Canonical models of Shimura curves

J.S. Milne

April 4, 2003, v0.0

Abstract

As an introduction to Shimura varieties, and, in particular, to Deligne's Bourbaki and Corvallis talks (Deligne 1971, 1979), I explain the main ideas and results of the general theory of Shimura varieties in the context of Shimura curves.

These notes had their origin in a two-hour lecture I gave on September 10, 2002. They are available at www.jmilne.org/math/. Please send corrections and comments to me at math@jmilne.org.

Contents

Introduction

Let
$$X^{+}=\{z\in\mathbb{C}\mid\Im(z)>0\}.$$
Then $\mathrm{SL}_2(\mathbb{R})$ acts transitively on X^{+},
$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\cdot z=\frac{az+b}{cz+d},$$
and the subgroup fixing i is the compact group
$$\mathrm{SO}_2=\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix}\middle| a^2+b^2=1\right\}.$$
A *congruence subgroup* Γ of $\mathrm{SL}_2(\mathbb{Z})$ is any subgroup containing the *principal congruence subgroup of level* N,
$$\Gamma(N)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})\middle|\begin{pmatrix} a & b\\ c & d\end{pmatrix}\equiv\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}\bmod N\right\}.$$
Consider[1]
$$S_{\Gamma}^{\circ}\overset{\text{df}}{=}\Gamma\backslash X^{+}.$$
Initially, this is a Riemann surface, but when a finite set of points (the "cusps") is added, it becomes a compact Riemann surface, which is automatically[2] a nonsingular projective algebraic curve. Therefore, S_{Γ}° is an algebraic curve.[3]

The theorem I want to discuss is that S_{Γ}° has a canonical model C_{Γ}° over a certain number field F_{Γ}. More precisely, there exists a curve C_{Γ}° over F_{Γ} equipped with an isomorphism $(C_{\Gamma}^{\circ})_{\mathbb{C}}\to S_{\Gamma}^{\circ}$ satisfying certain natural conditions sufficient to determine it uniquely. So one thing I'll have to do is tell you how to attach a number field F_{Γ} to a congruence subgroup. Later, I'll discuss a similar theorem for curves $S_{\Gamma}^{\circ}=\Gamma\backslash X^{+}$ where Γ is again a congruence subgroup, but in a group different from SL_2.

Note that, in general, a variety over $\mathbb{C}$ will not have a model over a number field, and when it does, it will usually have many. For example, an elliptic curve E over $\mathbb{C}$ has a model over a number field if and only if its j-invariant $j(E)$ is an algebraic number, and if $Y^2Z=X^3+aXZ^2+bZ^3$ is one model of E over a number field k (meaning, $a,b\in k$), then $Y^2Z=X^3+ac^2XZ^2+bc^3Z^3$ is a second which is isomorphic to the first only if c is

[1]Unfortunately, in his Bourbaki talk, Deligne writes this as X^{+}/Γ. There used to be left-wingers (those who write the discrete group on the left) and right-wingers. Now there are only left-wingers — the right wingers either converted or ....

[2]The functor $C\mapsto C(\mathbb{C})$ from nonsingular projective curves over $\mathbb{C}$ to compact Riemann surfaces is an equivalence of categories. For a discussion of this result, see my notes on modular forms, 7.3–7.7.

[3]The same is not true of X^{+}, i.e., it is not possible to realize X^{+} (with its complex structure) as a Zariski-open subset of a nonsingular projective C curve over $\mathbb{C}$ — if you could, the complement of X^{+} in $C(\mathbb{C})$ would be a finite set, and any bounded holomorphic function on X^{+} would extend to a bounded holomorphic function on $C(\mathbb{C})$, and so would be constant, but $\frac{z-i}{z+i}$ is holomorphic on X^{+} and $\left|\frac{z-i}{z+i}\right|<1$.

This is one reason we work with $\Gamma\backslash X^{+}$ rather than X^{+} — as X^{+} is not an algebraic curve, it makes no sense to talk of it having a model over a number field.

a square in k. As another example, all the projective curves $aX^2 + bY^2 + cZ^2 = 0$ over $\mathbb{Q}$ become isomorphic to $X^2 + Y^2 + Z^2 = 0$ over $\mathbb{C}$, but they fall into infinitely many distinct isomorphism classes over $\mathbb{Q}$.

A problem with the theorem as stated above is that the fields F_Γ grow as Γ shrinks. One of Deligne's innovations in his Bourbaki talk was to replace (in a systematic way) the S_Γ° with nonconnected curves which have canonical models over $\mathbb{Q}$.

Notations and terminology

I use the language of algebraic varieties as, for example, in my course notes on algebraic geometry: the affine varieties over a field k are the ringed spaces $\operatorname{Specm} A$ with A a finitely generated k-algebra such that $A \otimes k^{\mathrm{al}}$ is reduced, and the varieties over k are the ringed spaces that are finite unions of open affine varieties satisfying a separatedness condition. Thus, a variety over k is essentially the same thing as a geometrically reduced separated scheme of finite type over k (not necessarily connected). For a variety V over k, $k[V] = \Gamma(V, \mathcal{O}_V)$ is the ring of regular functions on V and, when V is irreducible, $k(V)$ is the field of rational functions on V.

For simplicity, *throughout the notes "variety" will mean "nonsingular variety"*. With this convention, every connected variety is irreducible.

Throughout, $\mathbb{Q}^{\mathrm{al}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, and ι or $z \mapsto \bar{z}$ denotes complex conjugation on $\mathbb{C}$.

For a k-vector space V and a commutative k-algebra A, I often write $V(A)$ for the A-module $A \otimes_k V$.

Given an equivalence relation, [*] denotes the equivalence class containing *.

The notation $X \approx Y$ means that X and Y are isomorphic, whereas $X \cong Y$ means that they are canonically isomorphic or that there is a given (or unique) isomorphism.[4]

References

In addition to the references listed at the end, I refer to the following of my course notes.

GT	Group Theory	**FT**	Fields and Galois Theory.
AG	Algebraic Geometry.	**ANT**	Algebraic Number Theory
MF	Modular Functions and Modular Forms	**EC**	Elliptic Curves.
AV	Abelian Varieties.	**CFT**	Class Field Theory.

Prerequisites

I assume some familiarity with the classical theory of elliptic modular curves as, for example, in the first four sections of MF.

Acknowledgements

I thank the following for providing corrections and comments for an earlier version of the notes: Brian Conrad.

[4] For example, if V is a finite-dimensional vector space over a field k, then $V \approx V^\vee$ and $V \cong V^{\vee\vee}$.

1 Preliminaries

Algebraic varieties and their connected components

A variety V over a field k is said to be *geometrically connected* if $V_{k^{\mathrm{al}}}$ is connected, in which case, V_Ω is connected for every field Ω containing k (Hartshorne 1977, II, Exercise 3.15).

We first examine zero-dimensional varieties. Over $\mathbb{C}$, a zero-dimensional variety is nothing more than a finite set (finite disjoint union of copies $\mathbb{A}^0$). Over $\mathbb{R}$, a connected zero-dimensional variety V is either geometrically connected (e.g., $\mathbb{A}^0_{\mathbb{R}}$) or geometrically nonconnected (e.g., $V : X^2 + 1$; subvariety of $\mathbb{A}^1$), in which case $V(\mathbb{C})$ is a conjugate pair of complex points. Thus, one sees that to give a zero-dimensional variety over $\mathbb{R}$ is to give a finite set with an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

Similarly, a connected variety V over $\mathbb{R}$ may be geometrically connected, or it may decompose over $\mathbb{C}$ into a pair of conjugate varieties. Consider, for example, the following subvarieties of $\mathbb{A}^2$:

$L : Y + 1$ is a geometrically connected line over $\mathbb{R}$;

$L' : Y^2 + 1$ is connected over $\mathbb{R}$, but over $\mathbb{C}$ it decomposes as the pair of conjugate lines $Y = \pm i$.

Note that $\mathbb{R}$ is algebraically closed[5] in

$$\mathbb{R}[L] = \mathbb{R}[X, Y]/(Y + 1) \cong \mathbb{R}[X]$$

but not in

$$\mathbb{R}[L'] = \mathbb{R}[X, Y]/(Y^2 + 1) \cong \left(\mathbb{R}[Y]/(Y^2 + 1)\right)[X] \cong \mathbb{C}[X].$$

PROPOSITION 1.1. *A connected variety V over a field k is geometrically connected if and only if k is algebraically closed in $k(V)$.*

PROOF. This follows from the statement: let A be a finitely generated k-algebra such that A is an integral domain and $A \otimes_k k^{\mathrm{al}}$ is reduced; then $A \otimes k^{\mathrm{al}}$ is an integral domain if and only if k is algebraically closed in A (Zariski and Samuel 1958, III 15, Theorem 40). $\square$

PROPOSITION 1.2. *To give a zero-dimensional variety V over $\mathbb{Q}$ is to give (equivalently)*

(a) *a finite set E plus, for each $e \in E$, a finite field extension $\mathbb{Q}(e)$ of $\mathbb{Q}$, or*

(b) *a finite set S with a continuous*[6] *(left) action of $\Sigma =_{df} \mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$.*[7]

PROOF. The underlying topological space V of a zero-dimensional variety $(V, \mathcal{O}_V)$ is finite and discrete, and for each $e \in V$, $\Gamma(e, \mathcal{O}_V)$ is a finite field extension of $\mathbb{Q}$.

The set S in (b) is $V(\mathbb{Q}^{\mathrm{al}})$ with the natural action of Σ. We can recover $(V, \mathcal{O}_V)$ from S as follows: let V be the set $\Sigma\backslash S$ of orbits endowed with the discrete topology, and, for $e = \Sigma s \in \Sigma\backslash S$, let $\mathbb{Q}(e) = (\mathbb{Q}^{\mathrm{al}})^{\Sigma_s}$ where Σ_s is the stabilizer of s in Σ; then, for $U \subset V$, $\Gamma(U, \mathcal{O}_V) = \prod_{e \in U} \mathbb{Q}(e)$. $\square$

[5]A field k is algebraically closed in a k-algebra A if every $a \in A$ algebraic over k lies in k.

[6]This means that the action factors through the quotient of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ by an open subgroup (all open subgroups of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ are of finite index, but not all subgroups of finite index are open).

[7]The cognoscente will recognize this as Grothendieck's way of expressing Galois theory over $\mathbb{Q}$.

PROPOSITION 1.3. *Given a variety V over $\mathbb{Q}$, there exists a map $f\colon V \to \pi$ from V to a zero-dimensional variety π such that, for all $e \in \pi$, the fibre V_e is a geometrically connected variety over $\mathbb{Q}(e)$.*

PROOF. Let π be the zero-dimensional variety whose underlying set is the set of connected components of V over $\mathbb{Q}$ and such that, for each $e = V_i \in \pi$, $\mathbb{Q}(e)$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}(V_i)$. Apply (1.1) to see that the obvious map $f\colon V \to \pi$ has the desired property. □

EXAMPLE 1.4. Let V be a connected variety over a $\mathbb{Q}$, and let k be the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}(V)$. The map $f\colon V \to \operatorname{Specm} k$ realizes V as a geometrically connected variety over k. Conversely, for a geometrically connected variety $f\colon V \to \operatorname{Specm} k$ over a number field k, the composite of f with $\operatorname{Specm} k \to \operatorname{Specm} \mathbb{Q}$ realizes V as a variety over $\mathbb{Q}$ (connected, but not geometrically connected if $k \neq \mathbb{Q}$).

EXAMPLE 1.5. Let $f\colon V \to \pi$ be as in (1.3). When we regard π as a set with an action of Σ, then its points are in natural one-to-one correspondence with the connected components of $V_{\mathbb{Q}^{\mathrm{al}}}$ (equivalently $V_{\mathbb{C}}$) and its Σ-orbits are in natural one-to-one correspondence with the connected components of V. Let $e \in \pi$ and let $V' = f_{\mathbb{Q}^{\mathrm{al}}}^{-1}(e)$ — it is a connected component of $V_{\mathbb{Q}^{\mathrm{al}}}$. Let Σ_e be the stabilizer of e; then V' arises from a geometrically connected variety over $\mathbb{Q}(e) \overset{\mathrm{df}}{=} \mathbb{Q}^{\Sigma_e}$.

Easy descent theory

By descent (in these notes), I mean passing from objects over $\mathbb{C}$ to objects over $\mathbb{Q}$. One of the themes of these notes is that information on objects over $\mathbb{Q}$ (hence, possessing an interesting arithmetic) can be obtained from information on objects over $\mathbb{C}$ (hence, involving only analysis). Easy descent describes the information over $\mathbb{C}$ needed to determine a variety over $\mathbb{Q}$. Hard descent (see §3 below) will say which sets of information arise from varieties over $\mathbb{Q}$.

Let $\mathcal{A} = \operatorname{Aut}(\mathbb{C})$ (automorphisms of $\mathbb{C}$ as an abstract field). There are two obvious automorphisms, namely, the $z \mapsto z$ and $z \mapsto \iota z$ (complex conjugation), and the remainder can be constructed as follows. Recall that a transcendence basis B for $\mathbb{C}$ over $\mathbb{Q}$ is an algebraically independent set such that $\mathbb{C}$ is algebraic over $\mathbb{Q}(B)$. Transcendence bases exist (FT 8.13),[8] and any two have the same cardinality. Choose transcendence bases B and C for $\mathbb{C}$ over $\mathbb{Q}$; then any bijection $\sigma\colon B \to C$ defines an isomorphism of fields $\sigma\colon \mathbb{Q}(B) \to \mathbb{Q}(C)$, which extends to an automorphism of $\mathbb{C}$ (cf. FT 6.5).

For a vector space V over $\mathbb{Q}$, $\mathcal{A}$ acts on $V(\mathbb{C}) =_{\mathrm{df}} \mathbb{C} \otimes_{\mathbb{Q}} V$ through its action on $\mathbb{C}$:

$$\sigma(\textstyle\sum z_i \otimes v_i) = \textstyle\sum \sigma z_i \otimes v_i, \quad \sigma \in \mathcal{A}, \quad z_i \in \mathbb{C}, \quad v_i \in V.$$

LEMMA 1.6. *Let V be a vector space over $\mathbb{Q}$, and let W be a subspace of $\mathbb{C} \otimes V$. If W is stable under the action of $\mathcal{A}$, then $W \cap V$ spans W (and so $\mathbb{C} \otimes_{\mathbb{Q}} (W \cap V) \to W$ is an isomorphism).*

[8] This requires the Axiom of Choice. Probably, I could rewrite the notes to avoid assuming the Axiom of Choice, but that would complicate things.

PROOF. First note that $\mathbb{C}^{\mathcal{A}} = \mathbb{Q}$, i.e., every $z \in \mathbb{C} \smallsetminus \mathbb{Q}$ is moved by an element of $\mathcal{A}$: if z is transcendental, it is part of a transcendence basis for $\mathbb{C}$ over $\mathbb{Q}$, and any permutation of the transcendence basis extends to an automorphism of $\mathbb{C}$; if z is algebraic $\mathbb{Q}$, it is moved by an automorphism of $\mathbb{Q}^{\mathrm{al}}$, which extends to an automorphism of $\mathbb{C}$.

Next note that $(\mathbb{C} \otimes_{\mathbb{Q}} V)^{\mathcal{A}} = V$. To see this, choose[9] a basis $(e_i)_{i \in I}$ for V, and let $v = \sum z_i \otimes e_i \in \mathbb{C} \otimes_{\mathbb{Q}} V$. Then $\sigma v = \sum \sigma z_i \otimes e_i$ for $\sigma \in \mathcal{A}$, and so v is fixed by $\mathcal{A}$ if and only if each z_i is fixed.

