_{\mathbb{Q}_p}$.

By [Mil04], SV3, $\pi_i(H)$ is non-trivial. Therefore, for each i, one of the

$g_{i,j}$ is non-trivial. Since H_j is quasi-simple, $\ker g_{i,j}$ is finite and, therefore, $g_{i,j}(S_j)$ is non-trivial. $\square$

As $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$, the compact open subgroup $K_p := K'_p \cap G(\mathbb{Q}_p)$ of $G(\mathbb{Q}_p)$ is equal to $G_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and, for any $\alpha \in S(\mathbb{Q}_p)$,

$$[K_p : K_p \cap \alpha K_p \alpha^{-1}] = [K_p : K_p \cap \alpha G_{\mathbb{Z}_p}(\mathbb{Z}_p)\alpha^{-1}].$$

By [EY03], Lemma 7.4.3, for $q_i = \pi_{i|S}$ and $e = A$ (the positive integer given by Lemma 7.14), there exist a uniform constant k' and an element $\alpha \in S(\mathbb{Q}_p)$ such that no $\pi_i(\alpha)$ lies in a compact subgroup of $S_i(\mathbb{Q}_p)$ and

$$[K_p : K_p \cap \alpha^A G_{\mathbb{Z}_p}(\mathbb{Z}_p)\alpha^{-A}] < p^{k'}.$$

Next we define I_p following [KY], 8.3.2. Since S is a split torus and $S_{\mathbb{Z}_p}$ is a torus, $G_{\mathbb{Z}_p}(\mathbb{Z}_p) = K_p$ is in good position with respect to S (using the terminology of [KY], 4.1.6).

Let f be the constant, defined in [KY], Lemma 8.1.6 (b), for the group G'. We claim that there exists an Iwahori subgroup I_p^1 of $G(\mathbb{Q}_p)$ such that

$$[K_p : K_p \cap I_p^1] < p^f.$$

To see this we let K_p^1 be any maximal compact subgroup of $G(\mathbb{Q}_p)$ containing K_p. Since K_p is in good position with respect to S, so too is K_p^1. Thus, by [KY], Lemma 8.1.6 (b)(i), there exists an Iwahori subgroup $I_p^1 \subset K_p^1$ in good position with respect to S satisfying $[K_p^1 : I_p^1] < p^f$. Thus,

$$[K_p : K_p \cap I_p^1] < p^f.$$

Let S' be a maximal split torus of $G_{\mathbb{Q}_p}$ containing S such that I_p^1 is in good position with respect to S'. Let M be the centraliser of S' in $G_{\mathbb{Q}_p}$. Let

$\mathcal{B}$ be the (extended) Bruhat-Tits building of $G_{\mathbb{Q}_p}$ and $\mathcal{A} \subset \mathcal{B}$ the apartment of $\mathcal{B}$ associated to S'.

The group $M(\mathbb{Q}_p)$ acts on $\mathcal{A}$ as follows: we denote by

$$\mathrm{ord}_M : M(\mathbb{Q}_p) \to X_*(M)_{\mathbb{Q}_p}$$

the homomorphism characterised by

$$\langle \mathrm{ord}_M(m), \chi \rangle = \mathrm{ord}_p(\chi(m))$$

for all $\chi \in X^*(M)_{\mathbb{Q}_p}$, where ord_p is the normalised additive valuation on $\mathbb{Q}_p^*$ and $X_*(M)_{\mathbb{Q}_p}$ (resp. $X^*(M)_{\mathbb{Q}_p}$) denotes the group of cocharacters (resp. characters) of M defined over $\mathbb{Q}_p$. Let $\Lambda \subset X_*(M)_{\mathbb{Q}_p}$ be the free $\mathbb{Z}$-module $\mathrm{ord}_M(M(\mathbb{Q}_p))$. Then $M(\mathbb{Q}_p)$ acts on $\mathcal{A}$ via Λ-translations.

Let K_p^m be a special compact subgroup containing I_p^1 and let $x \in \mathcal{A}$ be the unique special vertex fixed by K_p^m. Recall the element $\alpha \in S(\mathbb{Q}_p)$ chosen above. The vector $\mathrm{ord}_M(\alpha) \in \Lambda$ is non-trivial. Let C be the chamber of $\mathcal{A}$ fixed pointwise by I_p^1 (it contains x in its closure). Consider the chamber $C' = C + \mathrm{ord}_M(\alpha)$. Let $\mathcal{C} \subset \mathcal{A}$ be the unique Weyl chamber with apex x containing C'. Finally, let I_p^2 be the Iwahori subgroup of $G(\mathbb{Q}_p)$ fixing the unique chamber of $\mathcal{C}$ containing x in its closure.

Define I_p as the intersection $K_p \cap I_p^1 \cap I_p^2$. Since I_p^2 stabilises a chamber in $\mathcal{A}$ it is also in good position with respect to S' and, therefore, S. Thus, I_p is in good position with respect to S. It follows from [KY], Lemma 8.1.6 (b)(ii) that

$$[K_p : I_p] = [K_p : K_p \cap I_p^1 \cap I_p^2] \leq [K_p^1 : I_p^1 \cap I_p^2] < p^f,$$

which is the first condition of Theorem 7.13. By Lemma 7.14, we have $\widetilde{V} \subset T_{\alpha^A}(\widetilde{V})$, which is the second condition of Theorem 7.13.

Let $S'_i := \pi_i(S')$ and denote by $M_i := \pi_i(M)$ its centraliser. Let C_i be the unique chamber of the Bruhat-Tits building $\mathcal{B}_i$ of $G_{i,\mathbb{Q}_p}$ fixed by the Iwahori subgroup $\pi_i(I_p^2)$ and let x_i be the vertex in the closure of C_i fixed by $\pi_i(K_p^m)$. Finally, let $\mathcal{C}_i$ be the unique Weyl chamber of the apartment $\mathcal{A}_i$ corresponding to S'_i with apex x_i and containing C_i.

