### Automorphism groups of Shimura varieties and reciprocity laws

J.S. Milne and Kuang-yen Shih

(T<sub>E</sub>Xed May 28, 2023)

This paper has two purposes: the first is to extend Shimura's results, as described in his talk (Shimura 1971b) to more general arithmetic quotients of bounded symmetric domains and the second is to interpret some of the results of Milne and Shih 1982b as non-abelian reciprocity laws at the special points of the symmetric domain. The latter can be regarded as nonabelian solutions to Hilbert's twelfth problem.

Before describing our results in more detail, we review the classical case. A modular function (on the upper half-plane) of level N is said to be arithmetic if its Fourier expansion with respect to  $e^{2\pi i z/N}$  has coefficients in  $\mathbb{Q}(e^{2\pi i/N})$ . The arithmetic modular functions form a field F' on which  $\mathrm{GL}_2(\mathbb{A})^+$  acts and there is an exact sequence of topological groups

$$1 \to \mathbb{Q}^{\times} \cdot \mathrm{GL}_{2}(\mathbb{R})^{+} \to \mathrm{GL}_{2}(\mathbb{A})^{+} \xrightarrow{\tau} \mathrm{Aut}(F') \to 1$$

(Shimura 1971a, 6.23). The sequence generalizes the exact sequence

$$1 \to \mathbb{Q}^{\times} \cdot \mathbb{R}^{\times +} \to \mathbb{A}_{\mathbb{Q}}^{\times} \to \operatorname{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to 1$$

of class field theory. We have  $\mathbb{Q}^{ab} \subset F'$  and for  $u \in GL_2(\mathbb{A})^+$ , the restriction of  $\tau(u)$  to  $\mathbb{Q}^{ab}$  is given by  $\det(u)^{-1} \in \mathbb{A}^{\times}_{\mathbb{Q}}$  via the Artin reciprocity map. Moreover, let z be a special point of the upper half-plane, so that  $\mathbb{Q}(z)$  is a quadratic imaginary extension of  $\mathbb{Q}$ . Let  $\mathbb{Q}(z)^{\times} \hookrightarrow GL_2$  be the normalized embedding (ibid., p. 104). The reciprocity law at z asserts the following: if  $f \in F'$  is defined at z, then  $f(z) \in \mathbb{Q}(z)^{ab}$ ; for any  $v \in \mathbb{A}^{\times}_{\mathbb{Q}(z)} \subset GL_2(\mathbb{A})^+$ ,  $\tau^{(v)^{-1}}f(z) = [v]f(z)$ , where [v] is the image of v in  $Gal(\mathbb{Q}(z)^{ab}/\mathbb{Q}(z))$ .

More generally, one starts with a bounded symmetric domain  $X^+$  and a reductive group G such that  $G^{ad}(\mathbb{R})^+$  is the identity component of the group of holomorphic automorphisms of  $X^+$ . The field F' consists of meromorphic functions on  $X^+$  that are automorphic relative to a congruence subgroup of  $G^{der}(\mathbb{Q})$  and are arithmetic. In defining this last notion, it is not always possible to use Fourier expansions. Instead one must first construct a family of varieties defined over number fields (a canonical model) and require an arithmetic automorphic function to be defined on one of the varieties in the family. Then, under certain assumptions, there is an exact sequence,

$$1 \to \widehat{Z(\mathbb{Q})} \cdot G(\mathbb{R})_+ \to \mathcal{G}(G, X) \stackrel{\tau}{\longrightarrow} \operatorname{Aut}(F'/E)$$

Manuscript received June 16, 1980

Both authors were supported by the National Science Foundation.

American Journal of Mathematics, 1981, Vol. 103, No. 5, pp. 911–935 Copyright ©1981 The Johns Hopkins Press.

in which  $\mathcal{G}(G, X)$  is a certain subgroup of  $G(\mathbb{A})$ , Z is the centre of  $G, \overline{Z(\mathbb{Q})}$  is the closure of  $Z(\mathbb{Q})$  in  $Z(\mathbb{A})$ , and E is a certain field associated with G and X (called the reflex field). The image of  $\tau$  in Aut(F'/E) is an open subgroup of finite index. It is frequently possible to enlarge  $\mathcal{G}(G, X)$  to make  $\tau$  surjective. Attached to a special point z of  $X^+$  there is a finite extension field E(z) of E and a map  $\eta: E(z)^{\times} \to G$  of  $\mathbb{Q}$ -rational algebraic groups such that  $\eta(\mathbb{A}): \mathbb{A}_{E(z)}^{\times} \to G(\mathbb{A})$  factors through  $\mathcal{G}(G, X)$ . The reciprocity law at z asserts the following:

if 
$$f \in F'$$
 is defined at z, then  $f(z) \in E(z)^{ab}$ ; if  $v \in \mathbb{A}_{E(z)}^{\times}$  and  $u = \eta(v)^{-1}$ ,  
then  $\tau^{(u)}f(z) = [v]f(z)$ , where  $[v]$  is the image of v in  $\operatorname{Gal}(E(z)^{ab}/E(z))$ .

The above results were proved in Shimura 1970, K. Miyake 1971, Shih 1979 for a group whose derived group is simply connected and Q-simple of type C, A, and B respectively. We prove them whenever G is classical and the canonical model is known to exist. (In this generality it is more natural to replace the exact sequence by an inclusion  $\overline{\mathcal{E}}(G, X) \hookrightarrow$ Aut(F'/E).) The essential step, which is carried out in §1, is to compute the automorphism group of a connected Shimura variety. An argument of T. Miyake allows us in §2 to show that the automorphism group of the variety is equal to the automorphism group of its function field. The above results, concerning Shimura's canonical models, can then be deduced without difficulty from Deligne's results (1979) concerning his canonical models. This is done in §3 and §4.