We now prove the lemma. Let W' be a complement of $W \cap V$ in V, so that

$$V = (W \cap V) \oplus W'.$$

If $W \cap V$ doesn't span W, there will exist a nonzero $w \in W$ in the $\mathbb{C}$-span of W'. Choose a basis $(e_i)_{i \in I}$ for W', and write

$$w = \textstyle\sum_{i \in I} c_i e_i \quad (c_i \in \mathbb{C}).$$

We may suppose that w has been chosen so that the sum has the fewest nonzero coefficients c_i, and, after scaling, that $c_{i_0} = 1$ for some $i_0 \in I$. For $\sigma \in \mathcal{A}$, $\sigma w - w \in W$ and

$$\sigma w - w = \textstyle\sum_{i \neq i_0} (\sigma c_i - c_i) e_i$$

has fewer nonzero coefficients than w, and so $\sigma w - w = 0$. Since this holds for all σ, $w \in W \cap (V \otimes \mathbb{C})^{\mathcal{A}} = W \cap V$, which is a contradiction because

$$\mathbb{C} \otimes V = (\mathbb{C} \otimes (W \cap V)) \oplus (\mathbb{C} \otimes W').$$

□

PROPOSITION 1.7. *Let V be a variety over $\mathbb{Q}$, and let W be a closed subvariety of $V_{\mathbb{C}}$. If $W(\mathbb{C})$ is stable under the action of $\mathcal{A}$ on $V(\mathbb{C})$, then $W = W_{0\mathbb{C}}$ for a (unique) closed subvariety W_0 of V.*

PROOF. Suppose first that V is affine, and let $I(W) \subset \mathbb{C}[V_{\mathbb{C}}]$ be the ideal of functions zero on W. Because W is stable under $\mathcal{A}$, so also is $I(W)$, and so $I(W)$ is spanned by $I(W) \cap \mathbb{Q}[V]$ (Lemma 1.6). Therefore, the zero-set of $I(W) \cap \mathbb{Q}[V]$ is a closed subvariety W_0 of V with the property that $W = W_{0\mathbb{C}}$.

To deduce the general case, cover V with open affines. □

PROPOSITION 1.8. *Let V and W be varieties over $\mathbb{Q}$, and let $f\colon V_{\mathbb{C}} \to W_{\mathbb{C}}$ be a regular map. If f commutes with the actions of $\mathcal{A}$ on $V(\mathbb{C})$ and $W(\mathbb{C})$, then f arises from a (unique) regular map $V \to W$ over $\mathbb{Q}$.*

PROOF. Apply Proposition 1.7 to the graph of f, $\Gamma_f \subset (V \times W)_{\mathbb{C}}$. □

COROLLARY 1.9. *A variety V over $\mathbb{Q}$ is uniquely determined (up to a unique isomorphism) by $V_{\mathbb{C}}$ together with the action of $\mathcal{A}$ on $V(\mathbb{C})$.*

PROOF. An isomorphism $V_{\mathbb{C}} \to V'_{\mathbb{C}}$ commuting with the actions of $\mathcal{A}$ arises from a unique isomorphism $V \to V'$. □

REMARK 1.10. Proposition 1.8 says that the functor $V \mapsto (V_{\mathbb{C}}, \mathcal{A}\text{-action})$ is fully faithful. Later (hard descent theory) we shall determine the essential image of the functor, i.e., the pairs that arise (up to isomorphism) from varieties over $\mathbb{Q}$.

[9] Axiom of Choice again since we are not assuming V to be finite dimensional.

Adèles

Let $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ (product over the prime numbers $2, 3, 5, \ldots$). As each $\mathbb{Z}_\ell$ is compact, Tikhonov's theorem shows that $\hat{\mathbb{Z}}$ is a compact topological ring. It equals the inverse limit $\varprojlim \mathbb{Z}/m\mathbb{Z}$.

The *ring* $\mathbb{A}_f$ *of finite adèles* is defined to be the subring of $\prod_\ell \mathbb{Q}_\ell$ consisting of families $(a_\ell)_\ell$ such that $a_\ell \in \mathbb{Z}_\ell$ for almost all[10] ℓ. Thus $\mathbb{A}_f \supset \hat{\mathbb{Z}}$ and consists of the $\alpha \in \prod_\ell \mathbb{Q}_\ell$ such that $m\alpha \in \hat{\mathbb{Z}}$ for some m. In fact, $\mathbb{A}_f \cong \mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$. When endowed with the topology for which $\hat{\mathbb{Z}}$ is an open subring, $\mathbb{A}_f$ becomes a locally compact topological ring. A basis of neighbourhoods of 0 is formed by the sets $\prod U_\ell$ with U_ℓ an open neighbourhood of 0 in $\mathbb{Z}_\ell$ for all ℓ and equal to $\mathbb{Z}_\ell$ for almost all ℓ.

Similarly, for $G = \mathbb{G}_m$ ($=_{\text{df}} \mathrm{GL}_1$), SL_2, GL_2 etc., define the topological group $G(\mathbb{A}_f)$ to be

$$\{(a_\ell) \in \textstyle\prod_\ell G(\mathbb{Q}_\ell) \mid a_\ell \in G(\mathbb{Z}_\ell) \text{ for almost all } \ell\}$$

endowed with the topology for which $\prod_\ell G(\mathbb{Z}_\ell)$ is an open subgroup. It is locally compact. We embed $G(\mathbb{Q})$ in $G(\mathbb{A}_f)$ diagonally, $a \mapsto (a, a, a, \ldots)$.

For example, $\mathbb{G}_m(\mathbb{A}_f) = \mathbb{A}_f^\times$ (the *group of finite idèles*) is the topological group

$$\mathbb{A}_f^\times = \{(a_\ell) \in \textstyle\prod \mathbb{Q}_\ell^\times \mid a_\ell \in \mathbb{Z}_\ell^\times \text{ for almost all } \ell\}$$

endowed with the topology for which $\hat{\mathbb{Z}}^\times = \prod \mathbb{Z}_\ell^\times$ is an open subgroup. A basis for the neighbourhoods of 1 is formed by the sets $\prod U_\ell$ with U_ℓ an open neighbourhood of 1 in $\mathbb{Z}_\ell^\times$ for all ℓ and equal to $\mathbb{Z}_\ell$ for almost all ℓ. Note that $\mathbb{A}_f^\times$ is the group of units in $\mathbb{A}_f$, but the topology on it is stronger (has more open subsets) than the subspace topology.[11]

LEMMA 1.11. *The field* $\mathbb{Q}$ *(embedded diagonally) is dense in* $\mathbb{A}_f$.

PROOF. It suffices to prove the following statement: given an $\varepsilon > 0$ and elements $a_\ell \in \mathbb{Q}_\ell$ for ℓ in a finite set S, there exists an $a \in \mathbb{Q}$ such that

$$|a - a_\ell|_\ell < \varepsilon \text{ for } \ell \in S, \text{ and}$$
$$|a|_\ell \leq 1 \text{ for } \ell \notin S.$$

After replacing the a_ℓ with ma_ℓ for some $m \in \mathbb{Z}$ (and possibly changing ε and S), we may suppose that the a_ℓ lie in $\mathbb{Z}_\ell$. The Chinese remainder theorem states that

$$\mathbb{Z} \to \textstyle\prod_{\ell \in S} \mathbb{Z}/\ell^{n(\ell)}\mathbb{Z}$$

is surjective for all families $(n(\ell))_{\ell \in S}$, $n(\ell) > 0$. Any $a \in \mathbb{Z}$ having the same image in $\prod_{\ell \in S} \mathbb{Z}/\ell^{n(\ell)}\mathbb{Z}$ as $(a_\ell)_{\ell \in S}$ for sufficiently large $n(\ell)$ will satisfy the requirement. □

THEOREM 1.12 (STRONG APPROXIMATION). *The group* $\mathrm{SL}_2(\mathbb{Q})$ *is dense in* $\mathrm{SL}_2(\mathbb{A}_f)$.

---

[10] This means "for all but (possibly) finitely many".

[11] Let $\alpha(n)$ be the idèle whose n^{th} component is the n^{th} prime and whose other components are 1. Then $\alpha(n) \to 1$ as $n \to \infty$ in $\mathbb{A}_f$ but not in $\mathbb{A}_f^\times$.

PROOF. For any field k, $\mathrm{SL}_2(k)$ is generated by the subgroups

$$A(k)=\left\{\left(\begin{array}{cc}1 & a\\ 0 & 1\end{array}\right)\middle|\, a\in k\right\},\quad B(k)=\left\{\left(\begin{array}{cc}1 & 0\\ b & 1\end{array}\right)\middle|\, b\in k\right\}.$$

This follows, for example, from the equalities:

$$\begin{aligned}
\left(\begin{array}{cc}1 & \frac{a-1}{c}\\ 0 & 1\end{array}\right)\left(\begin{array}{cc}1 & 0\\ c & 1\end{array}\right)\left(\begin{array}{cc}1 & \frac{d-1}{c}\\ 0 & 1\end{array}\right) &= \left(\begin{array}{cc}a & \frac{ad-1}{c}\\ c & d\end{array}\right), \quad c\neq 0,\\
\left(\begin{array}{cc}1 & 0\\ \frac{a^{-1}-1}{b} & 1\end{array}\right)\left(\begin{array}{cc}1 & b\\ 0 & 1\end{array}\right)\left(\begin{array}{cc}1 & 0\\ \frac{a-1}{b} & 1\end{array}\right) &= \left(\begin{array}{cc}a & b\\ 0 & \frac{1}{a}\end{array}\right), \quad a,b\neq 0,\\
\left(\begin{array}{cc}1 & -ba\\ 0 & 1\end{array}\right)\left(\begin{array}{cc}1 & 0\\ \frac{a^{-1}-1}{b} & 1\end{array}\right)\left(\begin{array}{cc}1 & b\\ 0 & 1\end{array}\right)\left(\begin{array}{cc}1 & 0\\ \frac{a-1}{b} & 1\end{array}\right) &= \left(\begin{array}{cc}a & 0\\ 0 & \frac{1}{a}\end{array}\right), \quad a,b\neq 0.
\end{aligned}$$

In fact, the equalities show that, for any finite set of primes S, $\prod_{\ell\in S}\mathrm{SL}_2(\mathbb{Q}_\ell)$ is generated by its subgroups $\prod_{\ell\in S}A(\mathbb{Q}_\ell)$ and $\prod_{\ell\in S}B(\mathbb{Q}_\ell)$.

We now prove the theorem. According to the lemma, $A(\mathbb{A}_f)$ and $B(\mathbb{A}_f)$ are contained in the closure of $\mathrm{SL}_2(\mathbb{Q})$ (even of $A(\mathbb{Q})$ and $B(\mathbb{Q})$). Thus, the closure of $\mathrm{SL}_2(\mathbb{Q})$ contains $\prod_{\ell\in S}\mathrm{SL}_2(\mathbb{Q}_\ell)\times\prod_{\ell\neq S}1$ for every finite set S of primes, and these sets are obviously dense[12] in $\mathrm{SL}_2(\mathbb{A}_f)$. □

REMARK 1.13. The strong approximation theorem fails in each of the following cases:

(a) $\mathbb{G}_m$: the group $\mathbb{Q}^\times$ is not dense in $\mathbb{A}_f^\times$.[13]

(b) PGL_2: the determinant defines surjections

$$\begin{aligned}\mathrm{PGL}_2(\mathbb{Q}) &\to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}\\ \mathrm{PGL}_2(\mathbb{A}_f) &\to \mathbb{A}_f^\times/\mathbb{A}_f^{\times 2}\end{aligned}$$

and $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is not dense in $\mathbb{A}_f^\times/\mathbb{A}_f^{\times 2}$.

(c) The algebraic group G over $\mathbb{Q}$ such that $G(\mathbb{Q})$ is the group of elements of norm 1 in a quaternion division algebra D over $\mathbb{Q}$ for which $D\otimes\mathbb{R}$ is also a division algebra (hence isomorphic to the usual (Hamiltonian) quaternions). The proof in the case of SL_2 fails because G has no unipotent subgroups A, B, but the key reason that strong approximation fails for G is that $G(\mathbb{R})$ is compact, which forces $G(\mathbb{Q})$ to be too small.

These examples essentially exhaust the counterexamples to strong approximation: the general theorem says that $G(\mathbb{Q})$ is dense in $G(\mathbb{A}_f)$ whenever G is a simply connected semisimple group over $\mathbb{Q}$ without a $\mathbb{Q}$-factor H for which $H(\mathbb{R})$ is compact (Platonov and Rapinchuk 1994, Theorem 7.12, p427).

[12] Let $a=(a_\ell)\in\mathrm{SL}_2(\mathbb{A}_f)$ and let U be an open neighbourhood of 1. After possibly replacing U with a smaller open neighbourhood, we may suppose that $U=\prod U_\ell$. Let S be a finite set of primes containing all ℓ for which $a_\ell\notin\mathrm{SL}_2(\mathbb{Z}_\ell)$ or $U_\ell\neq\mathrm{SL}_2(\mathbb{Z}_\ell)$. Then $a\cdot U$ contains an element of $\prod_{\ell\in S}\mathrm{SL}_2(\mathbb{Q}_\ell)\times 1$.

[13] Let $(a_\ell)_\ell\in\prod\mathbb{Z}_\ell^\times\subset\mathbb{A}_f^\times$ and let S be a finite set. If $\mathbb{Q}^\times$ is dense, there is an $a\in\mathbb{Q}^\times$ that is close to a_ℓ for $\ell\in S$ and an ℓ-adic unit for $\ell\notin S$. But such an a would be an ℓ-adic unit for all ℓ, hence equal to ± 1, and so this is not always possible.

1.14 (CONGRUENCE SUBGROUPS OF $\mathrm{SL}_2(\mathbb{Q})$). The open subgroups of $\mathrm{SL}_2(\mathbb{A}_f)$ are those containing a basic open subgroup:

$$U = \prod\nolimits_\ell U_\ell,\ U_\ell \text{ open subgroup of } \mathrm{SL}_2(\mathbb{Q}_\ell) \text{ for all } \ell,\ U_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell) \text{ for almost all } \ell.$$

For a prime ℓ and $n \geq 0$, let

$$U_\ell(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_\ell) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \ell^n \right\}.$$

Thus,

$$U_\ell(n) = \mathrm{SL}_2(\mathbb{Z}_\ell) \iff n = 0.$$

For a fixed ℓ, the $U_\ell(n)$ form a basis of neighbourhoods of 1 in $\mathrm{SL}_2(\mathbb{Q}_\ell)$.

For a positive integer N, let

$$K(N) = \prod\nolimits_\ell U_\ell(\mathrm{ord}_\ell(N)).$$

Then the $K(N)$ form a basis of neighbourhoods of 1 in $\mathrm{SL}(\mathbb{A}_f)$, and

$$K(N) \cap \mathrm{SL}_2(\mathbb{Q}) = \Gamma(N).$$

Thus, for any open subgroup U of $\mathrm{SL}_2(\hat{\mathbb{Z}})$, $\Gamma = U \cap \mathrm{SL}_2(\mathbb{Q})$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. In fact, Γ is dense in U, and so there is a one-to-one correspondence between the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and the open subgroups $\mathrm{SL}_2(\hat{\mathbb{Z}})$:

$$\Gamma \leftrightarrow U, \quad \Gamma = U \cap \mathrm{SL}_2(\mathbb{Z}), \quad U = \text{closure of } \Gamma.$$

We define a *congruence subgroup of* $\mathrm{SL}_2(\mathbb{Q})$ to be any subgroup of the form

$$K \cap \mathrm{SL}_2(\mathbb{Q})$$

with K a compact open subgroup of $\mathrm{SL}_2(\mathbb{A}_f)$. A congruence subgroup is commensurable[14] with $\mathrm{SL}_2(\mathbb{Z})$ and contains $\Gamma(N)$ for some N. It is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ when it is contained in $\mathrm{SL}_2(\mathbb{Z})$.