For M_i we have a homomorphism

$$\mathrm{ord}_{M_i} : M_i(\mathbb{Q}_p) \to X_*(M_i)_{\mathbb{Q}_p},$$

defined analogously to ord_M. We denote the image $\mathrm{ord}_{M_i}(M_i(\mathbb{Q}_p)$ by Λ_i. Thus, $M_i(\mathbb{Q}_p)$ acts on $\mathcal{A}_i$ by Λ_i-translations. We denote by $\Lambda_i^+ \subset \Lambda_i$ the positive cone stabilising $\mathcal{C}_i$. By virtue of our choice of I_p^2, since $\pi_i(\alpha)$ does not lie in a compact subgroup of $S_i(\mathbb{Q}_p)$, $\mathrm{ord}_{M_i}(\pi(\alpha))$ lies in $\Lambda_i^+ \backslash \{0\}$. Hence, $\mathrm{ord}_{M_i}(\pi_i(\alpha^A))$ must also belong to $\Lambda_i^+ \backslash \{0\}$. Thus, by [KY], Proposition 8.1.4, for any $k_1, k_2 \in I_p^2$ (in particular for any $k_1, k_2 \in I_p$), $\pi_i(k_1 \alpha^A k_2)$ generates an unbounded subgroup of $G_i(\mathbb{Q}_p)$. This is the third condition of Theorem 7.13.

Finally, from the previous discussion we have

$$\begin{aligned}
& [I_p : I_p \cap \alpha^A I_p \alpha^{-A}] \\
= \; & [I_p : I_p \cap \alpha^A K_p \alpha^{-A}] \cdot [I_p \cap \alpha^A K_p \alpha^{-A} : I_p \cap \alpha^A I_p \alpha^{-A}] \\
\leq \; & [K_p : K_p \cap \alpha^A K_p \alpha^{-A}] \cdot [K_p : I_p] \\
\leq \; & [K_p : K_p \cap \alpha^A G_{\mathbb{Z}_p}(\mathbb{Z}_p) \alpha^{-A}] \cdot [K_p : I_p] \leq p^{k'+f} := p^k.
\end{aligned}$$

This is the fourth condition of Theorem 7.13.

□

7.7 The geometric criterion

Next we explain the procedure via which we replace strongly special subvarieties with higher-dimensional strongly special subvarieties given the existence of suitable Hecke correspondences:

Theorem 7.18. *Let (G, X) be a Shimura datum and let $K \subset G(\mathbb{A}_f)$ be a neat compact open subgroup, the product of compact open subgroups $K_p \subset G(\mathbb{Q}_p)$. Let X^+ be a connected component of X and let V be a special subvariety of $S_K(G, X)$. Suppose that V is properly contained in a Hodge generic irreducible subvariety Z of $S_K(G, X)$ and assume that there exist a prime p and an $\alpha \in G(\mathbb{Q}_p)$ such that*

- *$Z \subset T_\alpha(Z)$.*
- *For every $k_1, k_2 \in K_p$, the element $k_1 \alpha k_2$ generates an unbounded subgroup of $G_i(\mathbb{Q}_p)$ for each i.*

Then Z contains a special subvariety V' containing V properly. Moreover, if V is strongly special then V' is strongly special.

This theorem is very similar to [KY], Theorem 7.2.1 and the proof here is nearly a carbon copy of the proof found there. Our situation is slightly simplified by the fact that Z is geometrically irreducible. Ensuring that V' properly contains V is where we require the stronger condition on α.

Lemma 7.19. *If the conclusion of Theorem 7.18 holds for all Shimura data (G, X) with G semisimple of adjoint type, then it holds for all Shimura data.*

Proof. Consider the situation in Theorem 7.18. We have a finite morphism of Shimura varieties

$$f : \mathrm{Sh}_K(G, X) \to \mathrm{Sh}_{K^{\mathrm{ad}}}(G^{\mathrm{ad}}, X^{\mathrm{ad}}).$$

Let Z^{ad} be the image of Z under this morphism. Similarly, let V^{ad} be the image of V. Thus, V^{ad} is a special subvariety of $S_{K^{\mathrm{ad}}}(G^{\mathrm{ad}}, X^{\mathrm{ad}})$.

Let α^{ad} denote the image of α in $G^{\mathrm{ad}}(\mathbb{Q}_p)$. The inclusion $Z \subset T_\alpha(Z)$ implies that $Z^{\mathrm{ad}} \subset T_{\alpha^{\mathrm{ad}}}(Z^{\mathrm{ad}})$. As K^{ad} is a product of compact open subgroups $K_p^{\mathrm{ad}} \subset G^{\mathrm{ad}}(\mathbb{Q}_p)$, the second condition of Theorem 7.18 implies the analogous condition for α^{ad} and K_p^{ad}.

As irreducible components of the preimage of a special subvariety by a finite morphism of Shimura varieties are special, it is enough to show that Z^{ad} contains a special subvariety V'^{ad} containing V^{ad} properly. □

Therefore, we henceforth assume that G is semisimple of adjoint type. We fix a $\mathbb{Z}$-structure on G by choosing a finitely generated free $\mathbb{Z}$-module W, choosing a faithful representation

$$\xi : G \hookrightarrow \mathrm{GL}(W_{\mathbb{Q}})$$

and taking the Zariski closure of G in $\mathrm{GL}(W)$. We may choose ξ in such a way that K is contained in $\mathrm{GL}(W_{\hat{\mathbb{Z}}})$. This canonically induces a $\mathbb{Z}$-variation of Hodge structures $\mathcal{F}$ on $\mathrm{Sh}_K(G, X)$ and, in particular, on $S_K(G, X)$ (see [EY03], 3.2).

Let z be a Hodge generic point of the smooth locus Z^{sm} of Z. Let $\pi_1(Z^{\mathrm{sm}}, z)$ be the topological fundamental group of Z^{sm} at the point z. We choose a point $x \in X$ lying above z. This choice canonically identifies the fibre at z of the locally constant sheaf underlying $\mathcal{F}$ with the $\mathbb{Z}$-module W. The action of $\pi_1(Z^{\rm sm}, z)$ on this fibre is described by the monodromy representation

$$\rho : \pi_1(Z^{\rm sm}, z) \to \pi_1(S_K(G, X), z) = G(\mathbb{Q})_+ \cap K \hookrightarrow \mathrm{GL}(W).$$

Since Z is Hodge generic in $\mathrm{Sh}_K(G, X)$, the Mumford-Tate group of $\mathcal{F}_{|Z^{\rm sm}}$ at z is G. Thus, by [Moo98a], 1.4, given that the group G is adjoint, the group $\rho(\pi_1(Z^{\rm sm}, z))$ is Zariski dense in G. Having fixed a prime p (as in Theorem 7.18), [KY], Proposition 4.2.1, implies that the p-adic closure of $\rho(\pi_1(Z^{\rm sm}, z))$ in $G(\mathbb{Z}_p)$ is a compact open subgroup $K'_p \subset K_p$.