The non-abelian reciprocity laws proved in §5 take the following form. Recall that the Weil group of E(z) over E is an extension

$$1 \to E(z)^{\times} \setminus \mathbb{A}_{E(z)}^{\times} \to W_{E(z)/E} \xrightarrow{0} \operatorname{Hom}_{E}(E(z), \overline{\mathbb{Q}}) \to 1,$$

and that the map  $E(z)^{\times} \setminus \mathbb{A}_{E(z)}^{\times} \to \operatorname{Gal}(E(z)^{ab}/E(z))$  of class field theory extends to a map  $\nu \mapsto [\nu]: W_{E(z)/E} \to \operatorname{Hom}_{E}(E(z)^{ab}, \overline{\mathbb{Q}})$ . For any special  $z \in X$ , the abelian reciprocity law can be interpreted as stating the following:

let  $v \in E(z)^{\times} \setminus \mathbb{A}_{E(z)}^{\times}$  and let  $\eta(v)$  be its image in  $G(\mathbb{Q}) \setminus G(\mathbb{A})$  under the map defined by  $\eta$ ; then, for any lifting  $u = (u_{\infty}, u_f)$  of  $\eta(v)$  to  $G(\mathbb{A})$ ,

$$\tau(u_f^{-1})f(z) = [\nu]f(\operatorname{ad} u_{\infty} \circ z).$$

This makes sense because  $\tau(a^{-1}) f(z) = f(\operatorname{ad} a \circ z)$  for  $a \in G(\mathbb{Q})$ . The non-abelian reciprocity law states the following:

let *C* be the isotropy subgroup of  $G_{\mathbb{R}}$  at *z*; the map  $E(z)^{\times} \setminus \mathbb{A}_{E(z)}^{\times} \to G(\mathbb{Q}) \setminus G(\mathbb{A}) / C(\mathbb{R})$ defined by  $\eta$  extends to a map  $\xi: W_{E(z)/E} \to G(\mathbb{Q}) \setminus G(\mathbb{A}) / C(\mathbb{R})$ ; for any  $\nu \in W_{E(z)/E}$  and lifting  $u = (u_{\infty}, u_f)$  of  $\xi(\nu)$  to  $G(\mathbb{A})$ ,

$$\tau(u_f^{-1}) f(z) = [\nu] f(\operatorname{ad} u_{\infty} \circ z).$$

We remark that there are now three notions of canonical model: Shimura's model and Deligne's connected and non-connected models. Only Shimura's model provides one with a family of geometrically irreducible varieties defined over number fields, but in proving theorems it seems to be easier to work first with Deligne's models.

3

NOTATION AND CONVENTIONS.

For Shimura varieties and algebraic groups we generally follow the notation of Deligne 1979. Thus a reductive algebraic group G is always connected, with derived group  $G^{der}$ , adjoint group  $G^{ad}$ , and centre Z = Z(G). A central extension is an epimorphism  $G \to G'$  whose kernel is contained in Z(G), and a covering is a central extension such that G is connected and the kernel is finite.

A superscript <sup>+</sup> refers to a topological connected component; for example,  $G(\mathbb{R})^+$  is the identity component of  $G(\mathbb{R})$  relative to the real topology, and  $G(\mathbb{Q})^+ = G(\mathbb{Q}) \cap G(\mathbb{R})^+$ . For *G* reductive,  $G(\mathbb{R})_+$  is the inverse image of  $G^{ad}(\mathbb{R})^+$  in  $G(\mathbb{R})$  and  $G(\mathbb{Q})_+ = G(\mathbb{Q}) \cap$  $G(\mathbb{R})_+$ . In contrast to Deligne 1979, we use the superscript ^ to denote both completions and closures.

We write Sh(G, X) for the Shimura variety defined by a pair (G, X) and  $Sh^{\circ}(G, G', X^+)$  for the connected Shimura variety defined by a triple  $(G, G', X^+)$ . The canonical model of Sh(G, X) is denoted by M(G, X).

Vector spaces are finite-dimensional, number fields are of finite degree over  $\mathbb{Q}$  (and usually contained in  $\mathbb{C}$ ), and  $\overline{\mathbb{Q}}$  is the algebraic closure of  $\mathbb{Q}$  in  $\mathbb{C}$ . If *V* is a vector space over  $\mathbb{Q}$  and *R* is a  $\mathbb{Q}$ -algebra, we often write V(R) for  $V \otimes R$ .

We write  $\widehat{\mathbb{Z}} = \lim_{E \to \infty} \mathbb{Z}/m\mathbb{Z}$ ,  $\mathbb{A}_f = \mathbb{Q} \otimes \widehat{\mathbb{Z}}$  for the ring of finite adèles of  $\mathbb{Q}$ , and  $\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$  for the ring of adèles of  $\mathbb{Q}$ . For E a number field,  $\mathbb{A}_{E,f}$  and  $\mathbb{A}_E$  denote  $E \otimes_{\mathbb{Q}} \mathbb{A}_f$  and  $E \otimes \mathbb{A}$ . The group of idèles of E is  $\mathbb{A}_E^{\times}$  and the idèle class group is  $C_E = \mathbb{A}_E^{\times}/E^{\times}$ .

We use [\*] to denote an equivalence class containing \*; for example, if  $x \in X$  and  $g \in G(\mathbb{A}_f)$ , then [x,g] denotes the element of  $\operatorname{Sh}(G,X) = G(\mathbb{Q}) \setminus X \times G(\mathbb{A}_f) / Z(\mathbb{Q})^{\wedge}$  containing (x,g).

Throughout the paper, all groups actions are from the left.

We normalize the reciprocity isomorphism of class field theory so that a uniformizing parameter corresponds to the reciprocal of the (arithmetic) Frobenius element; we thus agree with Deligne 1979 and Tate 1979, but disagree with Langlands 1979.<sup>1</sup>

# 1 The automorphism group of a connected Shimura variety

Let *G* be a semi-simple  $\mathbb{Q}$ -rational adjoint group, *G'* a covering of *G*, and  $X^+$ a family of maps  $\mathbb{C}^{\times} \to G(\mathbb{R})$ . The topology on  $G(\mathbb{Q})$  defined by *G'* is that for which the images of the congruence subgroups of  $G'(\mathbb{Q})$  form a fundamental system of neighbourhoods. Let  $\Sigma = \Sigma(G')$  be the set of arithmetic subgroups  $\Gamma$  of  $G(\mathbb{Q})^+$  that are open relative to this topology and are torsion-free. Under certain hypotheses (Deligne 1979, 2.1.8),  $(G, G', X^+)$  defines a connected Shimura variety  $\mathrm{Sh}^{\circ}(G, G', X^+)$  equal to the projective limit of  $\Gamma \setminus X^+$ ,  $\Gamma \in \Sigma$ . An automorphism of  $\mathrm{Sh}^{\circ} = \mathrm{Sh}^{\circ}(G, G', X^+)$  is a morphism  $\alpha: \mathrm{Sh}^{\circ} \to \mathrm{Sh}^{\circ}$  such that,

<sup>&</sup>lt;sup>1</sup>27.05.23. This refers to the fact that the signs in Langlands disagree with those in Deligne. However, the signs in Deligne 1979 require correction — see my letter to Deligne 28.03.90 — and so our signs should agree with those in Langlands.