ASIDE 1.15. Let V be a 2-dimensional vector space over $\mathbb{Q}$, and let $G = \mathrm{SL}(V)$, i.e., G is the algebraic group over $\mathbb{Q}$ such that, for any $\mathbb{Q}$-algebra R,

$$G(R) = \{\alpha \in \mathrm{End}_R(V(R)) \mid \det(\alpha) = 1\}.$$

Choose a lattice Λ in V, and define

$$G(\mathbb{A}_f) = \{(a_\ell) \in \prod G(\mathbb{Q}_\ell) \mid a_\ell \Lambda_\ell = \Lambda_\ell \text{ for almost all } \ell\}$$

[14]Two subgroups H_1 and H_2 of a group are said to be *commensurable* if $H_1 \cap H_2$ has finite index both in H_1 and in H_2. Evidently, if H_1 and H_2 are both compact and open, then $H_1/H_1 \cap H_2$ and $H_2/H_1 \cap H_2$ are both compact and discrete, and so H_1 and H_2 are commensurable. In particular, any two compact open subgroups of $\mathrm{SL}_2(\mathbb{A}_f)$ are commensurable, which implies that their intersections with $\mathrm{SL}_2(\mathbb{Q})$ are commensurable.

In general, a subgroup of $\mathrm{SL}_2(\mathbb{Q})$ commensurable with $\mathrm{SL}_2(\mathbb{Z})$ is said to be an *arithmetic subgroup*. Not all arithmetic subgroups are congruence.

where $\Lambda_\ell = \mathbb{Z}_\ell \otimes \Lambda$. If Λ' is a second lattice in V, then $\Lambda_\ell = \Lambda'_\ell$ for almost all ℓ, and so $G(\mathbb{A}_f)$ is independent of the choice of Λ. Endow $G(\mathbb{A}_f)$ with the obvious topology. A *congruence subgroup of* $G(\mathbb{Q})$ is any subgroup of the form $K \cap G(\mathbb{Q})$ with K a compact open subgroup of $G(\mathbb{A}_f)$. The choice of a basis for V determines an isomorphism $G \approx \mathrm{SL}_2$ under which the notions of congruence subgroup coincide. An advantage of the adèlic approach is that it only requires an algebraic group over $\mathbb{Q}$ (i.e., there is no need for a $\mathbb{Z}$-structure).

2 Elliptic modular curves over $\mathbb{C}$

We shall define a curve S_K over $\mathbb{C}$ which is a finite disjoint union of the curves $S_\Gamma^\circ = \Gamma\backslash X^+$ considered in the introduction, and we shall realize it as a moduli variety for elliptic curves with level structure. In the next section, we shall see that, unlike S_Γ°, S_K always has a canonical model over $\mathbb{Q}$.

The curve S_Γ° as a double coset space

PROPOSITION 2.1. *Let K be a compact open subgroup of $\mathrm{SL}_2(\mathbb{A}_f)$, and let*

$$\Gamma = K \cap \mathrm{SL}_2(\mathbb{Q})$$

be the corresponding congruence subgroup of $\mathrm{SL}_2(\mathbb{Q})$. The map $x \mapsto [x,1]$ defines a bijection

$$\Gamma\backslash X^+ \cong \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/K. \tag{1}$$

Here $\mathrm{SL}_2(\mathbb{Q})$ acts on both X^+ and $\mathrm{SL}_2(\mathbb{A}_f)$ on the left, and K acts on $\mathrm{SL}_2(\mathbb{A}_f)$ on the right:

$$q\cdot(x,a)\cdot k = (qx, qak), \quad q \in \mathrm{SL}_2(\mathbb{Q}), \quad x \in X^+, \quad a \in \mathrm{SL}_2(\mathbb{A}_f), \quad k \in K.$$

When we endow X^+ with its usual topology and $\mathrm{SL}_2(\mathbb{A}_f)$ with the adèlic topology (equivalently, the discrete topology), this becomes a homeomorphism.

PROOF. Consider

$$x \mapsto [x,1]\colon X^+ \to \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/K.$$

For $\gamma \in \Gamma = K \cap \mathrm{SL}_2(\mathbb{Q})$,

$$(\gamma x, 1) = (\gamma x, \gamma\cdot\gamma^{-1}) = \gamma(x,1)\gamma^{-1},$$

and so

$$[\gamma x, 1] = [x,1].$$

Thus, the map factors through $\Gamma\backslash X^+$.

By definition, $[x,1] = [x',1]$ if and only if there exist $q \in \mathrm{SL}_2(\mathbb{Q})$ and $k \in K$ such that $x' = qx$, $1 = qk$. The second equation implies that $q = k^{-1} \in \Gamma$, and so $[x] = [x']$ in $\Gamma\backslash X^+$. We have shown that

$$[x] \mapsto [x,1]\colon \Gamma\backslash X^+ \to \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/K$$

is injective, and it remains to show that it is surjective. Let $[x,a]$ be an element of the target space. Because K is open, the strong approximation theorem (1.12) shows that $\mathrm{SL}_2(\mathbb{A}_f) = \mathrm{SL}_2(\mathbb{Q})\cdot K$. Write $a = q\cdot k$, $q \in \mathrm{SL}_2(\mathbb{Q})$, $k \in K$. Then

$$(x,a) = (x,qk) = q(q^{-1}x,1)k$$

and so
$$[q^{-1}x] \mapsto [x,a].$$

Consider
$$\begin{array}{ccc} X^+ & \xrightarrow{x\mapsto(x,[1])} & X^+ \times (\mathrm{SL}_2(\mathbb{A}_f)/K) \\ \downarrow & & \downarrow \\ \Gamma\backslash X^+ & \xrightarrow{[x]\mapsto[x,1]} & \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/K. \end{array}$$

As K is open, $\mathrm{SL}_2(\mathbb{A}_f)/K$ is discrete, and so the upper map is a homeomorphism of X^+ onto its image, which is open. It follows easily that the lower map is a homeomorphism. □

ASIDE 2.2. (a) What happens when we pass to the inverse limit over Γ? There is a map
$$X^+ \to \varprojlim \Gamma\backslash X^+$$
which is injective because $\cap\Gamma = \{1\}$. Is the map surjective? The example
$$\mathbb{Z} \to \varprojlim \mathbb{Z}/m\mathbb{Z} = \hat{\mathbb{Z}}$$
is not encouraging — it suggests $\varprojlim \Gamma\backslash X^+$ might be some sort of completion of X^+ relative to the Γ's. This is correct. In fact, when we pass to the limit on the right in (1), we get the obvious answer, namely,
$$\varprojlim{}_K \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/K = \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f).$$
Why the difference? Well, given an inverse system $(G_i)_{i\in K}$ of groups acting on an inverse system $(S_i)_{i\in I}$ of topological spaces, there is always a canonical map
$$\varprojlim G_i\backslash \varprojlim S_i \to \varprojlim (G_i\backslash S_i)$$
and it is known that, under certain hypotheses, the map is an isomorphism (Bourbaki 1989, III §7). The system on the right in (1) satisfies the hypotheses; that on the left doesn't.

(b) Why replace the single coset space on the left with the more complicated double coset space on the right? One reason is that it makes transparent the action of $\mathrm{SL}_2(\mathbb{A}_f)$ on the inverse system $(\Gamma\backslash X^+)_\Gamma$, and hence, for example, the action of $\mathrm{SL}_2(\mathbb{A}_f)$ on
$$\varinjlim H^1(\Gamma\backslash X^+, \mathbb{Q}).$$
Another reason will be seen presently — we define S_K as a double coset. Double coset spaces are pervasive in work on the Langlands program.[15]

[15] Casselman 2001, p220, writes: Tamagawa tells me it might have been Taniyama who first noticed that one could translate classical automorphic forms to certain function on adèle quotients.

A finiteness statement

LEMMA 2.3. *For any compact open subgroup K of $\mathrm{GL}_2(\mathbb{A}_f)$,*

$$\mathbb{Q}^\times \backslash \{\pm\} \times \mathbb{A}_f^\times / \det K$$

is finite and discrete. Here $\{\pm\} = \{+, -\}$ is a discrete two-element set, $\mathbb{Q}^\times$ acts on both sets on the left, and $\det K$ acts on $\mathbb{A}_f^\times$ on the right.

PROOF. The map

$$(r, (u_\ell)_\ell) \mapsto (\mathrm{sign}(r), (ru_\ell)_\ell) \colon \mathbb{Q}^\times \times \prod \mathbb{Z}_\ell^\times \to \{\pm\} \times \mathbb{A}_f^\times$$

is a topological isomorphism (discrete topology on $\mathbb{Q}^\times$) — cf. CFT V 5.9. Therefore,

$$\mathbb{Q}^\times \backslash \{\pm\} \times \mathbb{A}_f^\times \cong \hat{\mathbb{Z}}^\times,$$

which is compact. On the other hand, $\det(K)$ is open, and so $\left(\{\pm\} \times \mathbb{A}_f^\times\right) / \det(K)$ is discrete. On combining these statements, we find that $\mathbb{Q}^\times \backslash \{\pm\} \times \mathbb{A}_f^\times / \det K$ is compact and discrete, and is therefore finite. $\square$

REMARK 2.4. From the projection

$$\{\pm\} \times \mathbb{A}_f^\times \to \mathbb{A}_f^\times$$

we obtain a topological isomorphism

$$\mathbb{Q}^\times \backslash \{\pm\} \times \mathbb{A}_f^\times \to \mathbb{Q}^{>0} \backslash \mathbb{A}_f^\times$$

and hence a bijection

$$\mathbb{Q}^\times \backslash \{\pm\} \times \mathbb{A}_f^\times / \det K \to \mathbb{Q}^{>0} \backslash \mathbb{A}_f^\times / \det K.$$

The curve S_K

Let X be the complex plane with the real axis removed:

$$X = \mathbb{C} \smallsetminus \mathbb{R} = X^+ \sqcup X^-.$$

Then $\mathrm{GL}_2(\mathbb{R})$ acts transitively on X:

$$\alpha(z) = \frac{az+b}{cz+d}, \quad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}). \tag{2}$$

Note that

$$\Im(\alpha z) = \Im\left(\frac{az+b}{cz+d}\right) = \Im\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = \frac{\Im(adz+bc\bar{z})}{|cz+d|^2} = \frac{(ad-bc)\cdot\Im(z)}{|cz+d|^2},$$

and so α preserves the upper half-plane or interchanges it with the lower half-plane according as $\det(\alpha) > 0$ or $\det(\alpha) < 0$.

LEMMA 2.5. *Let K be a compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$. For any $a_0 \in \mathrm{GL}_2(\mathbb{A}_f)$, the fibre of*

$$[x,a] \mapsto [[x], \det a] \colon \mathrm{GL}_2(\mathbb{Q})\backslash X \times \mathrm{GL}_2(\mathbb{A}_f)/K \to \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times/\det(K)$$

containing $[X^+, a_0]$ is

$$\mathrm{SL}_2(\mathbb{Q})\backslash \left(X^+ \times \mathrm{SL}_2(\mathbb{A}_f)\cdot a_0\right)/K \cap \mathrm{SL}_2(\mathbb{A}_f).$$

PROOF. We shall use the following (obvious) statement:

> (*) Let G be a group, and let $f\colon A \to B$ be a map of G-sets; for each $b \in B$, the fibre of $G\backslash A \to G\backslash B$ over $G\cdot b$ is $G_b\backslash f^{-1}(b)$ where G_b stabilizer of b in G.

We apply this first to

$$(x,a) \mapsto ([x], \det a)\colon X \times \mathrm{GL}_2(\mathbb{A}_f) \to \{\pm\} \times \mathbb{A}_f^\times$$

regarded as a map of $\mathrm{GL}_2(\mathbb{Q})$-sets. Note that $\mathrm{GL}_2(\mathbb{Q})$ acts on $\{\pm\}\times\mathbb{A}_f^\times$ through its quotient $\mathbb{Q}^\times$. For any $(+,b) \in \{+\} \times \mathbb{A}_f^\times$, the stabilizer of $(+,b)$ in $\mathrm{GL}_2(\mathbb{Q})$ is $\mathrm{SL}_2(\mathbb{Q})$, and so (*) shows that the fibre of

$$\mathrm{GL}_2(\mathbb{Q})\backslash X \times \mathrm{GL}_2(\mathbb{A}_f) \to \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times$$

over $\mathbb{Q}^\times\cdot(+,b)$ is $\mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)\cdot a_0$ where a_0 is any element of $\mathrm{GL}_2(\mathbb{A}_f)$ with $\det(a_0) = b$.

Next note that K acts on $\mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times$ through its quotient $\det(K)$. For any $[+,b] \in \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times$ the stabilizer of $[+,b]$ in K is $K \cap \mathrm{SL}_2(\mathbb{A}_f)$, and so (*) shows that the fibre over $[+,b]$ is

$$\mathrm{SL}_2(\mathbb{Q})\backslash \left(X^+ \times \mathrm{SL}_2(\mathbb{A}_f)\cdot a_0\right)/K \cap \mathrm{SL}_2(\mathbb{A}_f)$$

with a_0 as before. $\square$

REMARK 2.6. Of course, the lemma holds with $+$ replaced by $-$, but we won't need this because every fibre of the map contains $[X^+, a]$ for some a.

On taking $a_0 = 1$ in the lemma, we obtain a fibre product diagram:

$$\begin{tikzcd}
\mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/K \cap \mathrm{SL}_2(\mathbb{A}_f) \arrow[r, hook] \arrow[d] & \mathrm{GL}_2(\mathbb{Q})\backslash X \times \mathrm{GL}_2(\mathbb{A}_f)/K \arrow[d, "\mathrm{sign}\times\det"] \\
\{[+,1]\} \arrow[r, hook] & \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times/\det(K).
\end{tikzcd}$$

Therefore, according to (2.1), the fibre over $[+,1]$ is the connected curve $\Gamma\backslash X^+$ with $\Gamma = K \cap \mathrm{SL}_2(\mathbb{Q})$. A similar remark applies to all fibres.