We have a Galois, pro-étale cover

$$\pi_{K_p} : \mathrm{Sh}_{K^p}(G, X) \to \mathrm{Sh}_K(G, X),$$

with group K_p, as defined in [KY], Section 4.1.3. Let $\widetilde{Z}$ be an irreducible component of the preimage of Z in $\mathrm{Sh}_{K^p}(G, X)$ and let $\widetilde{V}$ be an irreducible component of the preimage of V in $\widetilde{Z}$. By [KY], Lemma 7.2.3, we have

Lemma 7.20. *The variety $\widetilde{Z}$ is stabilised by the group K'_p and the set of irreducible components of $\pi_{K_p}^{-1}(Z)$ is naturally identified with the finite set K_p/K'_p.*

The inclusion $Z \subset T_\alpha(Z)$ implies that $\widetilde{Z}$ is an irreducible component of $\pi_{K_p}^{-1}(T_\alpha(Z))$. However, these components are of the form $\widetilde{Z} \cdot k_1 \alpha k_2$ for $k_1, k_2 \in K_p$. Therefore, there exist $k_1, k_2 \in K_p$ such that $\widetilde{Z} = \widetilde{Z} \cdot k_1 \alpha k_2$.

Corollary 7.21. *Let U_p be the group generated by K'_p and $k_1 \alpha k_2$. The variety $\widetilde{Z}$ is stabilised by the group U_p.*

We now conclude the proof of Theorem 7.18. Again, let $\pi_i : G \to G_i$ denote the natural morphisms. By the condition placed on α, the group $\pi_i(U_p)$ is unbounded in $G_i(\mathbb{Q}_p)$ for all i. Let $G_{1,\mathbb{Q}_p} = \prod_i H_i$ be the decomposition of $G_{1,\mathbb{Q}_p}$ into simple factors. Up to renumbering, we can assume that the projection of U_p to $H_1(\mathbb{Q}_p)$ is unbounded in $H_1(\mathbb{Q}_p)$. Let

$$\tau : \widetilde{H}_1 \to H_1$$

be the universal cover of H_1. We have [KY], Lemma 7.2.6:

Lemma 7.22. *The group $U_p \cap H_1(\mathbb{Q}_p)$ contains the group $\tau(\widetilde{H}_1(\mathbb{Q}_p))$ with finite index.*

Let $K_{p,1}$ be the compact open subgroup $\pi_1(K_p)$ of $G_{1,\mathbb{Q}_p}$ and let $K_{p,>1}$ be the projection of K to $G_{>1,\mathbb{Q}_p} := \prod_{i>1} G_{i,\mathbb{Q}_p}$. As U_p is an open subgroup of $G(\mathbb{Q}_p)$, it contains a compact open subgroup of $G_{1,\mathbb{Q}_p}$ and, in particular, a compact open subgroup $U_{p,1}$ of $K_{p,1} \cap \prod_{i>1} H_i(\mathbb{Q}_p)$. Similarly, U_p contains a compact open subgroup $U_{p,>1}$ of $K_{p,>1}$. By the previous lemma, U_p contains the unbounded subgroup $\tau(\widetilde{H}_1(\mathbb{Q}_p)) \cdot U_{p,1} \cdot U_{p,>1}$. We make the definition [KY], Definition 7.2.7:

Definition 7.23. *We replace U_p by its subgroup $\tau(\widetilde{H}_1(\mathbb{Q}_p)) \cdot U_{p,1} \cdot U_{p,>1}$. We denote by V' the Zariski closure of $\pi_{K_p}(\widetilde{V} \cdot U_p)$.*

Since, $\widetilde{Z}$ is stabilised by U_p, the variety V' is a subvariety of Z. Therefore, let $K_i := \pi_i(K)$ and let $\mathcal{K}$ be the neat compact open subgroup $\prod_i K_i$. We have the natural finite morphism

$$f : \mathrm{Sh}_K(G, X) \to \mathrm{Sh}_{\mathcal{K}}(G, X)$$

of Shimura varieties and we let $\mathcal{V}' := f(V')$ and $\mathcal{V} := f(V)$. The proof of [KY], Lemma 7.2.8 demonstrates that

$$\mathcal{V}' = S_{K_1}(G_1, X_1) \times \mathcal{V}'_{>1},$$

where $\mathcal{V}'_{>1}$ is the special subvariety of $\prod_{i>1} S_{K_i}(G_i, X_i)$ given by the projection of $\mathcal{V}'$. Hence, $\mathcal{V}'$ is a strongly special subvariety of $S_{\mathcal{K}}(G, X)$ and, therefore, since f is a finite morphism of Shimura varieties, V' is a strongly special subvariety of $S_K(G, X)$. Furthermore, after possibly renumbering the G_i (which we are free to do due to the condition placed on α), we may assume that $\mathcal{V}'$ properly contains $\mathcal{V}$. Therefore, V is properly contained in V', which concludes the proof of Theorem 7.18.

7.8 Proof of main result

Finally, we prove Theorem 7.3. In fact, we will prove the following, equivalent statement:

Theorem 7.24. *Let S be a Shimura variety and let Σ be a set of strongly special subvarieties contained in S. Let Z be an irreducible component of the Zariski closure of $\mathbf{\Sigma}$ in S. Then Z is a strongly special subvariety of S.*

Lemma 7.25. *Theorem 7.24 is equivalent to Theorem 7.3.*

Proof. Consider the situation described in Theorem 7.24. If we assume that Theorem 7.3 holds then there exists a finite set $\{V_1, ..., V_k\}$ of strongly special subvarieties contained in Z such that, for every $V \in \Sigma$, V is contained in one of the V_i. Therefore, $\mathbf{\Sigma}$ is contained in the union of the V_i, which is itself contained in Z. Since Z is an irreducible component of the Zariski closure of $\mathbf{\Sigma}$, it must be equal to one of the V_i, proving Theorem 7.24.

Now consider the situation described in Theorem 7.3 and consider the set Σ of all strongly special subvarieties of S contained in Z. If we assume that Theorem 7.24 holds, the Zariski closure of $\mathbf{\Sigma}$ is a union of finitely many strongly special subvarieties $V_1, ..., V_k$. Thus, any strongly special subvariety contained in Z is contained in one of the V_i, proving Theorem 7.3. □

Note that, in order to prove Theorem 7.24, we may assume that the elements of Σ are of equal dimension. We first prove the following Theorem, following the proof of [KY], Theorem 9.2.1:

Theorem 7.26. *Let (G', X') be a Shimura datum such that $G' = G'^{\text{ad}}$ and fix a faithful representation*

$$\rho : G' \hookrightarrow \mathrm{GL}_n.$$

Let K' be a neat compact open subgroup of $G'(\mathbb{A}_f)$, equal to a product of compact open subgroups $K'_p \subset G'(\mathbb{Q}_p)$, such that $K' \subset \mathrm{GL}_n(\hat{\mathbb{Z}})$. Let k and f be the positive integers given by Theorem 7.13.