4

for any  $\Gamma \in \Sigma$ , there exist a  $\Gamma' \in \Sigma$  and a commutative diagram

1

$$\begin{array}{ccc} \operatorname{Sh}^{\circ} & \xrightarrow{\alpha} & \operatorname{Sh}^{\circ} \\ & \downarrow_{\operatorname{canonical}} & \downarrow_{\operatorname{canonical}} \\ & \Gamma' \backslash X^{+} & \xrightarrow{\alpha_{\Gamma}} & \Gamma \backslash X^{+} \end{array}$$

with  $\alpha_{\Gamma}$  an isomorphism. (The morphisms are required to be analytic; according to Borel 1972, 3.10, they will then be algebraic.) Denote the group of automorphisms of Sh<sup>°</sup> by Aut<sub>C</sub>(Sh<sup>°</sup>). For a  $\Gamma \in \Sigma$ , the  $\alpha \in Aut_{C}(Sh^{°})$  such that

$$(\mathrm{Sh}^{\circ} \xrightarrow{\alpha} \mathrm{Sh}^{\circ} \xrightarrow{\mathrm{can}} \Gamma \setminus X^{+}) = (\mathrm{Sh}^{\circ} \xrightarrow{\mathrm{can}} \Gamma \setminus X^{+})$$

form a subgroup of  $\operatorname{Aut}_{\mathbb{C}}(\operatorname{Sh}^{\circ})$ . The group  $\operatorname{Aut}_{\mathbb{C}}(\operatorname{Sh}^{\circ})$  is given the topology for which these subgroups form a fundamental system of neighbourhoods of the identity element. In this section, we give an explicit description of this topological group, assuming *G* is classical in the sense of Kneser 1969, 2.3, i.e., it is not exceptional and neither  ${}^{3}D_{4}$  nor  ${}^{6}D_{4}$  occurs as a component of its universal covering group.

1.1. According to Weil 1960 (see also Kneser 1969, Chapter 2), we can identify the classical group with the identity component of the automorphism group of a semi-simple algebra with involution over  $\mathbb{Q}$ . The algebra with involution is a direct product of  $(L, \sigma)$  of the following types:

(A) L is a central simple algebra over a quadratic totally imaginary extension of a totally real field  $F_0$ , and  $\sigma$  is an involution of the second kind.

(B),  $(D^{\mathbb{R}}) L = \operatorname{End}_{F_0}(V)$ , where V is a finite-dimensional vector space over a totally real field  $F_0$  and  $\sigma$  is defined by  $q(\alpha x, y) = q(x, \alpha^{\sigma} y)$ , where q is a nondegenerate quadratic form on V.

(C)  $L = \operatorname{End}_B(\Lambda)$ , where B is a quaternion algebra over a totally real field  $F_0$  and  $\Lambda$  is a free left B-module of finite rank;  $\sigma$  is defined by  $\varphi(\alpha x, y) = \varphi(x, \alpha^{\sigma} y)$ , where  $\varphi$  is a B-valued form on  $\Lambda$  that is hermitian with respect to the main involution of B.

 $(D^{\mathbb{H}})$  L is the same as in (C), but  $\sigma$  is defined by an anti-hermitian form  $\varphi$ .

We impose the following conditions: for type (A),  $[L: F_0] \ge 2 \cdot 3^2$ ; for types (B) and  $(\mathbb{D}^{\mathbb{R}})$ ,  $\dim_{F_0} V \ge 7$ ; and for type  $(\mathbb{D}^{\mathbb{H}})$ ,  $\operatorname{rank}_B \Lambda \ge 4$ . Then for the given semisimple adjoint group *G*, there is a unique  $(L, \sigma)$  (up to isomorphism) such that the direct factors of  $(L, \sigma)$  satisfy the above conditions and such that the identity component of the automorphism group of  $(L, \sigma)$  is *G*. We refer to  $(L, \sigma)$  as the algebra with involution corresponding to *G*.

1.2. Let  $(G, G', X^+)$  define a connected Shimura variety, with G classical. Let  $(L, \sigma)$  be the algebra with involution corresponding to G, and A the automorphism group of  $(L, \sigma)$ . Since G is the identity component of A, inner automorphisms of A define an injection ad:  $A \to \operatorname{Aut}(G)$ . In fact ad is an isomorphism. This follows from the fact that if  $G_1$ ,  $G_2$  are classical Q-simple groups and  $(L_1, \sigma_1)$ ,  $(L_2, \sigma_2)$  are the corresponding algebras with involution, then every isomorphism of  $G_1$  to  $G_2$  is induced by a unique isomorphism of  $(L_1, \sigma_1)$  to  $(L_2, \sigma_2)$ . Let  $A(\mathbb{Q})^*$  be the group consisting of the  $\gamma \in A(\mathbb{Q})$  such that  $\operatorname{ad} \gamma: G(\mathbb{Q}) \to G(\mathbb{Q})$  is a homeomorphism with respect to the topology defined by G'. If G is Q-simple, then every  $\operatorname{ad} \gamma, \gamma \in A(\mathbb{Q})$ , lifts to an automorphism of  $G'(\mathbb{Q})$ . Therefore  $A(\mathbb{Q})^* = A(\mathbb{Q})$  in this case.

Decompose  $L \otimes_{\mathbb{Q}} \mathbb{R}$  into the direct product of simple algebras  $L_1, \ldots, L_g$  over  $\mathbb{R}$ . Then  $\sigma$  induces an involution  $\sigma_v$  on each factor  $L_v$ . Let  $A_v$  be the group of automorphisms

of  $(L_v, \sigma_v)$ . Denote by S the group of permutations  $\tau$  of  $\{1, \ldots, g\}$  such that  $(L_v, \sigma_v)$  is isomorphic to  $(L_{\tau(v)}, \sigma_{\tau(v)})$  for all v. Then we have an exact sequence

$$1 \to \prod A_{v}(\mathbb{R}) \to A(\mathbb{R}) \to S \to 1.$$

Let  $G_v$  be the identity component of the algebraic group  $A_v$  over  $\mathbb{R}$ . Then  $G_{\mathbb{R}} = \prod G_v$ .