PROPOSITION 2.7. *Let K be a compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$, and let $b_1, \ldots, b_h$ be a set of representatives in $\mathbb{A}_f^\times$ for the orbits in $\mathbb{Q}^{>0}\backslash\mathbb{A}_f^\times$. For each i, choose an $a_i \in \mathrm{GL}_2(\mathbb{A}_f)$ with $\det(a_i) = b_i$, and let $\Gamma_i = \mathrm{SL}_2(\mathbb{Q}) \cap a_i K a_i^{-1}$. Then Γ_i is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Q})$, and the maps*

$$[x_i] \mapsto [x_i, a_i] \colon \Gamma_i\backslash X^+ \to \mathrm{GL}_2(\mathbb{Q})\backslash X \times \mathrm{GL}_2(\mathbb{A}_f)/K \tag{3}$$

define a topological isomorphism

$$\coprod \Gamma_i\backslash X^+ \to \mathrm{GL}_2(\mathbb{Q})\backslash X \times \mathrm{GL}_2(\mathbb{A}_f)/K. \tag{4}$$

PROOF. Clearly, $\mathrm{SL}_2(\mathbb{A}_f) \cap a_i K a_i^{-1}$ is a compact open subgroup of $\mathrm{SL}_2(\mathbb{A}_f)$, and so its intersection with $\mathrm{SL}_2(\mathbb{Q})$ is a congruence subgroup. We have canonical isomorphisms

$$\begin{aligned} \Gamma_i\backslash X^+ &\xrightarrow{(2.1)} \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)/\,\mathrm{SL}_2(\mathbb{A}_f) \cap a_i K a_i^{-1} \\ &\xrightarrow{[x,a]\mapsto[x,a\cdot a_i]} \mathrm{SL}_2(\mathbb{Q})\backslash X^+ \times \mathrm{SL}_2(\mathbb{A}_f)\cdot a_i/\,\mathrm{SL}_2(\mathbb{A}_f) \cap K \\ &\xrightarrow{(2.5)} \text{fibre over } [+, b_i] \text{ in } \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times/\det K. \end{aligned}$$

Thus, the statement follows from Lemma 2.3. □

DEFINITION 2.8. For a compact open subgroup K of $\mathrm{GL}_2(\mathbb{Q})$, S_K is the algebraic curve over $\mathbb{C}$ for which

$$S_K(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})\backslash X \times \mathrm{GL}_2(\mathbb{A}_f)/K$$

and (4) is an isomorphism of Riemann surfaces.

Thus, S_K is an algebraic curve over $\mathbb{C}$ such that

(a) the set of connected components of S_K,

$$\pi_0(S_K) \cong \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times/\det(K)$$

(b) each connected component of S_K is a curve S_Γ° for a suitable congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Q})$.

REMARK 2.9. For varying K, the S_K form a variety (scheme) with a right action of $\mathrm{GL}_2(\mathbb{A}_f)$ in the sense of Deligne 1979, 2.7.1. This means the following:

(a) the S_K form an inverse system of algebraic curves indexed by the compact open subgroups K of $\mathrm{GL}_2(\mathbb{A}_f)$ (if $K \subset K'$, there is an obvious quotient map $S_{K'} \to S_K$);

(b) there is an action ρ of $\mathrm{GL}_2(\mathbb{A}_f)$ on the system $(S_K)_K$ defined by isomorphisms (of algebraic curves) $\rho_K(a) \colon S_K \to S_{g^{-1}Kg}$ (on points, $\rho_K(a)$ is $[x, a'] \mapsto [x, a'a]$);

(c) for $k \in K$, $\rho_K(k)$ is the identity map; therefore, for K' normal in K, there is an action of the finite group K/K' on $S_{K'}$; the curve S_K is the quotient of $S_{K'}$ by the action of K/K'.

REMARK 2.10. When we regard the S_K as schemes, the inverse limit of this system in (2.9) exists[16]:

$$S = \varprojlim S_K.$$

This is a scheme over $\mathbb{C}$, not(!) of finite type, with a right action of $\mathrm{GL}_2(\mathbb{A}_f)$, and, for K a compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$,

$$S_K = S/K$$

(Deligne 1979, 2.7.1). Thus, the system $(S_K)_K$ together with its right action of $\mathrm{GL}_2(\mathbb{A}_f)$ can be recovered from S with its right action of $\mathrm{GL}_2(\mathbb{A}_f)$. Moreover,

$$S(\mathbb{C}) \cong \varprojlim S_K(\mathbb{C}) = \varprojlim G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K \cong G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f).$$

The first isomorphism follows from the definition of inverse limits,

$$S(\mathbb{C}) \overset{\text{df}}{=} \mathrm{Hom}(\operatorname{Spec}\mathbb{C}, S) \cong \varprojlim \mathrm{Hom}(\operatorname{Spec}\mathbb{C}, S_K) \overset{\text{df}}{=} \varprojlim S_K(\mathbb{C}),$$

and the second requires Bourbaki 1989, III 7.2.

REMARK 2.11. The curves S_Γ° for Γ a *torsion-free* congruence subgroup of $\mathrm{SL}_2(\mathbb{Q})$ have the following remarkable property: every holomorphic map $V \to S_\Gamma^\circ$ from a smooth complex algebraic variety V to S_Γ° is a morphism of algebraic varieties (Borel 1972, 3.10). Note that this is false without the condition that Γ be torsion-free: $S_{\Gamma(1)}^\circ \approx \mathbb{A}^1$ and there are certainly holomorphic maps $\mathbb{A}^1(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$, i.e., $\mathbb{C} \to \mathbb{C}$, that are not regular, for example, e^z.

Re-interpretation of X

Let V be a finite dimensional vector space over $\mathbb{R}$. By a *complex structure* on V we mean an $\mathbb{R}$-linear action of $\mathbb{C}$ on V, i.e., a homomorphism of $\mathbb{R}$-algebras $h\colon \mathbb{C} \to \mathrm{End}_{\mathbb{R}}(V)$.

PROPOSITION 2.12. *The following sets are in natural one-to-one correspondence:*

(a) *the complex structures on V;*

(b) *the endomorphisms J of V such that $J^2 = -1$;*

[16] Let $(A_i)_{i\in I}$ be a direct system of commutative rings indexed by a directed set I, and let $A = \varinjlim A_i$. Then, for any scheme X,

$$\mathrm{Hom}(X, \operatorname{Spec} A) \cong \mathrm{Hom}(A, \Gamma(X, \mathcal{O}_X)) \cong \varprojlim \mathrm{Hom}(A_i, \Gamma(X, \mathcal{O}_X)) \cong \varprojlim \mathrm{Hom}(X, \operatorname{Spec} A_i).$$

(For the first and third isomorphisms, see Hartshorne 1977, II, Exercise 2.4; the middle isomorphism is the definition of direct limit). This shows that $\operatorname{Spec} A$ is the inverse limit of the inverse system $(\operatorname{Spec} A_i)_{i\in I}$ in the category of schemes. More generally, inverse limits of schemes in which the transition morphisms are affine exist, and can be constructed in the obvious way. In our case, the schemes S_K, being noncomplete curves, are themselves affine.

(c) *the pairs*[17] *of subspaces* (V^+, V^-) *of* $V(\mathbb{C})$ *such that* $\iota V^+ = V^-$ *and* $V(\mathbb{C}) = V^+ \oplus V^-$ *(here* ι *denotes complex conjugation* $\iota \otimes 1$ *on* $\mathbb{C} \otimes V = V(\mathbb{C})$*);*

(d) *(case* $\dim V = 2$*) the nonreal lines* W *in* $V(\mathbb{C})$ *passing through* 0 *(nonreal means* $W \neq \iota W$*).*

PROOF. (a)↔(b). Given a complex structure h, take $J = h(i)$. Conversely, given J, let $\mathbb{C}$ act through the isomorphism $a + bi \mapsto a + bJ\colon \mathbb{C} \to \mathbb{R}[J]$.

(b)↔(c). Given J, define V^+ and V^- to be the $+i$ and $-i$ eigenspaces of $1 \otimes J$ acting on $\mathbb{C} \otimes V$. Conversely, given (V^+, V^-), define J to be the operator on $V(\mathbb{C})$ that acts as $+i$ on V^+ and $-i$ on V^-. Because V^+ and V^- are complex conjugates of each other, J commutes with the action of ι,[18] and so preserves $V \subset V(\mathbb{C})$.

(c)→(a). The map $V \to V(\mathbb{C})/V^-$ is an isomorphism of real vector spaces, and so V acquires a complex structure from that on $V(\mathbb{C})/V^-$.

(c)↔(d). The subspace V^- determines the pair (V^+, V^-), and it can be any nonreal line when $\dim V = 2$; we let $(V^+, V^-) \leftrightarrow V^-$. □

2.13. Now take V to have dimension 2, and let Y be the set of complex structures on V. Let $\mathbb{P}^1 = \mathbb{P}(V)$, the projective space of lines through 0 in $V(\mathbb{C})$. The map sending a complex structure (V^+, V^-) on V to V^- is a bijection from Y onto $\mathbb{P}^1(\mathbb{C}) \smallsetminus \mathbb{P}^1(\mathbb{R})$. This bijection endows Y with the structure of a complex manifold. Note that

$$\mathbb{C} \smallsetminus \mathbb{R} = \mathbb{P}^1(\mathbb{C}) \smallsetminus \mathbb{P}^1(\mathbb{R}).$$

The choice of a basis for V identifies Y with X.

ASIDE 2.14. Observe that the map

$$z \mapsto \frac{z-i}{z+i} \tag{5}$$

sends i to 0 and the real line onto the unit circle $|z| = 1$ (because, if z is real, then $z - i$ is the complex conjugate of $z + i$). Therefore, it maps X^+ isomorphically (conformally) onto the interior of the disk, and it maps X isomorphically onto $\mathbb{P}^1(\mathbb{C}) \smallsetminus \{\text{unit circle}\}$.

Elliptic curves over $\mathbb{C}$

Define $\mathcal{T}$ to be the category:

---

[17] The cognoscente will recognize this as a Hodge structure of type $(-1, 0), (0, -1)$ on V. Implicitly, we are using Deligne's convention (Deligne 1979, 1.3) that $h(z)$ acts on $V^{p,q}$ as $z^{-p}\bar{z}^{-q}$.

[18] Let $x \in W^+$, $y \in W^-$. Then

$$\begin{aligned} \iota J(x+y) &= \iota(ix - iy) && \text{(definition of } J\text{)} \\ &= -i\iota x + i\iota y && (\iota \text{ is semilinear}) \\ &= J(\iota x + \iota y) && (\iota \text{ switches } W^+ \text{ and } W^-). \end{aligned}$$

OBJECTS: triples (V, J, Λ) with V a two-dimensional real vector space, J a complex structure on V, and Λ a lattice in V;

MORPHISMS: a morphism $(V, J, \Lambda) \to (V', J', \Lambda')$ is an $\mathbb{R}$-linear map $\alpha\colon V \to V'$ such that $J' \circ \alpha = \alpha \circ J'$ and $\alpha\Lambda \subset \Lambda'$.

Let $\mathsf{Ell}(\mathbb{C})$ be the category of elliptic curves over $\mathbb{C}$.

THEOREM 2.15. *The functor*

$$(V, J, \Lambda) \mapsto (V, J)/\Lambda\colon \mathcal{T} \to \mathsf{Ell}(\mathbb{C})$$

is an equivalence of categories.

PROOF. By $(V, J)/\Lambda$ we mean the quotient of the one-dimensional complex vector space (V, J) by the lattice Λ. Certainly, $(V, J, \Lambda) \mapsto (V, J)/\Lambda$ defines a functor from $\mathcal{T}$ to the category of compact Riemann surfaces of genus 1 provided with a "zero". That it is fully faithful (i.e., bijective on arrows) follows from EC 10.3. Now $(V, J)/\Lambda$ has a unique structure of a nonsingular algebraic curve of genus 1 (cf. footnote 2, p3, or use $\wp$ and $\wp'$ to embed $(V, J)/\Lambda$ in $\mathbb{P}^2$). Thus, we have a fully faithful functor $\mathcal{T} \to \mathsf{Ell}(\mathbb{C})$, and to show that it is an equivalence of categories, it remains to show that every elliptic curve over $\mathbb{C}$ is isomorphic to a curve of the form $(V, J)/\Lambda$. In fact, every elliptic curve over $\mathbb{C}$ is isomorphic to a curve of the form $\mathbb{C}/\Lambda$ (EC 10.14). $\square$

REMARK 2.16. We can define a quasi-inverse to $(V, J, \Lambda) \mapsto (V, J)/\Lambda\colon \mathcal{T} \to \mathsf{Ell}(\mathbb{C})$ as follows: the Abel-Jacobi mapping

$$P \mapsto \left(\omega \mapsto \int_0^P \omega\right) : E(\mathbb{C}) \to \frac{H^0(E, \Omega^1)^\vee}{H_1(E(\mathbb{C}), \mathbb{Z})}$$

is an isomorphism (easy case of the Abel-Jacobi theorem, Fulton 1995, 20.25). Thus, we can take $\Lambda = H_1(E(\mathbb{C}), \mathbb{Z})$ and $V = H^0(E, \Omega^1)^\vee$ with its natural complex structure.

Alternatively, because Λ is a lattice in $H^0(E, \Omega^1)^\vee$,

$$\mathbb{R} \otimes \Lambda \cong H^0(E, \Omega^1)^\vee \cong \mathrm{Tgt}_0(E). \tag{6}$$

Thus, we can take $\Lambda = H_1(E, \mathbb{Z})$, $V = H_1(E, \mathbb{R})$ ($\cong \mathbb{R} \otimes \Lambda$), and J equal to the complex structure on V defined by the canonical isomorphism $V \cong \mathrm{Tgt}_0(E)$.

Let $\mathsf{Ell}^0(\mathbb{C})$ be the category[19] whose objects are elliptic curves over $\mathbb{C}$, but whose morphisms are given by

$$\mathrm{Hom}^0(E_1, E_2) = \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}.$$

Let $\mathcal{T}^0$ be the category whose objects are pairs (V, J) with V a two-dimensional $\mathbb{Q}$-vector space and J a complex structure on $V \otimes \mathbb{R}$.

[19] This is called the category of "elliptic curves up to isogeny" — see Mumford 1970, p172. Presumably the name was suggested by the fact that two elliptic curves are isomorphic in $\mathsf{Ell}^0(\mathbb{C})$ if and only if they are isogenous. The name is unfortunate: a bit like referring to $\mathsf{Ell}(\mathbb{C})$ as the category of elliptic curves up to isomorphism. However, we seem to be stuck with it.

COROLLARY 2.17. *There is an equivalence of categories* $\mathcal{T}^0 \to \mathsf{Ell}^0(\mathbb{C})$.

PROOF. Obviously, the functor in (2.15) defines an equivalence of $\mathsf{Ell}^0(\mathbb{C})$ with the category obtained from $\mathcal{T}$ by tensoring the Hom's with $\mathbb{Q}$, but the functor $(V, J, \Lambda) \mapsto (\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda, J)$ is an equivalence of this category with $\mathcal{T}^0$. □

The above results are not difficult to prove, but they and their higher dimensional analogues are quite remarkable: they show that the study of elliptic curves and abelian varieties over $\mathbb{C}$, which are richly interesting objects, is nothing more than linear algebra. Note that for an automorphism σ of $\mathbb{C}$ and an elliptic curve E, the curve σE makes sense — it is the elliptic curve obtained by applying σ to the coefficients of a polynomial defining E — whereas, applying σ to an object of $\mathcal{T}$ has no obvious meaning (except via the equivalence of $\mathcal{T}$ with $\mathsf{Ell}(\mathbb{C})$).

NOTATIONS 2.18. For an elliptic curve E over $\mathbb{C}$, we let

$$T_f E = H_1(E, \mathbb{Z}) \otimes \hat{\mathbb{Z}}, \quad V_f E = H_1(E, \mathbb{Z}) \otimes \mathbb{A}_f.$$

If $E(\mathbb{C}) = (V, J)/\Lambda$, then

$$H_1(E, \mathbb{Z}) \cong \Lambda, \quad H_1(E, \mathbb{Q}) \cong \mathbb{Q} \otimes \Lambda,$$

and so

$$T_f E = \Lambda \otimes \hat{\mathbb{Z}}, \quad V_f E = \Lambda \otimes \mathbb{A}_f.$$

In particular, $T_f E$ is a free $\hat{\mathbb{Z}}$-module of rank 2, and $V_f E$ is a free $\mathbb{A}_f$-module of rank 2.