Let Σ be a set of strongly special subvarieties contained in $S_{K'}(G', X')$. Assume that the elements of Σ are of equal dimension d and that the Zariski closure Z of $\mathbf{\Sigma}$ is irreducible. For each $V \in \Sigma$, let (H_V, X_V) be the Shimura subdatum defining V and put $\Pi_V := \Pi(H_V, K_H)$.

Let (G, X) be a Shimura subdatum of (G', X') such that Z is contained and Hodge generic in $S_K(G, X)$, where $K := K' \cap G(\mathbb{A}_f)$. Let $r := \dim Z - d > 0$ and make ONE of the following assumptions:

- *The Π_V are bounded as V ranges through Σ.*

- *For each $V \in \Sigma$, there exists a prime p not dividing Π_V such that $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and*

$$p^{(k+2f)\cdot 2^r} \cdot (\deg_{\mathcal{L}_K} Z)^{2^r} < c \cdot \Pi_V^{\delta}.$$

Then, for each $V \in \Sigma$, Z contains a strongly special subvariety of $S_{K'}(G', X')$ containing V properly.

In the situation described in the theorem, we will use the term uniform to mean depending only on (G', X'), K' and ρ.

Proof. Firstly, we consider the case that, as V ranges through Σ, Π_V is bounded. That is to say, the primes dividing any given Π_V belong to a fixed, finite set, whose product we denote Π.

By Theorem 7.13, for any prime p not dividing Π such that $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$, there exists a compact open subgroup

$$I_p \subset K_p := K'_p \cap G(\mathbb{Q}_p) = G_{\mathbb{Z}_p}(\mathbb{Z}_p)$$

and an element $\alpha \in G(\mathbb{Q}_p)$ satisfying the four requirements of Theorem 7.13, for each $V \in \Sigma$. However, in this case we will choose these objects slightly more precisely: recall that, by Lemma 7.15, for each $V \in \Sigma$, there exists a non-trivial maximal split torus $S_V \subset H_{V,\mathbb{Q}_p}$ such that $S_{V,\mathbb{Z}_p}$ is a torus. Since S_V is split, it is conjugate via an element of $\mathrm{GL}_n(\mathbb{Q}_p)$ to a subtorus of the diagonal matrices. By Lemma 7.16, after possibly replacing $\boldsymbol{\Sigma}$ by a Zariski dense subset, we may assume that this torus is fixed i.e. that the S_V are all conjugate by elements of $\mathrm{GL}_n(\mathbb{Q}_p)$ to a fixed torus $S := S_{V_0}$ for some $V_0 \in \Sigma$. Let $I_p \subset K_p$ and $\alpha \in G(\mathbb{Q}_p)$ be the objects given by Theorem 7.13 applied to V_0.

Now consider another $V \in \Sigma$ and let $g \in \mathrm{GL}_n(\mathbb{Q}_p)$ be such that $gS_Vg^{-1} = S$. Since $S_{V,\mathbb{Z}_p}$ is a torus, S stabilises the lattice $g\mathbb{Z}_p^n$. Therefore, by [EY03], Lemma 3.3.1, since $S_{\mathbb{Z}_p}$ is a torus, there exists an element $c \in Z_G(S)(\mathbb{Q}_p)$ such that $g\mathbb{Z}_p^n = c\mathbb{Z}_p^n$, where $Z_G(S)$ is the centraliser of S in G. Therefore, there exists $k \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that $g = ck$ and so the S_V are all conjugate by elements of $\mathrm{GL}_n(\mathbb{Z}_p)$. If we further assume that p is a prime such that $G_{\mathbb{F}_p}$ is smooth, the final paragraph of the proof of [EY03], Proposition 7.3.1, explains that, again, after possibly replacing $\mathbf{\Sigma}$ by a Zariski dense subset, we may assume that the S_V are all conjugate by elements of K_p and, therefore, by elements of I_p.

Therefore, for each $V \in \Sigma$, we let $g_V \in I_p$ be such that $S_V = g_V S g_V^{-1}$. It follows that I_p and $\alpha_V := g_V \alpha g_V^{-1}$ satisfy the requirements of Theorem 7.13 applied to V. Furthermore, if we let $I \subset K$ be the compact open subgroup $K^p I_p \subset G(\mathbb{A}_f)$, then the Hecke correspondences T_{α_V} on $\mathrm{Sh}_I(G,X)$ all coincide with T_α.

Let

$$\tau : \mathrm{Sh}_I(G,X) \to \mathrm{Sh}_K(G,X)$$

be the induced morphism of Shimura varieties and let $\widetilde{Z}$ be an irreducible component of the preimage $\tau^{-1}(Z)$. For each $V \in \Sigma$, let $\widetilde{V} \subset S_I(G,X)$ be an irreducible component of the preimage $\tau^{-1}(V)$ contained in $\widetilde{Z}$. Each $\widetilde{V}$ is a strongly special subvariety of $S_I(G,X)$ defined by the Shimura subdatum (H_V, X_V). Denote the set of the $\widetilde{V}$ by $\widetilde{\Sigma}$. By the second requirement of Theorem 7.13, we have $\widetilde{V} \subset T_\alpha(\widetilde{V})$ for every $\widetilde{V} \in \widetilde{\Sigma}$. Hence, $\widetilde{\mathbf{\Sigma}}$ is contained in $\widetilde{Z} \cap T_\alpha(\widetilde{Z})$ and, therefore, $\widetilde{Z} \subset T_\alpha(\widetilde{Z})$.

As α satisfies the third requirement of Theorem 7.13, we can apply Theorem 7.18 to this α and conclude that, for each $\widetilde{V} \in \widetilde{\Sigma}$, there exists a special subvariety $\widetilde{V}' \subset \widetilde{Z}$ containing $\widetilde{V}$ properly whose image in $\mathrm{Sh}_{K'}(G', X')$ is strongly special. As τ preserves the property of being special, exhibiting a special subvariety $V' \subset Z$ containing V properly is equivalent to exhibiting a special subvariety $\widetilde{V}' \subset \widetilde{Z}$ containing $\widetilde{V}$ properly.