For each v, there is a  $G_v(\mathbb{R})^+$ -conjugacy class  $X_v^+$  of homomorphisms of  $\mathbb{C}^{\times}$  into  $G_v$ such that  $X^+ = \prod X_v^+$ . The adjoint action of A (resp.  $A_v$ ) on G (resp.  $G_v$ ) induces an action of  $A(\mathbb{R})$  (resp.  $A_v(\mathbb{R})$ ) on the set of homomorphisms of  $\mathbb{C}^{\times}$  into  $G_{\mathbb{R}}$  (resp.  $G_v$ ), and we let  $A(\mathbb{R})^1$  (resp.  $A_v(\mathbb{R})^1$ ) be the subgroup that preserves  $X^+$  (resp.  $X_v^+$ ). For each v,  $G_v(\mathbb{R})^+$  is a subgroup of  $A_v(\mathbb{R})^1$  of index at most 2, and ad:  $A_v(\mathbb{R})^1 \to \operatorname{Aut}(X_v)$  is an isomorphism. Furthermore, it is easy to see that we have the following commutative diagram

It follows that  $\operatorname{ad}: A(\mathbb{R})^1 \to \operatorname{Aut}(X^+)$  is an isomorphism. In fact, for  $\gamma \in \operatorname{Aut}(X^+)$  there is a permutation  $\tau$  of  $\{1, \ldots, g\}$  such that  $\gamma$  is given componentwise by isomorphisms  $X_v^+ \xrightarrow{\approx} X_{\tau(v)}^+$ . Then  $\tau \in S$ . Let  $\alpha$  be an element of  $A(\mathbb{R})^1$  that maps to  $\tau$ . Then  $\operatorname{ad} \alpha^{-1} \circ \gamma \in \prod \operatorname{Aut}(X_v)$ . Hence  $\operatorname{ad} \alpha^{-1} \circ \gamma = \prod \operatorname{ad} \alpha_v = \operatorname{ad}(\prod \alpha_v), \alpha_v \in A_v(\mathbb{R})^1$ . Therefore  $\gamma \in \operatorname{ad}(A(\mathbb{R})^1)$ .

Put  $A(\mathbb{Q})^1 = A(\mathbb{Q})^* \cap A(\mathbb{R})^1$ . Then  $A(\mathbb{Q})^1$  acts on the set  $\Sigma$ , and therefore on the connected Shimura variety  $\mathrm{Sh}^\circ(G, G', X^+)$ . The inclusion ad:  $A(\mathbb{Q})^1 \hookrightarrow \mathrm{Aut}(\mathrm{Sh}^\circ(G, G', X^+))$  extends by continuity to the completion  $A(\mathbb{Q})^{1\wedge}(\mathrm{rel}\,G')$  of  $A(\mathbb{Q})^1$  with respect to the topology defined by G'. Note that  $G(\mathbb{Q})^+$  is a subgroup of  $A(\mathbb{Q})^1$  of finite index.

THEOREM 1.3. Under the above hypotheses,  $A(\mathbb{Q})^{1\wedge}(\operatorname{rel} G')$  is the full group of automorphisms of Sh<sup>o</sup>( $G, G', X^+$ ).

Let  $(L, \sigma)$  be the algebra with involution corresponding to G. Let U be the algebraic group over  $\mathbb{Q}$  defined by  $\{x \in L^{\times} \mid xx^{\sigma} = 1, Nx = 1\}$ , where N denotes the reduced norm of L to its centre F. Then U is semisimple and  $U^{ad} = G$ , see Weil 1960, Theorem 2. Let  $\tilde{G}$ be the universal covering group of G and consider the covering  $\tilde{G} \to U$ .

LEMMA 1.4. Let  $\Delta$  be an arithmetic subgroup of  $U(\mathbb{Q})$  that is open with respect to the topology defined by  $\tilde{G}$ . Then for any natural number m,  $\{\delta^m \mid \delta \in \Delta\}$  spans L over  $\mathbb{Q}$ .

PROOF. We follow the argument of Shimura (1970, 6.6) and and K. Miyake (1971, 4.8). Since the image of an arithmetic subgroup under an isogeny is arithmetic (Borel 1969, 8.9), we can assume that  $\Delta$  is the image of a congruence subgroup  $\widetilde{\Delta}$  of  $\widetilde{G}(\mathbb{Q})$ . Choose a rational prime  $p \neq 2$  such that

- (i) the congruence condition defining  $\widetilde{\Delta}$  does not involve *p*;
- (ii) p splits completely in F, the centre of L;
- (iii)  $(L \otimes_{\mathbb{Q}} \mathbb{Q}_p, \sigma)$  splits, i.e., it is the direct product of algebras with involution over  $\mathbb{Q}_p$  of the following types:

(A)  $(M_n(\mathbb{Q}_p) \oplus M_n(\mathbb{Q}_p), \sigma)$ , where  $(X, Y)^{\sigma} = (Y^{\text{tr}}, X^{\text{tr}}), n \ge 3$ ;

(B) and (D)  $(M_n(\mathbb{Q}_n), \sigma)$ , where  $X^{\sigma} = X^{\text{tr}}, n \ge 7$ ;

(C) 
$$(M_{2n}(\mathbb{Q}_p), \sigma)$$
, where  $X^{\sigma} = JX^{\mathrm{tr}}J^{-1}$ ,  $J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ ,  $n \ge 1$ .

Then  $U(\mathbb{Q}_p)$  is isomorphic to the direct product of simple groups of the forms

- (A)  $SL_n(\mathbb{Q}_p), n \geq 3$ ,
- (B) and (D)  $SO_n(\mathbb{Q}_p), n \ge 7$ ,
- (C)  $\operatorname{Sp}_n(\mathbb{Q}_p), n \ge 1.$

Using this isomorphism, we can choose a  $\mathbb{Z}_p$ -order  $\mathcal{O}_p$  in  $L_p \stackrel{\text{def}}{=} L \otimes_{\mathbb{Q}} \mathbb{Q}_p$  invariant under  $\sigma$  such that  $U(\mathbb{Z}_p) \stackrel{\text{def}}{=} \mathcal{O}_p^{\times} \cap U(\mathbb{Q}_p)$  is the direct product of groups of the forms

- (A)  $\operatorname{SL}_n(\mathbb{Z}_p), n \geq 3$ ,
- (B) and (D)  $SO_n(\mathbb{Z}_p), n \geq 7$ ,
- (C)  $\operatorname{Sp}_n(\mathbb{Z}_p), n \ge 1$ .

For a  $\sigma$ -skew symmetric element w of  $p\mathcal{O}_p$ , the Cayley transformation of w lies in  $U(\mathbb{Z}_p)$ . Let  $U' \subset U(\mathbb{Z}_p)$  be the set of Cayley transformations of such elements. Then it is easy to see that for any integer  $m \ge 1$ ,  $\{\alpha^m \mid \alpha \in U'\}$  spans  $L_p$  over  $\mathbb{Q}_p$ .