Let $E[N]$ denote the subgroup of $E(\mathbb{C})$ of points killed by N. If $E(\mathbb{C}) = (V, J)/\Lambda$, then

$$E[N] \cong \tfrac{1}{N}\Lambda/\Lambda \cong \Lambda/N\Lambda,$$

and so, on passing to the inverse limit, we find that

$$T_f E \cong \varprojlim E[N]$$

and

$$V_f(E) \cong T_f E \otimes \mathbb{Q}.$$

Note that $E \mapsto V_f E$ is a functor on both $\mathsf{Ell}(\mathbb{C})$ and $\mathsf{Ell}^0(\mathbb{C})$, but $E \mapsto T_f E$ is a functor only on $\mathsf{Ell}(\mathbb{C})$.

Elliptic modular curves as parameter spaces over $\mathbb{C}$

Now fix a two-dimensional $\mathbb{Q}$-vector space V, and let $G = \mathrm{GL}(V)$, i.e., G is the algebraic group over $\mathbb{Q}$ such that $G(R) = \mathrm{Aut}_R(V(R))$ for any $\mathbb{Q}$-algebra R. In particular,

$$G(\mathbb{A}_f) = \mathrm{Aut}_{\mathbb{A}_f}(V(\mathbb{A}_f)).$$

We now define X to be the set of complex structures J on $V(\mathbb{R})$ (cf. 2.13), and we let $G(\mathbb{Q})$ act on X by conjugation:

$$qJ = q \circ J \circ q^{-1}.$$

The choice of a basis for V identifies G with GL_2, X with the space in $\mathbb{C} \smallsetminus \mathbb{R}$, and the action of G on X with that in (2), but making such a choice would only confuse things.

For a compact open subgroup K of $G(\mathbb{A}_f)$, let S_K be the (nonconnected) algebraic curve over $\mathbb{C}$ such that

$$S_K(\mathbb{C}) = G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$$

(see 2.8).

Consider the set $\mathcal{E}$ of pairs (E, η) with E an elliptic curve over $\mathbb{C}$ and η an $\mathbb{A}_f$-linear isomorphism

$$V(\mathbb{A}_f) \to V_f(E).$$

An isomorphism $(E, \eta) \to (E', \eta')$ is an isomorphism $\alpha\colon E \to E'$ in $\mathsf{Ell}^0(\mathbb{C})$ such that

$$\begin{tikzcd}
 & V(\mathbb{A}_f) \arrow[dl, "\eta"'] \arrow[dr, "\eta'"] & \\
V_f(E) \arrow[rr, "V_f(\alpha)"] & & V_f(E')
\end{tikzcd}$$

commutes. There is a natural action of $G(\mathbb{A}_f)$ on $\mathcal{E}$,

$$\mathcal{E} \times G(\mathbb{A}_f) \to \mathcal{E}, \quad (E, \eta), a \mapsto (E, \eta \circ a),$$

which preserves isomorphism classes: $(E, \eta) \overset{\alpha}{\approx} (E', \eta') \implies (E, \eta \circ a) \overset{\alpha}{\approx} (E', \eta' \circ a)$.

$$\begin{tikzcd}
 & V(\mathbb{A}_f) \arrow[d, "a"] \arrow[ddl, "\eta\circ a"'] \arrow[ddr, "\eta'\circ a"] & \\
 & V(\mathbb{A}_f) \arrow[dl, "\eta"'] \arrow[dr, "\eta'"] & \\
V_f(E) \arrow[rr, "V_f(\alpha)"] & & V_f(E').
\end{tikzcd}$$

Given (E, η) in $\mathcal{E}$, choose an isomorphism

$$\alpha\colon H_1(E, \mathbb{Q}) \to V.$$

Let J be the complex structure on $V \otimes \mathbb{R}$ corresponding to the complex structure on $H_1(E, \mathbb{R})$ (see 2.16), and let a be the composite

$$V \otimes \mathbb{A}_f \xrightarrow{\eta} V_f(E) \xrightarrow{\alpha\otimes 1} V(\mathbb{A}_f).$$

Thus, from (E, η) and a choice of α, we obtain a pair

$$(J, a) \in X \times G(\mathbb{A}_f).$$

When α is replaced by $q \circ \alpha$, (J, α) is replaced by $(qJ, q\alpha)$, and so we have a well-defined map

$$\mathcal{E} \to G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f).$$

PROPOSITION 2.19. *The map just defined gives a bijection*

$$\mathcal{E}/{\approx} \to G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f).$$

It is compatible with the action of K, and therefore induces a bijection

$$(\mathcal{E}/{\approx})/K \to S_K(\mathbb{C}).$$

PROOF. Using (2.17), we see that isomorphism classes of pairs (E, η) are in one-to-one correspondence with isomorphism classes of triples (W, J, a) where W is a two-dimensional $\mathbb{Q}$-vector space, J is a complex structure on W, and a is an isomorphism $V(\mathbb{A}_f) \to W(\mathbb{A}_f)$. But any such triple is isomorphic to one with $W = V$. Thus $\mathcal{E}/{\approx}$ is in one-to-one correspondence with the isomorphism classes of pairs (J, a) where J is a complex structure on V and a is an isomorphism $V(\mathbb{A}_f) \to V(\mathbb{A}_f)$, i.e., with isomorphism classes of pairs in $X \times G(\mathbb{A}_f)$. An isomorphism $(J, a) \to (J', a')$ is an isomorphism $q\colon V \to V$ of $\mathbb{Q}$-vector spaces carrying J to J' and a to a'. Thus, the isomorphism classes of pairs are the orbits of $X \times G(\mathbb{A}_f)$ under the action of $G(\mathbb{Q}) = \mathrm{Aut}(V)$.

It follows from the definitions that the bijection is compatible with the action of K. Therefore, on passing to the quotient, we obtain a bijection

$$(\mathcal{E}/{\approx})/K \to G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K \overset{\text{df}}{=} S_K(\mathbb{C}).$$

□

REMARK 2.20. Let K be a compact open subgroup $G(\mathbb{A}_f)$, and let E be an elliptic curve over $\mathbb{C}$. For an isomorphism $\eta\colon V(\mathbb{A}_f) \to V_f E$, write $[\eta]_K$ for the K-orbit $\{\eta \circ a \mid a \in K\}$ of η. Define $\mathcal{E}_K$ to be the set of pairs $(E, [\eta]_K)$. With the obvious notion of isomorphism for objects in $\mathcal{E}_K$, there is a commutative diagram of bijections

$$\begin{array}{ccc}
(\mathcal{E}/{\approx})/K & \xrightarrow{1:1} & \left(G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)\right)/K \\
\downarrow{\scriptstyle 1:1} & & \downarrow{\scriptstyle 1:1} \\
\mathcal{E}_K/{\approx} & \xrightarrow{1:1} & G(\mathbb{Q})\backslash\left(X \times G(\mathbb{A}_f)/K\right)
\end{array}$$

EXAMPLE 2.21. Choose a lattice Λ in V, and let $K(N)$ be the subgroup of $G(\mathbb{A}_f)$ stabilizing $\Lambda \otimes \hat{\mathbb{Z}}$ (inside $V \otimes \mathbb{A}_f$) and acting as the identity on $(\Lambda \otimes \hat{\mathbb{Z}})/N(\Lambda \otimes \hat{\mathbb{Z}})$ ($\cong \Lambda/N\Lambda$). Let E be an elliptic curve. Every isomorphism

$$\nu\colon \Lambda/N\Lambda \to E[N]$$

lifts to an isomorphism

$$\tilde{\nu}\colon \Lambda \otimes \hat{\mathbb{Z}} \to T_f E,$$

whose orbit $\tilde{\nu} \cdot K(N)$ is independent of the choice of $\tilde{\nu}$. Let

$$\eta = \tilde{\nu} \otimes \mathbb{Q}\colon V \otimes \mathbb{A}_f \to V_f E.$$

Then $(E, \nu) \mapsto (E, [\eta])$ gives a bijection

$$\{(E, \nu)\}/{\approx} \to \mathcal{E}_{K(N)}/{\approx}.$$

When $V=\mathbb{R}^2$ and $\Lambda=\mathbb{Z}^2$, $K(N)$ is the group in (1.14), and an isomorphism $\nu\colon(\mathbb{Z}/N\mathbb{Z})^2\to E[N]$ is a level-N structure on E. The map β

$$\{(E,\nu)\}/{\approx}\to\mathbb{Q}^\times\backslash\{\pm\}\times\mathbb{A}_f^\times/K(N)\cong(\mathbb{Z}/N\mathbb{Z})^\times$$

sends (E,ν) the composite

$$\mathbb{Z}/N\mathbb{Z}\cong{\textstyle\bigwedge}^2(\mathbb{Z}/N\mathbb{Z})^2\xrightarrow{\bigwedge^2\nu}{\textstyle\bigwedge}^2E[N]\cong\mu_N(\mathbb{C})\cong\mathbb{Z}/N\mathbb{Z}$$

the second isomorphism being defined by the e_N-pairing and the last by $e^{2\pi in/N}\mapsto n \bmod N$. This last map is a discrete invariant of (E,ν) — in fact, the only discrete invariant, for the pairs with the same invariant lie in the connected family.

ASIDE 2.22. Every isomorphism class of triples (V,J,Λ) in $\mathcal{T}$ is represented by a triple in which $(V,J)=\mathbb{C}$, and $\Lambda=\mathbb{Z}\oplus\mathbb{Z}z$, $z\in X^+$.

Elliptic modular curves as moduli varieties over $\mathbb{C}$

In the previous subsection, we showed that there is a one-to-one correspondence between the $\mathbb{C}$-valued points of S_K and the isomorphism classes of elliptic curves over $\mathbb{C}$ with a level K-structure. This by itself doesn't determine S_K: in fact, for any curve C over $\mathbb{C}$, $C(\mathbb{C})$ has the same cardinality as $\mathbb{C}$. In this subsection, we prove an additional property of the correspondence that does determine S_K uniquely (up to a unique isomorphism).

Definition of a moduli variety

A *moduli problem* $(\mathcal{M},\sim)$ *over* $\mathbb{C}$ consists of a contravariant functor $\mathcal{M}$ from the category of algebraic varieties over $\mathbb{C}$ to the category of sets, and equivalence relations $\sim$ on each of the sets $\mathcal{M}(T)$ that are compatible with morphisms in the sense that

$$m\sim m'\implies\varphi^*(m)\sim\varphi^*(m'),\quad m,m'\in\mathcal{M}(S),\quad\varphi\colon T\to S.$$

A point t of a variety T with coordinates in $\mathbb{C}$ can be regarded as a map $\operatorname{Specm}\mathbb{C}\to T$, and so defines a map

$$m\mapsto m_t\overset{\text{df}}{=}t^*m\colon\mathcal{M}(T)\to\mathcal{M}(\mathbb{C}).$$

A *solution to the moduli problem* is a variety V over $\mathbb{C}$ together with a bijection $\alpha\colon\mathcal{M}(\mathbb{C})/{\sim}\to V(\mathbb{C})$ with the properties:

(a) For any variety T over $\mathbb{C}$ and $m\in\mathcal{M}(T)$, the map $t\mapsto\alpha(m_t)\colon T(\mathbb{C})\to V(\mathbb{C})$ is regular (i.e., defined by a morphism of algebraic varieties);

(b) *(Universality)* Let Z be a variety over $\mathbb{C}$ and let $\beta\colon\mathcal{M}(\mathbb{C})\to Z(\mathbb{C})$ be a map such that, for any pair (T,m) as in (a), the map $t\mapsto\beta(f_t)\colon T(\mathbb{C})\to Z(\mathbb{C})$ is regular; then the map $\beta\circ\alpha^{-1}\colon V(\mathbb{C})\to Z(\mathbb{C})$ is regular.

A variety V that occurs as the solution of a moduli problem is called a *(coarse) moduli variety*.

PROPOSITION 2.23. *Up to a unique isomorphism, there exists at most one solution to a moduli problem.*

PROOF. Suppose there are two solutions (V,α) and (V',α'). Then because of the universality of (V,α), $\alpha'\circ\alpha^{-1}\colon V(\mathbb{C})\to V'(\mathbb{C})$ is a regular map, and because of the universality of (V',α'), its inverse is also a regular map. □

Of course, in general there may exist no solution to a moduli problem, and when there does exist a solution, it may be very difficult to prove it.

The moduli variety (V,α) is *fine* if there exists a universal $m_0\in\mathcal{M}(V)$, i.e., an object such that, for all varieties T over $\mathbb{C}$ and $m\in\mathcal{M}(T)$, there exists a unique regular map $\varphi\colon T\to V$ such that $\varphi^*m_0\approx m$. Then V represents the functor $T\mapsto\mathcal{M}(T)/\sim$.

REMARK 2.24. The above definitions can be stated also for the category of complex manifolds: simply replace "algebraic variety" by "complex manifold" and "regular map" by "holomorphic (or complex analytic) map". Proposition 2.23 clearly also holds in the context of complex manifolds.

The curve S_1 as a coarse moduli variety over $\mathbb{C}$

Recall (e.g., EC §5) that an elliptic curve over a field k is a pair (E,O) consisting of a complete nonsingular curve E of genus 1 over k and a point $O\in E(k)$. A morphism $(E,O)\to(E',O')$ is a regular map $E\to E'$ carrying O to O'.[20] The plane projective curve

$$E: Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \tag{7}$$

with the distinguished point $O=(0:1:0)$ is an elliptic curve provided it is nonsingular (equivalently, the discriminant $\Delta(a_1,a_2,a_3,a_4,a_6)\neq 0$), and every elliptic curve over k is isomorphic to one of this form.

Let T be a variety over a field k'. We define an *elliptic curve* (better, *family of elliptic curves*) over T to be a pair consisting of a smooth morphism of algebraic varieties $\varphi\colon E\to T$ whose fibres are complete nonsingular curves of genus 1 and a (zero) section $o\colon T\to E$ to φ. A morphism $(E,\varphi,o)\to(E',\varphi',o')$ is a regular map $E\to E'$ carrying φ and o to φ' and o'. As for an elliptic curve over a field, one can show that, locally for the Zariski topology on T, there exist regular functions a_i such that $\Delta(a_1,a_2,a_3,a_4,a_6)$ is never zero and E is isomorphic to the subvariety of $T\times\mathbb{P}^2$ defined by the equation (7).

For a variety T, let $\mathcal{E}(T)$ be the set of elliptic curves over T. On taking $\sim$ to be $\approx$, we get a moduli problem. The j-invariant defines a map

$$E\mapsto j(E):\mathcal{E}(\mathbb{C})\to\mathbb{A}^1(\mathbb{C})=\mathbb{C},$$

and the theory of elliptic curves shows that this map is a bijection.

THEOREM 2.25. *The pair $(\mathbb{A}^1,j)$ is a solution to the moduli problem $(\mathcal{E},\approx)$.*

[20] There is a unique group law on E having the distinguished element as zero, and a morphism of elliptic curves is automatically a homomorphism of groups.

PROOF. Let $E \to T$ be a family of elliptic curves over T, where T is a variety over $\mathbb{C}$. The map $t \mapsto j(E_t) \colon T(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$ is regular because, locally on T, $j(E_t) = c_4^3/\Delta$ where c_4 is a polynomial in the a_i's and Δ is a nowhere-zero polynomial in the a_i's.