Thus, we consider the case that Π_V is unbounded as V ranges through Σ. Hence, we may assume that Π_V is larger than any uniform constant. We proceed by induction on r. Consider first the case $r = 1$ and let $V \in \Sigma$.

By the second assumption of Theorem 7.26, there exists a compact open subgroup $I_p \subset K_p$ and an element $\alpha \in G(\mathbb{Q}_p)$ satisfying the four requirements of Theorem 7.13 applied to V. Let $I \subset K$ be the compact open subgroup $K^p I_p \subset G(\mathbb{A}_f)$ and let

$$\tau : \mathrm{Sh}_I(G, X) \to \mathrm{Sh}_K(G, X)$$

be the induced morphism of Shimura varieties. It follows from the first requirement of Theorem 7.13 that the degree of τ is bounded above by p^f.

Let $\widetilde{V} \subset S_I(G, X)$ be an irreducible component of the preimage $\tau^{-1}(V)$. It is a strongly special subvariety of $S_I(G, X)$ defined by the Shimura subdatum (H_V, X_V) of (G, X). By the projection formula (see [KY], Proposition 5.3.2 (1)) and Theorem 7.4,

$$\deg_{\mathcal{L}_I} \widetilde{V} \geq \deg_{\mathcal{L}_K} V > c \cdot \Pi_V^{\delta}.$$

Let $\widetilde{Z}$ be an irreducible component of the preimage $\tau^{-1}(Z)$ containing $\widetilde{V}$. Thus, $\widetilde{Z}$ is Hodge generic in $\mathrm{Sh}_I(G, X)$ and

$$\deg_{\mathcal{L}_I} \widetilde{Z} \leq p^f \cdot d_Z.$$

As τ preserves the property of being special, exhibiting a special subvariety $V' \subset Z$ containing V properly is equivalent to exhibiting a special subvariety $\widetilde{V}' \subset \widetilde{Z}$ containing $\widetilde{V}$ properly.

By the second requirement of Theorem 7.13, we have $\widetilde{V} \subset T_\alpha(\widetilde{V})$. Hence, $\widetilde{V} \subset \widetilde{Z} \cap T_\alpha(\widetilde{Z})$. Given their dimensions, if $\widetilde{Z}$ and $T_\alpha(\widetilde{Z})$ intersect properly then $\widetilde{V}$ is an irreducible component of the intersection. Thus,

$$\begin{aligned} c \cdot \Pi_V^\delta < \deg_{\mathcal{L}_I} \widetilde{V} &\leq \deg_{\mathcal{L}_I}(\widetilde{Z} \cap T_\alpha(\widetilde{Z})) \\ &\leq (\deg_{\mathcal{L}_I} \widetilde{Z})^2 \cdot [I_p : I_p \cap \alpha I_p \alpha^{-1}] < p^{k+2f} \cdot d_Z^2, \end{aligned}$$

contradicting the second assumption of the theorem. Therefore, the intersection cannot be proper. Thus, $\widetilde{Z} \subset T_\alpha(\widetilde{Z})$ and, since α satisfies the second condition of Theorem 7.18, there exists a special subvariety $\widetilde{V}' \subset \widetilde{Z}$ containing $\widetilde{V}$ properly whose image in $\mathrm{Sh}_{K'}(G', X')$ is strongly special.

Therefore, we consider the case $r > 1$. Suppose that the conclusion of Theorem 7.26 holds for all subvarieties V and Z of $\mathrm{Sh}_K(G, X)$ as in the statement of Theorem 7.26 such that $0 < \dim Z - d < r$ and consider the case that $\dim Z = d + r$. We have $\widetilde{V}$, $\widetilde{Z}$, a compact open subgroup $I \subset K$ and an $\alpha \in G(\mathbb{Q}_p)$, constructed as in the case $r = 1$, where

$$\deg_{\mathcal{L}_I} \widetilde{V} > c \cdot \Pi_V^\delta$$

and $\deg_{\mathcal{L}_I} \widetilde{Z} \leq p^f \cdot d_Z$.

Suppose that $\widetilde{Z} \subset T_\alpha(\widetilde{Z})$. In this case we can apply Theorem 7.18 to deduce that there exists a special subvariety $\widetilde{V}' \subset \widetilde{Z}$ containing $\widetilde{V}$ properly whose image in $\mathrm{Sh}_{K'}(G', X')$ is strongly special.

Therefore, suppose that the intersection $\widetilde{Z} \cap T_\alpha(\widetilde{Z})$ is proper. By the second requirement of Theorem 7.13, $\widetilde{V} \subset \widetilde{Z} \cap T_\alpha(\widetilde{Z})$. Choose an irreducible component $\widetilde{Y} \subset S_I(G,X)$ of $\widetilde{Z} \cap T_\alpha(\widetilde{Z})$ containing $\widetilde{V}$ and denote its image in $\mathrm{Sh}_K(G,X)$ by Y. Thus, Y is irreducible and satisfies $r_Y := \dim Y - d < r$. To show that $r_Y > 0$ it suffices to check that $\widetilde{V}$ is not a component of $\widetilde{Z} \cap T_\alpha(\widetilde{Z})$. However, if this were true we would have

$$c \cdot \Pi_V^\delta < p^{k+2f} \cdot d_Z^2,$$

as in the case $r = 1$, contradicting the second assumption of Theorem 7.26.

Let (P, X_P) be a Shimura datum of (G,X), defining the smallest special subvariety of $S_I(G,X)$ containing $\widetilde{Y}$. Let $X_P^+ \subset X^+$ be the corresponding connected component of X_P. Define $K_P := K \cap P(\mathbb{A}_F)$ and $I_P := I \cap P(\mathbb{A}_f)$. We have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Sh}_{I_P}(P,X_P) & \xrightarrow{q} & \mathrm{Sh}_I(G,X) \\ \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau} \\ \mathrm{Sh}_{K_P}(P,X_P) & \xrightarrow{q} & \mathrm{Sh}_K(G,X). \end{array}$$

Let $\widetilde{V}_P$ be an irreducible component of $q^{-1}(\widetilde{V})$ contained in $S_{I_P}(P, X_P)$ and let $V_P := \tau(\widetilde{V}_P)$.