Let  $\Delta_p$  (resp.  $\widetilde{\Delta}_p$ ) be the closure of  $\Delta$  (resp.  $\widetilde{\Delta}$ ) in  $U(\mathbb{Q}_p)$  (resp.  $\widetilde{G}(\mathbb{Q}_p)$ ). Then  $\Delta_p$  is commensurable with  $U(\mathbb{Z}_p)$ . It follows that for any integer  $m \ge 1$ , there are  $\alpha_1, \ldots, \alpha_k \in \Delta_p$ such that  $\alpha_1^m, \ldots, \alpha_k^m$  form a basis for  $L_p$ . Lift each  $\alpha_i$  to an element  $\beta_i$  of  $\widetilde{\Delta}_p$  and apply the strong approximation theorem for  $\widetilde{G}$  to obtain elements  $b_i$  of  $\widetilde{G}(\mathbb{Q})$  that are in  $\widetilde{\Delta}$  and are close to  $\beta_i$ . Then  $a_i^m$ , where  $a_i \in \Delta$  is the image of  $b_i$ , will be close to  $\alpha_i^m$  in  $\Delta_p$ , and  $a_1^m, \ldots, a_k^m \in L$  will be linearly independent over  $\mathbb{Q}_p$ , and a fortiori over  $\mathbb{Q}$ . Thus the  $\mathbb{Q}$ -linear span of  $a_1^m, \ldots, a_k^m$  is L.

REMARK 1.5. Since any two arithmetic subgroups of  $U(\mathbb{Q})$  are commensurable, Lemma 1.4 holds for every arithmetic subgroup  $\Delta$  of  $U(\mathbb{Q})$ . As S. Kudla pointed out to us, this result also follows from Borel's density theorem (Borel 1966, Theorem 1).

To complete the proof of Theorem 1.3, we have to show that for  $\alpha \in Aut_{\mathbb{C}}(Sh^{\circ}(G, G', X^+))$ and  $\Gamma \in \Sigma$ , there is a  $\beta \in A(\mathbb{Q})^1$  such that

$$\left(\operatorname{Sh}^{\circ} \xrightarrow{\alpha} \operatorname{Sh}^{\circ} \xrightarrow{\operatorname{can}} \Gamma \setminus X^{+}\right) = \left(\operatorname{Sh}^{\circ} \xrightarrow{\operatorname{ad}} \beta \operatorname{Sh}^{\circ} \xrightarrow{\operatorname{can}} \Gamma \setminus X^{+}\right).$$

By definition, there is a  $\Gamma_1 \in \Sigma$  and an isomorphism  $\alpha_1 \colon \Gamma_1 \setminus X^+ \to \Gamma_1 \setminus X^+$  such that the diagram



commutes. As  $X^+$  is simply connected,  $\alpha_1$  can be lifted to an element of Aut $(X^+)$ , say ad  $\beta$  ( $\beta \in A(\mathbb{R})^1$ ). We first show that  $\beta \in A(\mathbb{Q})$ , i.e., it is an automorphism of  $(L, \sigma)$ . Since  $\beta \in A(\mathbb{R})$ , it suffices to show that  $\beta$  maps L into L.

Let  $\pi: U \to G$  be a covering map, and  $\ell$  its degree. Choose arithmetic subgroups  $\Delta, \Delta_1$ of  $U(\mathbb{Q})$  that are open with respect to the topology defined by  $\tilde{G}$  and such that  $\pi(\Delta) \subset \Gamma$ and  $\pi(\Delta_1) \subset \Gamma_1$ . Let *m* be the index of  $\pi(\Delta)$  in  $\Gamma$ . For  $\delta_1 \in \Delta_1$ , we have  $\pi(\delta_1) \in \Gamma_1$  and ad  $\beta(\pi(\delta_1)) \in \Gamma$ . Note that  $\beta(\delta_1^m) \in U(\mathbb{R})$  and  $\pi(\beta(\delta_1^m)) = \operatorname{ad} \beta(\pi(\delta_1))^m \in \pi(\Delta)$ . As the degree of  $\pi$  is  $\ell$ , we see that  $\beta(\delta_1^{m\ell}) \in \Delta$ . Thus  $\beta$  maps  $\{\delta_1^{m\ell} \mid \delta_1 \in \Delta_1\}$  into  $\Delta$ . In view of Lemma 1.4, this proves that  $\beta(L)$  is contained in L. Next we show that  $\operatorname{ad} \beta: G(\mathbb{Q}) \to G(\mathbb{Q})$  is a homeomorphism. Let  $\Gamma' \in \Sigma$  be a normal subgroup of  $\Gamma$ . Then there is a  $\Gamma'_1 \in \Sigma$  contained in  $\Gamma_1$  and an isomorphism  $\alpha'_1: \Gamma'_1 \setminus X^+ \to \Gamma' \setminus X^+$  such that the diagram



commutes. Here q and  $q_1$  denote the natural projections induced by the inclusions  $\Gamma' \hookrightarrow \Gamma$ and  $\Gamma'_1 \hookrightarrow \Gamma_1$ . Applying the above considerations to  $\alpha'_1$ , we see that there is a  $\beta' \in A(\mathbb{Q}) \cap$  $A(\mathbb{R})^1$  such that  $\alpha'_1$  lifts to ad  $\beta' \in \operatorname{Aut}(X^+)$ . We have ad  $\beta'(\Gamma'_1) = \Gamma'$ . As both ad  $\beta$  and ad  $\beta'$  induce  $\alpha_1$ , there is a  $\gamma \in \Gamma$  such that ad  $\beta = \operatorname{ad} \gamma \beta'$ . Hence

ad 
$$\beta(\Gamma'_1) = (\operatorname{ad} \gamma \circ \operatorname{ad} \beta')(\Gamma'_1) = \operatorname{ad} \gamma(\Gamma') = \Gamma',$$

because  $\Gamma'$  is a normal subgroup of  $\Gamma$ . Since the normal subgroups  $\Gamma'$  of  $\Gamma$ ,  $\Gamma' \in \Sigma$ , form a basis for the neighbourhoods of 1, this shows that  $\mathrm{ad}\,\beta$  is continuous. The same argument applied to  $\beta^{-1}$  shows that  $\beta$  is a homeomorphism. Therefore  $\beta \in A(\mathbb{Q})^* \cap A(\mathbb{R})^1 = A(\mathbb{Q})^1$ and  $\mathrm{ad}\,\beta \circ \alpha^{-1} \in \operatorname{Aut}_{\mathbb{C}}(\operatorname{Sh}^\circ)$  induces the identity map on  $\Gamma \setminus X^+$ .