Now let (Z, β) be a pair as in (b). We have to show that $j \mapsto \beta(E_j) \colon \mathbb{A}^1(\mathbb{C}) \to Z(\mathbb{C})$, where E_j is an elliptic curve over $\mathbb{C}$ with j-invariant j, is regular. Let U be the open subset of $\mathbb{A}^1$ obtained by removing the points 0 and 1728. Then

$$E : Y^2Z + XYZ = X^3 - \frac{36}{u-1728}XZ^2 - \frac{1}{u-1728}Z^3, \quad u \in U,$$

is an elliptic curve over U with the property that $j(E_u) = u$. Because of the property possessed by (Z, β), E/U defines a regular map $u \mapsto \beta(E_u) \colon U \to Z$. But this is just the restriction of the map $j \mapsto \beta(E_j)$ to $U(k)$, which is therefore regular, and it follows that the map is regular on the whole of $\mathbb{A}^1$. □

The Riemann surface $\Gamma(N)\backslash X$ as a moduli space

Fix a 2-dimensional $\mathbb{R}$-vector space V, a lattice $\Lambda \subset V$, and an integer N. We let X denote the set of nonreal lines in $V(\mathbb{C})$ (see 2.13), and we let $\Gamma(N)$ be the subgroup of $\mathrm{GL}(\Lambda \otimes \mathbb{Q})$ of elements that preserve Λ and act trivially on $\Lambda/N\Lambda$. If N is sufficiently large, $\Gamma(N)$ is torsion free.

Let T be a complex manifold. By a *local system of $\mathbb{Z}$-modules of rank* 2, we mean a sheaf H on T that is locally isomorphic to the constant sheaf defined by $\mathbb{Z}^2$ (or Λ). Then $\mathcal{O}_T \otimes H$ is a locally free sheaf of rank 2 on T, and we let H^- denote a locally free subsheaf of rank 1 such that, for all $t \in T$, H_t^- is a nonreal line in H_t. Let $\mathcal{H}_N(T)$ denote the set of triples (H, H^-, η) where η is an isomorphism from the constant sheaf on T defined by $\Lambda/N\Lambda$ to H/NH. With $\sim$ equal to the obvious notion of isomorphism, $\mathcal{H}_N$ becomes a moduli problem on the category of complex manifolds.

Let $(H, H^-, \eta) \in \mathcal{H}_N(\mathbb{C})$. Choose an isomorphism $\gamma \colon H \to \Lambda$. Then $\gamma_{\mathbb{C}}(H^-)$ is non-real line in $V(\mathbb{C})$ and $(H, H^-, \eta) \mapsto \gamma_{\mathbb{C}}(H^-)$ defines a bijection $\alpha \colon \mathcal{H}_N(\mathbb{C}) \to \Gamma(N)\backslash X$.

PROPOSITION 2.26. *If $\Gamma(N)$ is torsion free, the pair $(\Gamma(N)\backslash X, \alpha)$ is a fine moduli space for $\mathcal{H}_N$.*

PROOF. Let $m = (H, H^-, \eta) \in \mathcal{H}_N(T)$. We have to show that the map

$$\varphi_m \colon T \to \Gamma(N)\backslash X, \quad t \mapsto \alpha(m_t),$$

is holomorphic. Let $t_0 \in T$. Choose an open neighbourhood U of t_0 over which H is trivial, and fix an isomorphism $H|U \approx \Lambda_U$ (constant local system on U). This isomorphism identifies each H_t^- with a nonreal line through the origin in $V(\mathbb{C})$. Since the H_t^- vary holomorphically, $t \mapsto H_t^- : U \to X$ is holomorphic, and so the map $U \to X \to \Gamma(N)\backslash X$ is holomorphic. [To be continued.] □

The Shimura curve S_K as a moduli variety

[Summary.] Define a moduli problem $(\mathcal{M}, \sim)$ such that $(\mathcal{M}(\mathbb{C}), \sim) = (\mathcal{E}_K, \approx)$.

THEOREM 2.27. *The bijection $\mathcal{E}_K/\approx \to S_K(\mathbb{C})$ in (2.21) is a solution to the moduli problem.*

PROOF. It follows from Proposition 2.26 that it is a solution in the category of complex manifolds, but then (2.11) implies it is a solution in the category of nonsingular algebraic varieties. □

3 Canonical models of elliptic modular curves

[To be rewritten.]

Statement of the main theorem

Let ζ_m be the primitive m^{th}-root of one $e^{2\pi i/m}$. Recall that there is a canonical isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}),\ [n]\zeta_m = \zeta_m^n.$$

On passing to the inverse limit, we get an isomorphism

$$\hat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) \tag{8}$$

(Kronecker-Weber theorem).

Let E be an elliptic curve over $\mathbb{C}$, and let σ be an automorphism of $\mathbb{C}$. Define σE by the fibre product diagram

$$\begin{tikzcd} E \arrow[d] & \sigma E \arrow[l] \arrow[d] \\ \operatorname{Specm} k & \operatorname{Specm} k \arrow[l] \end{tikzcd}$$

in which the bottom arrow is induced by σ. If

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3,$$

then[21]

$$\sigma E : Y^2Z = X^3 + (\sigma a)XZ^2 + (\sigma b)Z^3.$$

A point $P = (x : y : z)$ on E defines a point $\sigma P = (\sigma x : \sigma y : \sigma z)$ on σE. This carries $0 = (0 : 1 : 0)$ on E to 0 on σE, and so is a homomorphism $\sigma\colon E(\mathbb{C}) \to (\sigma E)(\mathbb{C})$. Therefore, σ defines an isomorphism $E[N] \to \sigma E[N]$ for each N. On passing to the limit and tensoring with $\mathbb{Q}$, we obtain an isomorphism $\sigma\colon V_f(E) \to V_f(\sigma E)$. For a level

[21] Obviously,

$$\begin{tikzcd} \mathbb{C}[X,Y,Z]/(Y^2 - X^3 - aX - b) \arrow[r] & \mathbb{C}[X,Y,Z]/(Y^2 - X^3 - \sigma aX - \sigma b) \\ \mathbb{C} \arrow[u] \arrow[r, "\sigma"] & \mathbb{C} \arrow[u] \end{tikzcd}$$

is a tensor product diagram.

structure $\eta\colon V(\mathbb{A}_f) \to V_f E$, we define ${}^\sigma\eta\colon V \otimes \mathbb{A}_f \to V_f(\sigma E)$ to be $\sigma \circ \eta$. Therefore, we get an action of $\mathcal{A} =_{\text{df}} \operatorname{Aut}(\mathbb{C})$ on $\mathcal{E}$,

$$\sigma(E, \eta) = (\sigma E, {}^\sigma \eta),$$

which commutes with the action of $G(\mathbb{A}_f)$ and preserves isomorphism classes.

On the other hand, a model of S_K over $\mathbb{Q}$ determines an action of $\mathcal{A}$ on $S_K(\mathbb{C})$.

THEOREM 3.1. *For each compact open subgroup K of $G(\mathbb{A}_f)$, there exists a model C_K of S_K over $\mathbb{Q}$ for which*

$$(\mathcal{E}/\approx)/K \xleftrightarrow{1:1} G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$$

is compatible with the action of $\mathcal{A}$ on $\mathcal{E}$ and the action of $\mathcal{A}$ on $G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$ defined by its identification with $C_K(\mathbb{C})$.

We discuss the proof in the remainder of this section.

REMARK 3.2. According to Proposition 1.8, the model is uniquely determined by the condition. We shall see later that it is the canonical model of S_K.

REMARK 3.3. For compact open subgroups $K' \subset K$, the map $S_{K'}(\mathbb{C}) \to S_K(\mathbb{C})$ is compatible with the action of $\mathcal{A}$.

The Galois action on the set of connected components

Consider

$$\begin{array}{ccccc} \mathcal{E}/\approx & \longrightarrow & G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K & & \mathcal{A} \\ & & \downarrow & & \downarrow \\ & & \mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times/\det(K) & & \operatorname{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}). \end{array}$$

EXERCISE 3.4. Let $\mathcal{A}$ act on π through its quotient $\operatorname{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$ in the obvious way. Show that the map $\det$ in (3) is compatible with the actions of $\mathcal{A}$.

REMARK 3.5. The exercise answers one question raised in the introduction, namely, given a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, what is the field F_Γ that $\Gamma\backslash X^+$ is defined over? Choose a compact open subgroup K of $\mathrm{GL}_2(\mathbb{A}_f)$ such that $K \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma$, let U be the subgroup of $\hat{\mathbb{Z}}^\times$ fixing $[+, 1]$ in $\mathbb{Q}^\times\backslash\{\pm\} \times \mathbb{A}_f^\times/\det(K)$, and then F_Γ is the fixed field of U acting on $\mathbb{Q}^{\text{ab}}$.

(a) Let $\Gamma = \Gamma(N) = \mathrm{SL}_2(\mathbb{Z}) \cap K(N)$. Then $\det(K(N)) = \ldots$

(b) Let $\Gamma = \Gamma_0(N)$. Then $\det(K) = \hat{\mathbb{Z}}^\times$, and so $F_\Gamma = \mathbb{Q}$.

How, exactly, does $\mathcal{A}$ act on $S_K(\mathbb{C})$? Let $K = K(1)$ =Revert to the traditional approach.

$$\begin{array}{rcl} \Gamma(1)\backslash X^+ & \xleftrightarrow{1:1} & \{\text{elliptic curves}\}/\approx \\ z & \longleftrightarrow & E(z) \stackrel{\text{df}}{=} \mathbb{C}/(\mathbb{Z} + \mathbb{Z}z). \end{array}$$

Here, $E(z)$ is an elliptic curve over $\mathbb{C}$ with j-invariant $j(E(z)) = j(z)$, where the second j is the holomorphic function

$$j(z) = \frac{1}{q} + 744 + 196884q + \cdots, \quad q = e^{2\pi i z}.$$

The j-invariant of $\sigma E(z)$, is

$$j(\sigma E(z)) = \sigma(j(E(z)).$$

Thus, $\sigma E(z) = E({}^{\sigma}z)$ where ${}^{\sigma}z$ is any element of X^+ such that

$$\sigma(j(z)) = j({}^{\sigma}z).$$

Such a ${}^{\sigma}z$ exists, because j defines an isomorphism of $\Gamma(1)\backslash X^+ \to \mathbb{C}$, but, in general, there is nothing we can say about it that we haven't already said. Note that, unless $\sigma = 1$ or ι, it isn't continuous, so we can't expect anything like $\sigma(j(z)) = j(\sigma z)$ to hold.

Complex multiplication

Amazingly, when $z \in X^+$ is quadratic over $\mathbb{Q}$, we *can* describe how $\mathcal{A}$ acts on $j(z)$. Assume $[\mathbb{Q}[z] : \mathbb{Q}] = 2$ and (for simplicity) that that z generates the ring of integers in $\mathbb{Q}[z]$: then $j(z)$ generates the Hilbert class field of $\mathbb{Q}[z]$, and there is an explicit formula describing how $\mathrm{Gal}(\mathbb{Q}[z]^{\mathrm{ab}}/\mathbb{Q}[z])$ acts on $j(z)$ (see Serre 1967 or MF §12).

We can say more. For a number field F, define

$$\mathbb{A}_{f,F}^{\times} = \{(a_v) \in \prod F_v \mid a_v \in \mathcal{O}_v \text{ for almost all } v\}$$

where v runs through the finite (i.e., nonarchimedean) primes of F and, for such a prime, F_v is the completion of F and $\mathcal{O}_v$ is the ring of integers in F_v.

Let F be a quadratic imaginary field with a given embedding $\rho\colon F \hookrightarrow \mathbb{C}$, and let V be a one-dimensional F-vector space. We consider triples (E, i, η) with

- E an elliptic curve over $\mathbb{C}$,
- i an isomorphism $F \to \mathrm{End}^0(E)$ such that the homomorphism $F \to \mathbb{C}$ given by i and the action of $\mathrm{End}(E)$ on $\mathrm{Tgt}_0(E)$ is ρ, and
- η an $\mathbb{A}_{f,F}^{\times}$-isomorphism $V(\mathbb{A}_f) \to V_f(E)$.

An isomorphism $(E, i, \eta) \to (E', i', \eta')$ is an isomorphism $E \to E'$ in $\mathrm{Ell}^0(\mathbb{C})$ compatible with i and η. Given such a triple (E, i, η), choose an F-linear isomorphism $\alpha\colon H_1(E, \mathbb{Q}) \to V$, and let $a \in \mathbb{A}_{f,F}^{\times}$ be the composite

$$V \otimes_F \mathbb{A}_{f,F} \xrightarrow{\eta} V_f(E) \xrightarrow{\alpha\otimes 1} V \otimes_F \mathbb{A}_{f,F}.$$

The class of a in $F^{\times}\backslash\mathbb{A}_{f,F}^{\times}$ is independent of the choice α and depends only on the isomorphism class of (E, i, η).

LEMMA 3.6. *The map* $(E, i, \eta) \mapsto a$ *gives a bijection from the set of isomorphism classes of triples to* $F^{\times}\backslash\mathbb{A}_{f,F}^{\times}$.

PROOF. Consider the pairs (W, η) with W a one-dimensional F-vector space and η an isomorphism $V(\mathbb{A}_f) \to W(\mathbb{A}_f)$. On the one hand, the isomorphism classes of these pairs are obviously classified by $F^{\times}\backslash\mathbb{A}_{f,F}^{\times}$. On the other hand, the isomorphism $W \otimes_{\mathbb{Q}} \mathbb{R} \cong W \otimes_{F,\rho} \mathbb{C}$ provides $W \otimes_{\mathbb{Q}} \mathbb{R}$ with a complex structure J, and it follows from (2.17) that there is an equivalence of categories $(W, \eta) \mapsto (E, i, \eta)$. $\square$

For any number field F, class field theory provides a continuous surjective homomorphism

$$\mathrm{rec}_F \colon \prod_{v|\infty} F_v^{\times} \times \mathbb{A}_f^{\times} \to \mathrm{Gal}(F^{\mathrm{ab}}/F).$$

Since $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ is totally disconnected, this homomorphism factors through $\mathbb{A}_f^{\times}$ when F is totally imaginary. In fact, when $F = \mathbb{Q}$ or a quadratic imaginary field, it gives an isomorphism[22]

$$\mathrm{rec}_F \colon F^{\times}\backslash\mathbb{A}_{f,F}^{\times} \to \mathrm{Gal}(F^{\mathrm{ab}}/F).$$

Write $t(E, i, \eta)$ for the element of $F^{\times}\backslash\mathbb{A}_{f,F}^{\times}$ defined by a triple (E, i, η).

THEOREM 3.7. *For* $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$, *the isomorphism class of* $\sigma(E, i, \eta)$ *depends only on the restriction of* σ *to* F^{ab}, *and if* $\sigma|F^{ab} = \mathrm{rec}_F(b)$, *then*

$$t(\sigma(E, i, \eta)) = t(E, i, \eta)b$$

(or perhaps $t(E, i, \eta)b^{-1}$ *depending on the sign conventions).*

This is one statement of the Main Theorem of Complex Multiplication for elliptic curves.

ASIDE 3.8. The signs in Deligne's Bourbaki talk (Deligne 1971) are correct. Those in his Corvallis talk (Deligne 1979) are wrong[23] — specifically, delete "inverse" from line 10, page 269.