Let $\widetilde{Y}_P \subset S_{I_P}(P, X_P)$ be an irreducible component of $q^{-1}(\widetilde{Y})$ containing $\widetilde{V}_P$. In particular, $\widetilde{Y}_P$ is a Hodge generic subvariety of $S_{I_P}(P, X_P)$. Define $Y_P := \tau(\widetilde{Y}_P)$, a Hodge generic subvariety of $S_{K_P}(P, X_P)$.

We have

$$\deg_{\mathcal{L}_{K_P}} Y_P \leq \deg_{\mathcal{L}_{I_P}} \widetilde{Y}_P \leq \deg_{\mathcal{L}_I} \widetilde{Y} \leq \deg_{\mathcal{L}_I}(\widetilde{Z} \cap T_\alpha(\widetilde{Z})) < p^{k+2f} \cdot d_Z^2,$$

where the first inequality comes from the projection formula, the second comes from [KY], Proposition 5.3.10, the third is due to the fact that $\widetilde{Y}$ is an irreducible component of $\widetilde{Z} \cap T_\alpha(\widetilde{Z})$, and the last inequality was demonstrated previously.

Lemma 7.27. *The data P, X_P, X_P^+, K_P, V_P and Y_P satisfy the conditions of Theorem 7.26 (in place of G, X, X^+, K, V and Z, respectively).*

Proof. Firstly, note that the image of V_P in $\mathrm{Sh}_{K'}(G', X')$ is strongly special since it is still defined by the Shimura datum (H_V, X_V). Let $r_P := \dim Y_P - \dim V_P$. Thus, $r_P = r_Y > 0$. We must verify that P, X_P, X_P^+, K_P, V_P and Y_P satisfy the second condition of Theorem 7.26 for the same prime p.

From the above inequalities we have

$$p^{(k+2f)\cdot 2^{r_P}} \cdot (\deg_{\mathcal{L}_{K_P}} Y_P)^{2^{r_P}} \leq p^{(k+2f)\cdot 2^{r_P+1}} \cdot d_Z^{2^{r_P+1}}$$

and, as $r_P + 1 \leq r$, we deduce from the second assumption of Theorem 7.26 that

$$p^{(k+2f)\cdot 2^{r_P}} \cdot (\deg_{\mathcal{L}_{K_P}} Y_P)^{2^{r_P}} < c \cdot \Pi_V^{\delta}.$$

□

As $r_P < r$, by the induction hypothesis, we can apply Theorem 7.26 to P, X_P, X_P^+, K_P, V_P and Y_P. Thus Y_P contains a special subvariety V_P', which contains V_P properly and whose image in $\mathrm{Sh}_{K'}(G', X')$ is strongly special. This implies that Z contains a special subvariety V', which contains V properly and whose image in $\mathrm{Sh}_{K'}(G', X')$ is strongly special.

□

Therefore, in order to prove Theorem 7.24, it suffices to prove the following lemma:

Lemma 7.28. *Let $V \in \Sigma$. There exists a uniform constant c_{11} such that, if $\Pi_V > c_{11}$, then there exists a prime p not dividing Π_V such that $K_p' = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$*

and

$$p^{(k+2f)\cdot 2^r} \cdot (\deg_{\mathcal{L}_K} Z)^{2^r} < c \cdot \Pi_V^{\delta}.$$

Proof. By a theorem of Chebyshev, there exist absolute positive constants c_{12} and c_{13} such that the number of primes $\pi(x)$ less than a given real number $x \geq 2$ is bounded below by $c_{12}\frac{x}{\log x}$ and above by $c_{13}\frac{x}{\log x}$. Therefore, for any fixed $\gamma > \epsilon > 0$,

$$\pi(\Pi_V^{\gamma}) \gg \frac{\Pi_V^{\gamma}}{\log \Pi_V^{\gamma}} \gg \Pi_V^{\gamma-\epsilon}.$$

If we denote by $\omega(\Pi_V)$ the number of primes dividing Π_V, we have the trivial estimate

$$\omega(\Pi_V) \leq \frac{\log \Pi_V}{\log 2} \ll \Pi_V^{\epsilon}.$$

Note that $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$ holds for all primes p greater than a uniform constant. Therefore, if we set $\gamma = \frac{\delta}{(k+2f)2^r} - \epsilon > 2\epsilon > 0$, provided Π_V is larger than a uniform constant, we can find a prime p satisfying the requirements of the lemma.

□

7.9 The André-Oort conjecture

We will prove the following theorem, which appears as [KY], Theorem 1.2.2. The difference between our proof and the one appearing there is that ours does not depend on any results from ergodic theory.

Theorem 7.29. *Let (G, X) be a Shimura datum and let K be a compact open subgroup of $G(\mathbb{A}_f)$. Let Σ be a set of special subvarieties in $\mathrm{Sh}_K(G, X)$ and* *let Z be an irreducible component of the Zariski closure of $\mathbf{\Sigma}$ in $\mathrm{Sh}_K(G,X)$. We make ONE of the following assumptions:*

- *Assume the generalised Riemann hypothesis for CM fields.*
- *Assume that there exists a faithful representation $G \hookrightarrow \mathrm{GL}_n$ such that, with respect to this representation, the generic Mumford-Tate groups MT_V of the $V \in \Sigma$ lie in one $\mathrm{GL}_n(\mathbb{Q})$-conjugacy class.*

Then Z is a special subvariety of $\mathrm{Sh}_K(G,X)$.

Proof. Fix a connected component X^+ of X. We may assume that Z lies in the connected component $S_K(G,X)$. Now, [KY], Theorem 2.5.3, produces a dichotomy: either the subvarieties V have Galois orbits whose degrees are bounded from below by an invariant unbounded as we range through Σ or there exists a finite set $\{T_1,...,T_r\}$ of subtori of G, anisotropic over $\mathbb{R}$, such that each $V \in \Sigma$ is T_i-special for some $i \in \{1,...,r\}$ (see [UYa], Definition 3.1 and Definition 3.2 for the definition of T-special).

If the former occurs then [KY], Theorem 3.2.1, implies Theorem 7.29. Otherwise, we may assume that every $V \in \Sigma$ is T-special for some fixed subtorus T of G such that $T_{\mathbb{R}}$ is anisotropic. Thus, by [UYa], Lemma 3.3 and Lemma 3.5, there exist $q \in G(\mathbb{Q})$, $\theta \in G(\mathbb{A}_f)$ and, for each $V \in \Sigma$, a qTq^{-1}-Shimura subdatum (H_V, X_V) of (G,X), where H_V is the generic Mumford-Tate group of X_V, such that V is the image of $X_V^+ \times \{\theta\}$ in $S_K(G,X)$ (see [UYa], Definition 3.1 for the definition of a T-Shimura subdatum). Hence, after replacing Z by an irreducible component of its image under a suitable Hecke correspondence, we may assume that each V is a standard T-special subvariety of $S_K(G,X)$, associated to a T-Shimura subdatum (H_V, X_V), with

$H = \mathrm{MT}(X_V)$ (see [UYa] Definition 3.2 for the definition of a standard T-special subvariety).