1.6. The above techniques can be used to compute the automorphism group of a single  $\Gamma \setminus X^+$ . Let *G* be classical and  $\Gamma \in \Sigma$ . An automorphism  $\alpha$  of  $\Gamma \setminus X^+$  lifts to an automorphism  $\mathrm{ad}\beta$  of  $X^+$ ,  $\beta \in A(\mathbb{R})^1$ . The argument in the proof of 1.3 shows that  $\beta \in A(\mathbb{Q}) \cap A(\mathbb{R})^1$ . Conversely, every  $\beta \in A(\mathbb{Q}) \cap A(\mathbb{R})^1$  such that  $\mathrm{ad}\beta(\Gamma) = \Gamma$  defines an automorphism of  $\Gamma \setminus X^+$ . Thus  $\mathrm{Aut}_{\mathbb{C}}(\Gamma \setminus X^+)$  is the quotient of

$$\{\beta \in A(\mathbb{Q}) \cap A(\mathbb{R})^1 \mid \mathrm{ad}\,\beta(\Gamma) = \Gamma\}$$

by the subgroup of  $\beta$  such that

$$\left(X^+ \xrightarrow{\operatorname{ad}\beta} X^+ \xrightarrow{\operatorname{can}} \Gamma \setminus X^+\right) = \left(X^+ \xrightarrow{\operatorname{can}} \Gamma \setminus X^+\right).$$

In particular, if  $A(\mathbb{Q}) = A(\mathbb{Q})^*$  (this is the case if *G* is  $\mathbb{Q}$ -simple or  $G' = \tilde{G}$ , the universal covering group of *G*), then every element of  $\operatorname{Aut}_{\mathbb{C}}(\Gamma \setminus X^+)$  is induced by  $\operatorname{ad}\beta$  with  $\beta \in A(\mathbb{Q})^1$ , hence can be extended to an element of  $\operatorname{Aut}_{\mathbb{C}}(\operatorname{Sh}^\circ(G, G', X^+))$ ). This is not true if  $A(\mathbb{Q})^* \neq A(\mathbb{Q})$ . Note also that we need to assume that  $\Gamma$  is torsion free. For example, if  $X^+$  is the complex upper half plane, then the only automorphism of  $\operatorname{SL}_2(\mathbb{Z}) \setminus X^+$  that can be extended to an automorphism of  $\operatorname{Sh}^\circ(\operatorname{PGL}_2, \operatorname{SL}_2, X^+)$  is the identity map.

1.7. The automorphism group of a non-connected Shimura variety Sh(G, X) (Deligne 1979, 2.1) is very large and complicated. However, the subgroup of automorphisms commuting with the Hecke operators is small: it consists only of the identity element if G is adjoint.<sup>2</sup>

<sup>&</sup>lt;sup>2</sup>27.03.23. See Corollary 2.6 of Milne, J.S., *The action of an automorphism of*  $\mathbb{C}$  *on a Shimura variety and its special points* In: Arithmetic and Geometry, Papers dedicated to I.R. Shafarevich on the occasion of his sixtieth birthday, Progress in Math. 35 (1983), Birkhauser Verlag, 239-265.

# 2 The automorphism group of a field of automorphic functions

Let  $(G, G', X^+)$  define a connected Shimura variety, and let  $\Sigma$  be as in §1. For  $\Gamma \in \Sigma$ , we let  $\mathcal{F}(\Gamma)$  denote the function field of the algebraic variety  $\Gamma \setminus X^+$  and we let  $\mathcal{F} = \lim \mathcal{F}(\Gamma)$ .

An element f of  $\mathcal{F}(\Gamma)$  can be identified with a meromorphic function  $\tilde{f}$  on the bounded symmetric domain  $X^+$  invariant under  $\Gamma$ . A meromorphic function on  $X^+$  arising in this way is said to be automorphic with respect to  $\Gamma$ . Thus  $\mathcal{F}$  can be regarded as the field of all meromorphic functions on  $X^+$  automorphic with respect to some  $\Gamma \in \Sigma$ . When  $\Gamma \setminus X^+$  is compact, the comparison theorem (Shafarevich 1994, VIII, 3.1) shows that  $\mathcal{F}(\Gamma)$  is equal to the field of meromorphic functions on  $X^+$  invariant under  $\Gamma$ . The same is always true if Ghas no  $\mathbb{Q}$ -rational simple factors isomorphic to PGL<sub>2</sub> (Baily and Borel 1966, 10.12). For the remaining case, an automorphic function is required to be meromorphic at the cusps.

An automorphism  $\alpha$  of Sh<sup>°</sup>( $G, G', X^+$ ) defines an automorphism  $\alpha^*$  of  $\mathcal{F}$  over  $\mathbb{C}$  by the rule:  $\alpha^* f = f \circ \alpha^{-1}$ . If Aut( $\mathcal{F}/\mathbb{C}$ ) is given its usual topology (Shimura 1971b, 6.3), then  $\alpha \mapsto \alpha^*$  is continuous.

**PROPOSITION 2.1.** The map

$$\alpha \mapsto \alpha^* : \operatorname{Aut}_{\mathbb{C}}(\operatorname{Sh}^{\circ}(G, G', X^+)) \to \operatorname{Aut}(\mathcal{F}/\mathbb{C})$$

is an isomorphism of topological groups.

PROOF. As  $\Gamma \setminus X^+$  is separated as an algebraic variety, a morphism  $V \to \Gamma \setminus X^+$  is determined by its action on  $\mathcal{F}(\Gamma)$ . Thus  $\alpha \mapsto \alpha^*$  is injective. In proving that the map is surjective, we follow an argument of T. Miyake 1972, which is based on the following result:

every isomorphism  $X^+ \\ Y_1 \\ \to \\ X^+ \\ Y$ , where *Y* and *Y*<sub>1</sub> are proper analytic subsets of  $X^+$ , extends to an automorphism of  $X^+$  (ibid., §4(I)).