[22] To be consistent with (8), I choose the map to send prime elements to Frobenius elements ($x \mapsto x^q$). This convention is used in (7), my notes CFT, and Deligne 1971, but it is the reciprocal of that used in Deligne 1979 and most of the work on the Langlands program.

In general, the kernel of the reciprocity map is the closure of the image of the identity component of $\prod_{v|\infty} F_v^{\times}$ in $\mathbb{A}_F^{\times}/F^{\times}$, but the image of this identity component is already closed when $F = \mathbb{Q}$ or a quadratic imaginary field (and only then Artin and Tate 1961, Theorem 3, p90).

[23] I once wrote to Deligne to point this out, and noted that there were three changes of sign between his Bourbaki talk and his Corvallis article. He responded: "Mea culpa, mea maxima culpa. My sign is wrong, and your explanation ... plausible: I could not count to three." Thus, it appears that the prerequisite for understanding Shimura varieties is being able to count to two — three would be useful, but not strictly necessary.

Special points

Regard X as the complex double plane. A point $z \in X$ is *special* if $\mathbb{Q}(z)$ has degree 2 over $\mathbb{Q}$.

Regard X as the set of $\mathbb{R}$-homomorphisms $h\colon \mathbb{C} \to \mathrm{End}_{\mathbb{R}}(V \otimes \mathbb{R})$. Let F be a quadratic imaginary field, and choose an action of F on V, i.e., a homomorphism $F \to \mathrm{End}(V)$. On tensoring this with $\mathbb{C}$ we obtain a homomorphism $F \otimes \mathbb{R} \to \mathrm{End}_{\mathbb{R}}(V \otimes \mathbb{R})$. The composite of such an isomorphism with one of the two isomorphisms $\mathbb{C} \to F \otimes \mathbb{R}$ will be said to be *special*.

These definitions agree.

A point $[x, a]$ of $\mathrm{Sh}_K(\mathbb{C})$ is *special* if x is special[24].

DEFINITION 3.9. To be added: define the action of $\mathcal{A}$ on the special points.

THEOREM 3.10. *There exists a unique family of models* (C_K) *of* (Sh_K) *over* $\mathbb{Q}$ *such that the action of* $\mathcal{A}$ *on the special points is described by (3.9).*

PROOF. That the family of models in Theorem 3.1 has this property follows from the main theorem of complex multiplication for elliptic curves (9.2).

The uniqueness follows from the fact that the special points are Zariski dense. □

REMARK 3.11. The proof of the uniqueness is complicated by the fact that, for each special point $[x, a]$, we only know how the automorphisms fixing $\mathbb{Q}(x)$ act. However, in this case, the full group of automorphisms is generated by those fixing $\mathbb{Q}(x)$ and by ι, and it is possible to say also how ι acts.

In the general case, an extension of the main theorem of complex multiplication (due to Langlands and Deligne[25]) allows one to say how all automorphisms act on the special points.

Hard descent

Deligne bases his proof of the existence of canonical models on Mumford 1965. One shouldn't do this. Mumford proved the existence of moduli schemes for polarized abelian varieties with level N-structure over $\mathrm{Spec}\, \mathbb{Z}[\frac{1}{N}]$. This is a very difficult theorem, and is much more than one needs. Moreover, there are Shimura varieties to which Mumford's theorem can't be applied. Instead, one should use descent theory.[26]

Recall that "easy descent" gives us a fully faithful functor from varieties over $\mathbb{Q}$ to varieties over $\mathbb{C}$ + an action of $\mathcal{A}$ on their points. "Hard descent" will describe the essential image of the functor, i.e., it gives necessary and sufficient conditions for a pair to arise from a variety over $\mathbb{Q}$.

From now on, all varieties are quasi-projective.

---

[24] In this case, the special points are also CM.

[25] See Deligne's article *Motifs et groupes de Taniyama*, in Hodge Cycles, Motives, and Shimura Varieties, SLN 900, 1982. Also, my notes *Abelian varieties with complex multiplication (for pedestrians)*, available on my website.

[26] Also, so far as I know, Shimura and his students never used Mumford's results.

Consider a pair $(V,*)$ where V is a variety over $\mathbb{C}$ and $*$ is an action of $\mathcal{A}$ on $V(\mathbb{C})$, which I write

$$(\sigma,P)\mapsto\sigma*P\colon\mathcal{A}\times V(\mathbb{C})\to V(\mathbb{C}).$$

I'll say that $(V,*)$ is *effective* if there exists a variety V_0 over $\mathbb{Q}$ and an isomorphism $f\colon V_{0\mathbb{C}}\to V$ carrying the natural action of $\mathcal{A}$ on $V_0(\mathbb{C})$ into $*$. Such a pair (V_0,f) will be called a *model* of $(V,*)$ over $\mathbb{Q}$. Recall that easy descent shows that, when it exists, the model is unique up to a unique isomorphism.

Consider the following two conditions on a pair $(V,*)$.

Regularity condition: The map

$$\sigma P\mapsto\sigma*P\colon(\sigma V)(\mathbb{C})\to V(\mathbb{C})$$

is regular. (A priori, this is only a map of sets. The condition requires that it be induced by a regular map (morphism) $f_\sigma\colon\sigma V\to V$.)

Continuity condition: There exists a subfield L of $\mathbb{C}$ finitely generated over $\mathbb{Q}$ and a model (V_0,f) of $(V,*)$ over L, i.e., V_0 is a variety over L and $f\colon V_{0\mathbb{C}}\to V$ is an isomorphism carrying the natural action of $\mathrm{Aut}(\mathbb{C}/L)$ on $V_0(\mathbb{C})$ into $*$.

THEOREM 3.12. *A pair $(V,*)$ is effective if and only if it satisfies the regularity and continuity conditions.*

PROOF. $\Longrightarrow$: If $(V,*)$ has a model (V_0,ϕ) over $\mathbb{Q}$, then

$$f_\sigma=f\circ(\sigma f)^{-1},$$

and so $(V,*)$ satisfies the regularity condition. It obviously satisfies the continuity condition.

$\Longleftarrow$: At the moment, alas, one has to appeal to Weil 1956.[27] □

The next result replaces the continuity condition with another condition that is often easier to check.

COROLLARY 3.13. *A pair $(V,*)$ is effective if it satisfies the regularity condition and there exists a finite subset Σ of $V(\mathbb{C})$ such that*

(a) *any automorphism of V fixing the $P\in\Sigma$ is the identity;*

(b) *for some field L finitely generated over $\mathbb{Q}$, $\sigma*P=P$ for all $P\in\Sigma$ and all $\sigma\in\mathrm{Aut}(\mathbb{C}/L)$.*

PROOF. See Milne 1999. □

[27] Varshavsky has transcribed part of Weil's paper into the language of schemes (Appendix to his paper ArXive NT 9909142). Sometime, I'll explain how to derive the theorem from Grothendieck's faithfully flat descent (which is quite elementary).

EXERCISE 3.14. Assume the existence of a good theory of Jacobians over $\mathbb{C}$, and use (3.13) to deduce the existence of a good theory over any subfield of $\mathbb{C}$. (Hint: use that any automorphism of a polarized abelian variety fixing the points of order 3 is the identity).[28]

ASIDE 3.15. It is easy to construct examples of actions of automorphism groups that fail the regularity condition, the continuity condition, or both. However, in practice, any naturally arising action (for example, one arising from a moduli problem) will satisfy the conditions, although this has to be proved in each case.

Existence of canonical models

Of course, it is easy to prove the existence of canonical models of elliptic modular curves by ad hoc methods. Thus, what follows should be considered as an introduction to the general case.

Note that it suffices to prove the existence of the canonical model of S_K for K sufficiently small: if K' contains K as a normal subgroup, then $S_{K'}$ is the quotient of S_K by the action of the finite group K'/K. Thus, we can take $K = K(N)$ for N large. (Implicitly therefore, we are choosing a lattice Λ in V.)

The regularity condition

This is immediate from Theorem 2.27.

The continuity condition

Apply Corollary 3.13 with Σ equal to a set of special points — see Milne 1999.

Definition of "canonical"

There are three different ways of characterizing the family of models we have constructed.

(A) The moduli criterion

The model C_K of Sh_K satisfies the condition in Theorem 3.1.

(B) The analytic criterion

Since we know π_K, to characterize the C_K it suffices to characterize their geometrically connected components, i.e., the models C_Γ over F_Γ of the curves $\Gamma\backslash X^+$.

A holomorphic function f on X^+ is a modular form of weight $2k$ if and only if $f(dz)^k$ is invariant under the action of Γ, and hence defines a k-differential ω on $\Gamma\backslash X^+$. The curve C_Γ/F_Γ has the following property, which determines it: a k-differential $\omega = f(dz)^k$ arises from a k-differential on C_Γ if and only the Fourier coefficients of f lie F_Γ.

[28] Niranjan Ramachandran has pointed out that Corollary 3.13 can be used to show that certain abelian varieties attached by Murre to varieties (maximal algebraic quotients of intermediate Jacobians) are defined over the same subfield of $\mathbb{C}$ as the variety.

(C) Special points

The model C_K of Sh_K satisfies the condition in Theorem 3.10.

Which definition is best?

According to Deligne's approach, in defining a Shimura variety one begins with an abstract reductive group G and additional data X. In order to realize the Shimura variety over $\mathbb{C}$ as a moduli variety (when this is possible) it is necessary to choose a faithful representation of G. Thus, Definition A is not really intrinsic (you have to make a choice, and then show that it is independent of the choice). More significantly, many Shimura varieties are not moduli varieties, not even conjecturally, and so Definition A doesn't apply to such Shimura varieties.

Definition B has a similar problem: if the Shimura variety is compact (see below), there are no cusps, and hence no Fourier expansions. Hence Definition B doesn't apply to such Shimura varieties. Moreover, when the boundary components are not points (they will in general be lower dimensional Shimura varieties), the Fourier series become Fourier-Jacobi series whose coefficients are functions, not complex numbers, and so this criterion becomes complicated to state.

The correct, general definition, is C. Moreover, when either A or B apply, they will coincide with C. For A, this is essentially the Shimura-Taniyama Theorem (Deligne 1971, 4.19). For B, it is the theory of canonical models of automorphic vector bundles (see §4 below, or Milne 1990, Chapter III, for the general case).

ASIDE 3.16. Historically, Definition B seemed the natural definition. In his acceptance of the Steele prize (Shimura 1996) Shimura recounts that Siegel initially reacted with disbelief to his statement that he could prove the existence of canonical models for certain compact modular curves, presumably because of the lack of Fourier expansions. On the other hand, to algebraic geometers, Definition A is the most natural. Deligne once told me that initially he was very surprised that Shimura could prove the existence of canonical models for nonmodular curves.

4 Automorphic vector bundles

[To be added.]

5 Quaternionic Shimura curves

[To be completed.]

The elliptic modular curves are the simplest Shimura varieties, and for that reason provide a good introduction to the general theory. However, in some respects they are *too* simple, and so may lead to false expectations about the general case. In this section, we examine the other Shimura curves.

Quaternion algebras

(CFT Chapter IV, especially 5.1)

Let F be a field of characteristic zero. The matrix algebra $M_2(F)$ has the following properties:

(a) it is central, i.e., F is the centre of B;

(b) it is simple, i.e., it has no two-sided ideals;

(c) it has dimension 4 as an F-vector space.

Any F-algebra with these three properties is called a *quaternion algebra*.

For $a, b \in F^{\times}$, let $B = B_{a,b}$ be the F-algebra with basis $\{1, i, j, k\}$ and multiplication given by

$$i^2 = a,\, j^2 = b,\, ij = k = -ji.$$

Then B is a quaternion algebra, and every quaternion algebra is of this form for some a, b.

Let B be a quaternion algebra over F. According to a theorem of Wedderburn, either B is a division algebra or it is isomorphic to $M_2(F)$ (in which case B is said to be split). For $B = B_{a,b}$, the second case occurs exactly when the quadratic form $W^2 - aX^2 - bY^2 + abZ^2$ has a nontrivial zero in F.

For F algebraically closed, every quaternion algebra is split.

For $F = \mathbb{R}$, every quaternion algebra is isomorphic to $M_2(\mathbb{R})$ or the usual (Hamiltonian) quaternion algebra $B_{-1,-1}$.

For $F = \mathbb{Q}_p$ or a finite extension of $\mathbb{Q}_p$, there are again exactly two isomorphism classes of quaternion algebras.

Finally, let F be a number field. For a quaternion algebra B over F, let $d(B)$ be the set of primes v of F such that $F_v \otimes B$ is a division algebra. Then

- $d(B)$ is a finite set with an even number of elements;
- $B \approx B'$ if and only if $d(B) = d(B')$;
- every set containing a finite even number of primes of F is of the form $d(B)$ for some quaternion algebra over F.

For $F = \mathbb{Q}$, this statement has a fairly elementary proof, but for an arbitrary number field, the proof requires class field theory.

Quaternionic modular curves

Let B be a quaternion division algebra over $\mathbb{Q}$ split at infinity. Thus, B is a $\mathbb{Q}$-algebra such that

$$B \not\approx M_2(\mathbb{Q})$$

but

$$B \otimes \mathbb{R} \approx M_2(\mathbb{R}).$$

Let G be the algebraic group over $\mathbb{Q}$ such that $G(R) = (B \otimes_{\mathbb{Q}} R)^\times$ for all $\mathbb{Q}$-algebras R. Then, $G(\mathbb{R}) \approx \mathrm{GL}_{2,\mathbb{R}}$ and the choice of such an isomorphism determines an action of $G(\mathbb{R})$ on X. For any compact open subgroup K in $G(\mathbb{A}_f)$, we define

$$S_K = G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K,$$

as before. This is a finite union of *compact* Riemann surfaces. More precisely, let G^1 be the subgroup of G such that

$$G^1(\mathbb{Q}) = \mathrm{Ker}(B^\times \xrightarrow{\mathrm{Norm}} \mathbb{Q}^\times).$$

Then $\Gamma =_{\mathrm{df}} K \cap G^1(\mathbb{Q})$ is a discrete subgroup $G^1(\mathbb{Q})$, $\Gamma\backslash X^+$ is a compact Riemann surface, and S_K is a finite union of copies of $\Gamma\backslash X^+$ (Shimura 1971, Proposition 9.2).

Let B^{opp} be the opposite quaternion algebra. Thus $B^{\mathrm{opp}} = B$ as an abelian group, but multiplication is reversed: $a^{\mathrm{opp}}b^{\mathrm{opp}} = (ba)^{\mathrm{opp}}$. Let V be B regarded as a $\mathbb{Q}$-vector space. Left multiplication makes V into a left B-module, and right multiplication makes it into a right B-module or, what is the same thing, a left B^{opp}-module. These actions identify B and B^{opp} with commuting subalgebras of $\mathrm{End}_{\mathbb{Q}}(V)$. In fact, by counting dimensions, one sees that each is the centralizer of the other.

Let $\mathcal{A}$ be the set of triples (A, i, η) with A an abelian variety of dimension 2 over $\mathbb{C}$, i a homomorphism of $\mathbb{Q}$-algebras $B \to \mathrm{End}(A) \otimes \mathbb{Q}$, and η is a $B \otimes \mathbb{A}_f$-isomorphism $V(\mathbb{A}_f) \to V_f(A)$. An isomorphism $(A, i, \eta) \to (A', i', \eta')$ is an isomorphism $A \to A'$ in the category of abelian varieties up to isogeny commuting with i and η. The group $G(\mathbb{A}_f)$ acts on $\mathcal{A}$ through its action on $V(\mathbb{A}_f)$.