Thus, by [UYa], Lemma 3.6 and Lemma 3.7, for every $V \in \Sigma$, (H_V, X_V) is a Shimura subdatum of a fixed T-Shimura subdatum (L, X_L). Therefore, we may assume that $\mathbf{\Sigma}$ is contained in $S_{L(\mathbb{A}_f)\cap K}(L, X_L)$. Let $(L^{\mathrm{ad}}, X_L^{\mathrm{ad}})$ be the adjoint Shimura datum and let K_L be a compact open subgroup of $L^{\mathrm{ad}}(\mathbb{A}_f)$ containing the image of $L(\mathbb{A}_f) \cap K$. Thus, we have an induced morphism of Shimura varieties

$$f : \mathrm{Sh}_{L(\mathbb{A}_f)\cap K}(L, X_L) \to \mathrm{Sh}_{K_L}(L^{\mathrm{ad}}, X_L^{\mathrm{ad}}).$$

Let V^{ad} be the image of V under f. Since T is the connected centre of H_V and T is contained in the centre of L, V^{ad} is defined by a Shimura subdatum (H_V', X_V') of $(L^{\mathrm{ad}}, X_{L^{\mathrm{ad}}})$ such that H_V' is semisimple. Since Z is special if and only if its image under f is special, we have reduced Theorem 7.29 to Theorem 7.3.

□

References

[AD03] F. Amoroso and R. Dvornicich. Lower bounds for the height and size of the ideal class group in CM-fields. *Monatsh. Math.*, 138:85–94, 2003.

[And89] Y. André. *G-functions and geometry.* Aspects of Mathematics. Springer, 1989.

[And98] Y. André. Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire. *J. Reine Angew. Math.*, 505:203–208, 1998.

[BB66] W. Baily and A. Borel. Compactifications of arithmetic quotients of bounded symmetric domains. *Ann. of Math.*, 84:442–528, 1966.

[BG06] E. Bombieri and W. Gubler. *Heights in Diophantine geometry.* Cambridge University Press, 2006.

[Bor72] A. Borel. Some metric properties of arithmetic quotients of symmetric spaces and an extension theorem. *J. Differential Geometry*, 6:543–560, 1972.

[BT65] A. Borel and J. Tits. Groupes réductifs. *Publ. Math. IHES*, 27:55–151, 1965.

[BT84] F. Bruhat and J. Tits. Groupes réductifs sur un corps local II. *Publ. Math. IHES*, 60:1–184, 1984.

[Cox89] D. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley and Sons, 1989.

[CU05] L. Clozel and E. Ullmo. Equidistribution de sous-variétés spéciales. *Ann. of Math.*, 161:1571–1588, 2005.

[CU06] L. Clozel and E. Ullmo. Equidistribution adélique des tores et équidistribution des points CM. *Doc. Math.*, Volume en l'honneur de J. Coates:233–260, 2006.

[CW01] P.B. Cohen and G. Wüstholz. Application of the André-Oort conjecture to some questions in transcendence. In *A panorama in number theory*. Cambridge Univ. Press, 2001.

[Del71] P. Deligne. Travaux de Shimura. In *Séminaire Bourbaki, 1970-1971*, Lecture Notes in Maths. Springer-Verlag, 1971.

[Del77] P. Deligne. Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques. In *Automorphic forms, representations and L-functions*, Proc. Sympos. Pure Math. Amer. Math. Soc., 1977.

[DG63] M. Demazure and A. Grothendieck. *Schémas en groupes, SGA 3.* IHES, 1963. Exp. VIII-XIV, Fasc. 4.

[DKM10] R.C. Daileda, R. Krishnamoorthy, and A. Malyshev. Maximal class numbers of CM number fields. *Journal of Number Theory*, 130(4):936–943, 2010.

[DY11] C. Daw and A. Yafaev. An unconditional proof of the André-Oort conjecture for Hilbert modular surfaces. *Manuscripta Math.*, 135:263–271, 2011.

[Edi98] B. Edixhoven. Special points on the product of two modular curves. *Compositio Mathematica*, 114:315–328, 1998.

[Edi01] B. Edixhoven. The André-Oort conjecture for Hilbert modular surfaces. In *Moduli of abelian varieties (Texel Island, 1999)*, Progr. Math. Birkhäuser, 2001.

[Edi05] B Edixhoven. Special points on products of modular curves. *Duke Math. J.*, 126(2), 2005.

[EMO01] B. Edixhoven, B. Moonen, and F. Oort. Open problems in algebraic geometry. *Bull. Sci. Math.*, 125:1–22, 2001.

[EV07] J.S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. *IMRN*, 2007. doi:10.1093/imrn/rnm002.

[EY03] B. Edixhoven and A. Yafaev. Subvarieties of Shimura varieties. *Ann. of Math.*, 157(2):621–645, 2003.

[Fre90] E. Freitag. *Hilbert modular forms.* Springer, 1990.

[Har13] M. Harris. Courbes modulaires. Cours de l'Ecole Doctorale: Cohomologie cohérente des variétés de Shimura. Available at arXiv.org, arXiv:0406508, 2013.

[HP12] P. Habegger and J. Pila. Some unlikely intersections beyond André-Oort. *Compositio Math.*, 148:1–27, 2012.

[Küh12] L. Kühne. An effective result of André-Oort type. *Ann. of Math.*, 176(1):651–671, 2012.

[KUY13] B. Klingler, E. Ullmo, and A. Yafaev. The hyperbolic Ax-Lindemann-Weierstrass conjecture. Available at www.math.u-psud.fr/∼ullmo, 2013.

[KY] B. Klingler and A. Yafaev. The André-Oort conjecture. To appear in Ann. of Math. Available at www.math.jussieu.fr/∼klingler.

[Mar91] G. Margulis. *Discrete subgroups of semisimple lie groups*. Springer, 1991.

[Mil04] J.S. Milne. Introduction to Shimura varieties. Available at www.jmilne.org/math, 2004.

[Mil12] J.S. Milne. Modular functions and modular forms. Available at www.jmilne.org/math, 2012.