Let  $\alpha^*$  be an element of Aut( $\mathcal{F}/\mathbb{C}$ ). Then, for any  $\Gamma \in \Sigma$ , there is a unique  $\Gamma_1 \in \Sigma$  such that  $\alpha^*(\mathcal{F}(\Gamma)) = \mathcal{F}(\Gamma_1)$ ; ibid. §4.(I). Thus the restriction of  $\alpha^*$  to  $\mathcal{F}(\Gamma)$  defines a rational map  $\alpha_{\Gamma}: \Gamma_1 \setminus X^+ \dashrightarrow \Gamma \setminus X^+$ . We show that  $\alpha_{\Gamma}$  is an isomorphism. Let V and  $V_1$  be Zariskiopen subsets of  $\Gamma \setminus X^+$  and  $\Gamma_1 \setminus X^+$  such that  $\alpha_{\Gamma}$  is an isomorphism from  $V_1$  to V. The inverse images Y and  $Y_1$  of  $(\Gamma \setminus X^+) \smallsetminus V$  and  $(\Gamma_1 \setminus X^+) \backsim V_1$  are proper analytic subsets of  $X^+$ . Consider the coverings  $X^+ \backsim Y \to V$  and  $X^+ \backsim Y_1 \to V_1$ . The argument of T. Miyake (ibid., §4.(III)) shows that  $\alpha_{\Gamma}: V_1 \to V$  lifts to an isomorphism  $\tilde{\alpha}_{\Gamma}: X^+ \backsim Y_1 \to X^+ \backsim Y$  which, according to the result recalled above, extends to an automorphism  $\tilde{\alpha}_{\Gamma}$  of  $X^+$ . This  $\tilde{\alpha}_{\Gamma}$  induces an isomorphism of  $\Gamma_1 \setminus X^+$  to  $\Gamma \setminus X^+$  that agrees with  $\alpha_{\Gamma}$  on  $V_1$ . Therefore (ibid., Lemma 1)  $\alpha_{\Gamma}$  is defined everywhere and is an isomorphism from  $\Gamma_1 \setminus X^+$  to  $\Gamma \setminus X^+$ .

Thus, for every  $\Gamma \in \Sigma$ , there is a unique  $\Gamma_1 \in \Sigma$  and an isomorphism  $\alpha_{\Gamma}: \Gamma_1 \setminus X^+ \to \Gamma \setminus X^+$  such that  $\alpha_{\Gamma}^*: \mathcal{F}(\Gamma) \to \mathcal{F}(\Gamma_1)$  is the restriction of  $\alpha^*$  to  $\mathcal{F}(\Gamma)$ . If  $\Gamma' \in \Sigma$  is contained in  $\Gamma$ , then the corresponding  $\Gamma'_1$  is contained in  $\Gamma_1$ , and the diagram

$$\begin{array}{ccc} \Gamma_1' \backslash X^+ & \xrightarrow{\alpha_{\Gamma'}} & \Gamma' \backslash X^+ \\ \downarrow & & \downarrow \\ \Gamma_1 \backslash X^+ & \xrightarrow{\alpha_{\Gamma}} & \Gamma \backslash X^+ \end{array}$$

commutes. Therefore  $\{\alpha_{\Gamma} \mid \Gamma \in \Sigma\}$  defines an automorphism  $\alpha$  of  $Sh^{\circ}(G, G', X^+)$  whose image in  $Aut(\mathcal{F}/\mathbb{C})$  is  $\alpha^*$ .

# **3** The automorphism group of a field of arithmetic automorphic functions

3.1. Throughout this section, G will be assumed to be classical and  $\text{Sh}^{\circ}(G, G', X^+)$  will be assumed to have a canonical model  $M^{\circ}(G, G', X^+)$  in the sense of Deligne 1979, 2.7.10. (For a list of those Shimura varieties known<sup>3</sup> to have canonical models, see ibid., 2.7.20.) Let  $E = E(G, X^+)$  be the reflex field; then  $M^{\circ}(G, G', X^+)$  is a scheme over  $\overline{\mathbb{Q}}$  together with a left action of the middle term of the canonical extension

$$1 \to G(\mathbb{Q})^{+\wedge}(\operatorname{rel} G') \to \mathcal{E}(G, G', X^+) \xrightarrow{\sigma} \operatorname{Gal}(\overline{\mathbb{Q}}/E) \to 1$$

(ibid., 2.5.9). For any  $\Gamma \in \Sigma$ ,  $\Gamma \setminus M^{\circ}$  is a model for  $\Gamma \setminus X^{+}$  over  $\overline{\mathbb{Q}}$ . Thus its function field  $F(\Gamma)$  is a subfield of  $\mathcal{F}(\Gamma)$  linearly disjoint from  $\mathbb{C}$  over  $\overline{\mathbb{Q}}$  and such that  $\mathbb{C} \cdot F(\Gamma) = \mathcal{F}(\Gamma)$ . We define F, *the field of arithmetic automorphic functions* on  $X^{+}$  relative to (G, G') to be  $\bigcup F(\Gamma) \subset \mathcal{F}$ .

We note that a Hilbert or Siegel modular function is arithmetic in this sense if and only if it the quotient of two modular forms with algebraic Fourier coefficients (Shimura 1975).

3.2. For any  $\Gamma, \Gamma' \in \Sigma$ , there are only countable many isomorphisms  $\alpha: (\Gamma' \setminus M^{\circ})_{\mathbb{C}} \to (\Gamma \setminus M^{\circ})_{\mathbb{C}}$  that extend to automorphisms of  $\mathrm{Sh}^{\circ}(G, G', X^+)$ . Thus, each such  $\alpha$  is defined over  $\overline{\mathbb{Q}}$ , and we can identify  $\mathrm{Aut}_{\mathbb{C}}(\mathrm{Sh}^{\circ}(G, G', X^+))$  with its subgroup  $\mathrm{Aut}_{\overline{\mathbb{Q}}}(M^{\circ}(G, G', X^+))$ . Theorem 1.3 provides us with an isomorphism

$$A(\mathbb{Q})^{1\wedge}(\operatorname{rel} G') \xrightarrow{\simeq} \operatorname{Aut}_{\overline{\mathbb{Q}}}(M^{\circ}(G,G',X^+)).$$

The two actions of  $G(\mathbb{Q})^{+\wedge}(\operatorname{rel} G')$  on  $M^{\circ}(G, G', X^+)$ , arising from the actions of  $A(\mathbb{Q})^{1\wedge}(\operatorname{rel} G')$  and  $\mathcal{E}(G, G', X^+)$ , are the same. For any  $\alpha \in \mathcal{E}(G, G', X^+)$ ,

commutes (Deligne 1979, 2.7.10). Thus, we can define an action of  $\mathcal{E}(G, G', X^+)$  on F by setting  ${}^{\alpha}f = \sigma(\alpha) \circ f \circ \alpha^{-1}$  for  $f \in F$  and  $\alpha \in \mathcal{E}(G, G', X^+)$ . Note that if  $\alpha \in G(\mathbb{Q})^{+\wedge}$  (rel  $G') \subset \mathcal{E}(G, G', X^+)$ , then  ${}^{\alpha}f = \alpha^* f$  (with the notation of §2).