[Define the map $\mathcal{A} \to G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)$.]

PROPOSITION 5.1. *The map just defined gives a bijection*

$$\mathcal{A}/{\approx} \to G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f).$$

It is compatible with the action of K, and therefore induces a bijection

$$(\mathcal{A}/{\approx})/K \to G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K.$$

PROOF. The proof is similar to that of Proposition 2.19. □

THEOREM 5.2. *For each compact open subgroup K of $G(\mathbb{A}_f)$, there exists a model C_K of S_K over $\mathbb{Q}$ for which*

$$(\mathcal{A}/{\approx})/K \overset{1:1}{\longleftrightarrow} G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$$

is compatible with the action of $\mathcal{A}$ on $\mathcal{A}$ and the action of $\mathcal{A}$ on $G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$ defined by its identification with $C_K(\mathbb{C})$.

Etc.

REMARK 5.3. In this case, C_K has no $\mathbb{R}$-points, hence no $\mathbb{Q}$-points (explain).

Quaternionic nonmodular curves

Next let F be a totally real field of degree > 1 and let B be a quaternion algebra over F that is split at exactly one infinite prime of F, i.e., $B \otimes_{F,\rho_1} \mathbb{R} \approx M_2(\mathbb{R})$ for one embedding $\rho_1 \colon F \to \mathbb{R}$, and $B \otimes_{F,\rho} \mathbb{R} \approx \mathbb{H}$ for the remaining embeddings. Let G be the algebraic group over $\mathbb{Q}$ such that $G(R) = (B \otimes_{\mathbb{Q}} R)^\times$ for all $\mathbb{Q}$-algebras R. Then, $G(\mathbb{R}) \approx \mathrm{GL}_{2,\mathbb{R}} \times \mathbb{H}^\times \times \cdots$, and we let X be the conjugacy class of homomorphisms h that project onto the usual class on the first factor, and onto the trivial map on the other factors. For any compact open K in $G(\mathbb{A}_f)$, we define

$$S_K(G, X) = G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f)/K,$$

as before. Again, this is a finite union of complete algebraic curves, but this time it is *not* a moduli variety. Nevertheless, it does have a canonical model (over F rather than $\mathbb{Q}$ now).

The idea of the proof is as follows. Let Q be a quadratic imaginary extension of $\mathbb{Q}$, and let $L = Q \cdot F$ — it is a CM-field with largest real subfield F. Let V and W be one-dimensional vector spaces over B and L. Then $G \times (\mathbb{G}_m)_{L/\mathbb{Q}}$ acts on $V \otimes W$ throught the quotient G':

$$1 \to (\mathbb{G}_m)_{F/\mathbb{Q}} \to G \times (\mathbb{G}_m)_{L/\mathbb{Q}} \to G' \to 0.$$

Then

$$\begin{aligned} \mathbb{R} \otimes_{\mathbb{Q}} V &\cong \oplus_{\rho\colon F \to \mathbb{R}} V_\rho, \\ \mathbb{R} \otimes_{\mathbb{Q}} W &\cong \oplus_{\rho\colon F \to \mathbb{R}} W_\rho, \\ \mathbb{R} \otimes (V \otimes_F W) &\cong \oplus_{\rho\colon F \to \mathbb{R}} V_\rho \otimes W_\rho. \end{aligned}$$

The space $V \otimes_{F,\rho_1} \mathbb{R}$ has dimension 4 and $B \otimes_{F,\rho_1} \mathbb{R} \approx M_2(\mathbb{R})$ acts on it. The set of complex structures on $V \otimes_{F,\rho_1} \mathbb{R}$ commuting with the action of $B \otimes_{F,\rho_1} \mathbb{R}$ can be identified with X. Let J act on W_{ρ_1} as the identity and on W_ρ, $\rho \neq \rho_1$, as an element of square -1 in $L \otimes_{F,\rho} \mathbb{R}$. Then each $J \in X$ defines a complex structure on

$$\mathbb{R} \otimes_{\mathbb{Q}} (V \otimes_F W) \cong V(\mathbb{R}) \otimes_{F \otimes \mathbb{R}} W(\mathbb{R})$$

as follows: let J_W act on W_{ρ_1} as the identity and on W_ρ, $\rho \neq \rho_1$, as an element of square -1 in $L \otimes_{F,\rho} \mathbb{R}$; let J_V act on W_{ρ_1} as J and on W_ρ as the identity; then $J_{V \otimes W} = J_V \otimes J_W$. Let X' ($\cong X$) be the set of such complex structures. Then $S(G', X')$ is a moduli variety, and so has a canonical model over its reflex field L. Moreover, there is a canonical map

$$\varphi\colon S(G, X) \times S(T, \{h\}) \to S(G', X').$$

Endow $S(T, \{h\})$ with the obvious action of $\mathcal{A}$. If $S(T, \{h\})$ had a point P fixed by $\mathcal{A}$, then

$$x, P \mapsto \varphi(x, P)\colon S(G, X) \to S(G', X')$$

would realize $S(G, X)$ as a closed subvariety of $S(G', X')$ stable under $\mathcal{A}$. According to (1.7), it would then have a model $L = F \cdot Q$, which, because of our definitions, satisfies the condition on the special points to be canonical. But Q was any quadratic imaginary field, so this can be shown to imply that $S(G, X')$ has a model over F satisfying the condition.

Unfortunately, it is not that simple: $S(T, \{h\})$ does not have a point P fixed by $\mathcal{A}$. Nevertheless, essentially this argument can be made to work (Deligne 1971, §6).

6 Remarks on the general case

In the general theory, the complex upper half plane ($\cong$ to the open unit disk) is replaced by a bounded symmetric domain, i.e., with an open bounded subset X^+ of a space $\mathbb{C}^m$ that is symmetric in the sense that, for each $x \in X^+$, there exists an automorphism s_x of X^+ of order 2 having x as an isolated fixed point. E. Cartan (and Harish Chandra) classified the bounded symmetric domains in terms of semisimple real groups. Deligne showed that they could be reinterpreted as parameter spaces for certain special Hodge structures. [Mention the Borel embedding and Deligne's interpretation of it as the map sending a Hodge structure to the associated Hodge filtration.]

Deligne's axioms

Let $G = \mathrm{GL}(V)$ for V some two-dimensional $\mathbb{Q}$-vector space. Recall (2.13) that we saw that we could identify $X = \mathbb{C} \smallsetminus \mathbb{R}$ with the set of homomorphisms $\mathbb{C} \to \mathrm{End}_{\mathbb{R}}(V)$. According to the Noether-Skolem theorem (CFT, Theorem 2.10), these homomorphisms form a single conjugacy class. By restriction, we get a conjugacy class of homomorphisms $\mathbb{C}^\times \to G(\mathbb{R})$. These homomorphisms become homomorphisms of real algebraic groups when we realize $\mathbb{C}^\times$ as the points of the algebraic group

$$\mathbb{S} \stackrel{\text{df}}{=} \text{Specm}(\mathbb{R}[X,Y,T]/((X^2+Y^2)T-1).$$

We now take as our initial data, an abstract algebraic group G over $\mathbb{Q}$ for which there exists an isomorphism $G \approx \mathrm{GL}_2$ plus a conjugacy class X of homomorphisms of real algebraic groups $\mathbb{S} \to G_{\mathbb{R}}$. We define the Shimura variety purely in terms of the pair (G, X). Choosing an isomorphism $G \to \mathrm{GL}(V)$ realizes the Shimura variety as a moduli variety.

In Deligne's approach, to define a Shimura variety one needs a pair (a Shimura datum) (G, X) where G is a connected reductive group over $\mathbb{Q}$ and X is conjugacy class[29] of homomorphisms $\mathbb{S} \to G_{\mathbb{R}}$ satisfying certain axioms. From one perspective, the axioms ensure that X acquires a natural structure as a finite disjoint union of bounded symmetric domains. From another perspective, they ensure that attached to any representation $G \to \mathrm{GL}(V)$ of G, there is a variation of Hodge structures on X of a special type.

The axioms also imply that the restriction of an h to $\mathbb{G}_m \subset \mathbb{S}$ is independent of h. Thus, we have a well-defined homomorphism $w_X \colon \mathbb{G}_m \to G_{\mathbb{R}}$, called the *weight homomorphism*.[30] Note that it is a homomorphism, defined over $\mathbb{R}$, of algebraic groups defined over $\mathbb{Q}$. It makes sense to ask whether it is defined over $\mathbb{Q}$. For example, for elliptic modular curves or quaternionic modular curves it is defined over $\mathbb{Q}$, whereas for nonquaternionic modular curves it isn't. Conjecturally, the Shimura variety is a moduli variety (in general for motives) when w_X is defined over $\mathbb{Q}$, and it is not a moduli variety when w_X is not defined over $\mathbb{Q}$.

[29] Of course, X is determined by a single $h \in X$. In his Bourbaki talk, Deligne started with an h rather than X. Thus, the Shimura varieties of his Bourbaki talk have a distinguished point $[h, 1]$. He corrected this in his Corvallis article — Shimura varieties should not come with a distinguished point.

[30] According to the conventions of Deligne 1979, w_X is the inverse of $h|\mathbb{G}_m$.

Rough classification of Shimura varieties

PEL type: These are moduli varieties for polarized abelian varieties with endomorphism and level structure.

Hodge type: These are moduli varieties for polarized abelian varieties with Hodge class and level structure. (Hodge classes in the sense of Deligne 1982).

Hodge type includes PEL type, since endomorphisms of abelian varieties are Hodge classes. In both these cases, w_X is defined over $\mathbb{Q}$.

Abelian type: Initially, these are defined in terms of the classification of semisimple groups over $\mathbb{R}$. For the Shimura variety $\mathrm{Sh}(G, X)$ to be of abelian type, the group G modulo its centre can't have any $\mathbb{Q}$-simple factors that become of type E_6, E_7 or certain mixed types D over $\mathbb{R}$.

Not of abelian type: The rest.

Abelian type includes Hodge type. For Shimura varieties of abelian type, the weight homomorphism may, or may not, be defined over $\mathbb{Q}$. Each of the classes

$$\{\text{PEL type}\} \subset \{\text{Hodge type}\} \subset \{\text{abelian type}\}$$

is *much* larger than its predecessor.

Main results on the existence of canonical models (post Shimura)

Here, ignoring the earlier work of Shimura and his students[31], is a brief summary of work the existence of canonical models.

1971: Deligne gave an axiomatic definition of Shimura varieties and canonical models, and proved that canonical models (if they exist) are unique (Bourbaki talk, Deligne 1971).

1971: Deligne proved the existence of canonical models of Shimura varieties of PEL and Hodge type[32] (with hindsight, since Deligne's theory of Hodge classes didn't exist in 1971). He also proved the existence of canonical models of some associated Shimura varieties whose weight is not defined over $\mathbb{Q}$ by a method that he later called[33] "maladroite" (Bourbaki talk, Deligne 1971).

1979 Deligne proved the existence of canonical models for all Shimura varieties of abelian type (he deduced his general result from the case of Hodge type by a different, more adroit, method than in his Bourbaki talk) (Deligne 1979)

[31] Which, of course, was fundamental to the later work.

[32] Essentially by the method sketched above, except he used Mumford's GIT rather than Weil's descent theory.

[33] Corvallis talk p250.

1983 Borovoi and Milne (Milne 1983) proved the existence canonical models for all Shimura varieties, including those not of abelian type, by a method that is somewhat independent of preceding methods (it assumes only the existence of canonical models of Shimura varieties defined by groups of type A_1).

1994 I proved that all Shimura varieties of abelian type with rational weight are moduli varieties for abelian *motives*. Hence, the canonical models of such Shimura varieties can be shown to exist by the method sketched in the body of this talk. In a clearly retrograde step, I deduced the existence of canonical models for the remaining Shimura varieties of abelian type by Deligne's maladroit method (Milne 1994). The advantage of this approach is that it realizes many more canonical models as moduli varieties — it is much more than just an existence proof.

With the current technology, handling Shimura varieties of abelian type and their canonical models is not much more difficult than handling Shimura varieties of PEL type. However, the situation is very different when one looks at the varieties modulo p. Apart from Vasiu's big theorem (Vasiu 1999), not much is known here except for Shimura varieties of PEL type. Fortunately, the representation theorists have so far been able to find all the Galois representations they need in the cohomology of Shimura varieties of PEL type (see, for example, the proofs of the Langlands local conjecture by Harris and Taylor and by Henniart).

References

Artin, E. and J. Tate (1961). *Class field theory*. Harvard, Dept. of Mathematics.

Borel, A. (1972). Some metric properties of arithmetic quotients of symmetric spaces and an extension theorem. *J. Differential Geometry 6*, 543–560.

Bourbaki, N. (1989). *General topology. Chapters 1–4*. Elements of Mathematics. Berlin: Springer-Verlag.

Casselman, B. (2001). The L-group. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, Volume 30 of *Adv. Stud. Pure Math.*, pp. 217–258. Tokyo: Math. Soc. Japan.

Deligne, P. (1971). Travaux de Shimura. In *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, pp. 123–165. Lecture Notes in Math., Vol. 244. Berlin: Springer.

Deligne, P. (1979). Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pp. 247–289. Providence, R.I.: Amer. Math. Soc.

Deligne, P. (1982). Hodge cycles on abelian varieties. (Notes by J.S. Milne). In *Hodge cycles, motives, and Shimura varieties*, Volume 900 of *Lecture Notes in Mathematics*, pp. 9–100. Berlin: Springer-Verlag.

Fulton, W. (1995). *Algebraic topology*, Volume 153 of *Graduate Texts in Mathematics*. New York: Springer-Verlag.

Hartshorne, R. (1977). *Algebraic geometry*. New York: Springer-Verlag.

Milne, J. S. (1983). The action of an automorphism of $\mathbf{C}$ on a Shimura variety and its special points. In *Arithmetic and geometry, Vol. I*, Volume 35 of *Progr. Math.*, pp. 239–265. Boston, MA: Birkhäuser Boston.

Milne, J. S. (1990). Canonical models of (mixed) Shimura varieties and automorphic vector bundles. In *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988)*, Volume 10 of *Perspect. Math.*, pp. 283–414. Boston, MA: Academic Press.

Milne, J. S. (1994). Shimura varieties and motives. In *Motives (Seattle, WA, 1991)*, Volume 55 of *Proc. Sympos. Pure Math.*, pp. 447–523. Providence, RI: Amer. Math. Soc.

Milne, J. S. (1999). Descent for Shimura varieties. *Michigan Math. J. 46*(1), 203–208.

Mumford, D. (1965). *Geometric invariant theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 34. Berlin: Springer-Verlag.

Mumford, D. (1970). *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay.

Platonov, V. and A. Rapinchuk (1994). *Algebraic groups and number theory*, Volume 139 of *Pure and Applied Mathematics*. Boston, MA: Academic Press Inc.

Serre, J.-P. (1967). Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pp. 292–296. Thompson, Washington, D.C.

Shimura, G. (1971). *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo.

Shimura, G. (1996). 1996 Steele Prizes. *Notices Amer. Math. Soc. 43*(11), 1340–1347.

Vasiu, A. (1999). Integral canonical models of Shimura varieties of preabelian type. *Asian J. Math. 3*(2), 401–518.

Weil, A. (1956). The field of definition of a variety. *Amer. J. Math. 78*, 509–524.

Zariski, O. and P. Samuel (1958). *Commutative algebra, Volume I*. The University Series in Higher Mathematics. D. Van Nostrand Company, Inc., Princeton, New Jersey.