[Moo98a] B. Moonen. Linearity properties of Shimura varieties I. *Algebraic Geom.*, 7(3):539–567, 1998.

[Moo98b] B. Moonen. Linearity properties of Shimura varieties II. *Compositio Math.*, 114(1):3–35, 1998.

[Mum77] D. Mumford. Hirzebruch's proportionality principle in the non-compact case. *Invent. Math.*, 42:239–277, 1977.

[Oh01] H. Oh. Adelic version of Margulis arithmeticity theorem. *Math. Ann.*, 321(4):789–815, 2001.

[Oor97] F. Oort. Canonical lifts and dense sets of CM-points. In *Arithmetic Geometry*, Symposia Math. Cambridge Univ. Press, 1997.

[Orr13] M. Orr. Families of Abelian varieties with many isogenous fibres. *J. Reine Angew. Math.*, 2013.

[Pil09a] J. Pila. Algebraic points of definable sets and results of André-Oort-Manin-Mumford type. *IMRN*, 13:2476–2507, 2009.

[Pil09b] J. Pila. On the algebraic points of a definable set. *Selecta Math.*, 15(1):151–170, 2009.

[Pil11] J. Pila. O-minimality and the André-Oort conjecture for $\mathbb{C}^n$. *Ann. of Math.*, 173(3):1779–1840, 2011.

[Pin05a] R. Pink. A combination of the conjectures of Mordell-Lang and André-Oort. In *Geometric methods in algebra and number theory*, Progress in Mathematics. Birkhäuser, 2005.

[Pin05b] R. Pink. A common generalization of the conjectures of André-Oort, Manin-Mumford, and Mordell-Lang. Available at www.math.ethz.ch/∼pink, 2005.

[PR91] V.P. Platanov and A.S. Rapinchuk. *Algebraic groups and number theory*. Academic Press, Inc., 1991.

[Pra89] G. Prasad. Volumes of S-arithmetic quotients of semi-simple groups. *Publ. Math. IHES*, 69:91–114, 1989.

[PS13] K. Peterzil and S. Starchenko. Definability of restricted theta functions and families of abelian varieties. *Duke Math. J.*, 162(4):627–823, 2013.

[PT13] J. Pila and J. Tsimerman. The André-Oort conjecture for the moduli space of Abelian surfaces. *Compositio Math.*, 149:204–216, 2013.

[PT14] J. Pila and J. Tsimerman. Ax-lindemann for $\mathcal{A}_g$. *Ann. of Math.*, 179:659–681, 2014.

[PW06] J. Pila and A. Wilkie. The rational points of a definable set. *Duke Math. J.*, 133:591–616, 2006.

[PZ08] J. Pila and U. Zannier. Rational points in periodic analytic sets and the Manin-Mumford conjecture. *Rend. Mat. Acc. Lincei*, 19:149–162, 2008.

[RU09] N. Ratazzi and E. Ullmo. Galois+equidistribution=Manin-Mumford. In *Ecole d'été arithmetic geometry*, Clay Math. Proc. Amer. Math. Soc., 2009.

[Spr79] T.A. Springer. Reductive groups. In *Automorphic forms, representations and L-functions*, Proc. Sympos. Pure Math. Amer. Math. Soc., 1979.

[Tit79] J. Tits. Reductive groups over local fields. In *Automorphic forms, representations and L-functions*, Proc. Sympos. Pure Math. Amer. Math. Soc., 1979.

[Tsi12] J. Tsimerman. Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points. *J. Amer. Math. Soc.*, 25:1091–1117, 2012.

[Ull13] E. Ullmo. Quelques applications du théorème d'Ax Lindemann hyperbolique. To appear in Compositio Mathematicae. Available at www.math.u-psud.fr/∼ullmo, 2013.

[UYa] E. Ullmo and A. Yafaev. Galois orbits and equidistribution: towards the André-Oort conjecture. To appear in Ann. of Math. Available at www.math.u-psud.fr/∼ullmo.

[UYb] E. Ullmo and A. Yafaev. Nombre de classes des tores de multiplication complexe et bornes inférieures pour orbites Galoisiennes de points spéciaux. Available at www.math.u-psud.fr/∼ullmo.

[UY09] E. Ullmo and A. Yafaev. The André-Oort conjecture for products of modular curves. In *Ecole d'été arithmetic geometry*, Clay Math. Proc. Amer. Math. Soc., 2009.

[UY11] E. Ullmo and A. Yafaev. A characterisation of special subvarieties. *Mathematika*, 57(2):263–273, 2011.

[UY14] E. Ullmo and A. Yafaev. The hyperbolic Ax-Lindemann theorem in the cocompact case. *Duke Math. J.*, 163(2):267–463, 2014.

[Vas07] A. Vasiu. Geometry of Shimura varieties of Hodge type over finite fields. In *Proceedings of the NATO Advanced Study Institute on higher dimensional geometry over finite fields*. IOS Press, 2007.

[Vas12] A. Vasiu. Extension theorems for reductive group schemes. Available at arXiv.org, arXiv:0406508, 2012.

[vdG87] G. van der Geer. *Hilbert modular surfaces*. Springer-Verlag, 1987.

[vdGU82] G. van der Geer and K. Ueno. Families of abelian surfaces with real multiplications over Hilbert modular surfaces. *Nagoya Math. Journal*, 88:17–53, 1982.

[Vos98] V.E. Voskresensky. *Algebraic groups and their birational invariants*. American Mathematical Soc., 1998.

[Wat79] W.C. Waterhouse. *Introduction to affine group schemes*. Springer-Verlag New York Inc., 1979.

[Wol88] J. Wolfart. Werte hypergeometrische Funktionen. *Invent. Math.*, 92:187–216, 1988.

[Yaf01] A. Yafaev. Special points on products of two Shimura curves. *Manuscripta Math.*, 104:163–171, 2001.

[Yaf05] A. Yafaev. On a result of Moonen on the moduli space of principally polarized abelian varieties. *Compositio Math.*, 141(5):1103–1108, 2005.

[Yaf06] A. Yafaev. A conjecture of Yves André. *Duke Math. J.*, 132(3):393–407, 2006.

[Zha05] S-W. Zhang. Equidistribution of CM-points on quaternion Shimura varieties. *IMRN*, 59:3657–3689, 2005.

[Zil02] B. Zilber. Exponential sums equations and the Schanuel conjecture. *J. London Math. Soc.*, 65(2):27–44, 2002.