THEOREM 3.3. The map  $\mathcal{E}(G, G', X^+) \to \operatorname{Aut}(F/E)$  identifies  $\mathcal{E}(G, G', X^+)$  with an open subgroup of  $\operatorname{Aut}(F/E)$  of finite index.

PROOF. This follows from the commutative diagram

since we know from §1 and §2 that the left hand vertical arow identifies  $G(\mathbb{Q})^{+\wedge}$  (rel G') with an open subgroup of Aut $(F/\mathbb{Q})$  of finite index.

 $<sup>^{3}</sup>$ 27.03.23. In fact, all Shimura varieties are known to have canonical models — see the article in footnote 2.

3.4. The reciprocity law at a special  $h \in X^+$  (Deligne 1979, 2.7.10c) has the following interpretation. Let *T* be a  $\mathbb{Q}$ -rational torus *G* such that *h* factors through  $T(\mathbb{R})$ . In ibid. 2.5.10, Deligne constructs an extension  $\mathcal{D}$  of  $\operatorname{Gal}(\overline{\mathbb{Q}}/E(T,h))$  by  $T(\mathbb{Q})$  and a commutative diagram



Let  $\lambda \in \mathcal{D}$  have images  $\alpha(\lambda)$  in  $\mathcal{E}(G, G', X^+)$  and  $\sigma(\lambda)$  in  $\operatorname{Gal}(\overline{\mathbb{Q}}/E(T, h))$ . If z = [h] is the point on  $M(G, G', X^+)$  defined by h, then Deligne's reciprocity law says that  $\alpha(\lambda)z = z$ . Thus, for any  $f \in F$  that is defined at z,  $\alpha(\lambda)f(z) = \sigma(\lambda)(f(z))$ .

3.5. Let  $(L,\sigma)$  be the algebra with involution corresponding as in 1.1 to G, and let  $A = Aut(L,\sigma)$ . According to Deligne (1979, 2.7.16), there is a pair  $(G_1, X_1)$  satisfying the axioms for a Shimura variety and such that

$$(G_1^{\mathrm{ad}}, G_1^{\mathrm{der}}, X_1^+) = (G, G', X^+)$$
  
 $E(G_1, X_1) = E(G, X^+).$ 

We assume that it is possible to choose  $(G_1, X_1)$  so that there is an action ad:  $A \to \operatorname{Aut}(G_1)$ of A on  $G_1$  that is compatible with the action of A on G. (For this to be possible, it is obviously necessary that the action of A on  $Z(\tilde{G})$ , the centre of  $\tilde{G}$ , induces an action of Z(G'); in 3.7 below we show that this condition is also sufficient.) Under this assumption, we can apply the functor  $-*_{G_1(\mathbb{Q})+/Z_1(\mathbb{Q})} A(\mathbb{Q})^1$  to the first two terms of the sequence

$$1 \to G_1(\mathbb{Q})^{\wedge}_+ / Z_1(\mathbb{Q})^{\wedge} \to G_1(\mathbb{A}_f) / Z_1(\mathbb{Q})^{\wedge} \to \overline{\pi}_0 \pi(G_1) \to \mathbb{I}$$

and obtain an exact sequence

$$1 \to A(\mathbb{Q})^{1\wedge}(\operatorname{rel} G') \to \frac{G_1(\mathbb{A}_f)}{Z_1(\mathbb{Q})^{\wedge}} *_{G_1(\mathbb{Q})_+/Z_1(\mathbb{Q})} A(\mathbb{Q})^1 \to \overline{\pi}_0 \pi(G_1) \to 1$$

(cf. Deligne 1979, 2.5.1). On pulling-back relative  $\operatorname{Gal}(\overline{\mathbb{Q}}/E) \to \overline{\pi}_0 \pi(G)$ , we obtain the second row of the following exact commutative diagram

This diagram is independent of the choice of  $(G_1, X_1)$ . We give  $\mathcal{E}^e(G, G', X^+)$  the topology for which  $\mathcal{E}(G, G', X^+)$  is an open subgroup. The actions of  $A(\mathbb{Q})^{1\wedge}$  (rel G') and  $\mathcal{E}(G, G', X^+)$  on F combine to give an action of  $\mathcal{E}^{\sigma}(G, G', X^+)$  on F.

THEOREM 3.6. Under the above assumption, there is an isomorphism of topological groups  $\mathcal{E}^e(G, G', X^+) \to \operatorname{Aut}(F/E)$ .

PROOF. The proof is the same as that of 3.3.

LEMMA 3.7. With the notation of 3.5, assume that the action of A on  $Z(\tilde{G})$  induces an action of A on the quotient Z(G') of  $Z(\tilde{G})$ . Then there exists a  $(G_1, X_1)$  such that

$$(G_1^{\mathrm{ad}}, G_1^{\mathrm{der}}, X_1^+) = (G, G', X^+)$$
  
 $E(G_1, X_1) = E(G, X^+),$ 

and the action of A on G lifts to an action of  $G_1$ .

PROOF. We have only to modify slightly the proof in Milne and Shih 1982b, §3. Let T be a maximal torus in G and T' its inverse image in G'. Then

$$M \stackrel{\text{\tiny def}}{=} X_*(T) / X_*(T') \simeq \operatorname{Hom}(X^*(Z(G')), \mathbb{Q}/\mathbb{Z}),$$

and so, by assumption, has a natural action by  $A/A^{\circ}$ . The sequence

$$0 \to P_1 \to P_0 \to M \to 0$$

of Lemma 3.2, ibid., can then be chosen to have an action by  $A/A^\circ$ . The centre of the group  $G_1$  constructed ibid., 3.1, is a torus  $Z(G_1)$  such that  $X_*(Z(G_1)) = P_1$ . It therefore carries an action by  $A/A^\circ$  such that  $Z(\tilde{G}) \to Z(G_1)$  is equivariant. Since  $G_1 = \tilde{G} *_{Z(\tilde{G})} Z(G_1)$ , it also carries an action by A. According to ibid., 3.4, it is now possible to choose  $X_1$  such that  $E(G_1, X_1) = E(G, X^+)$ .

## 4 The main theorems for canonical models in the sense of Shimura

4.1. Let G be a reductive group and X a family of maps  $\mathbb{C}^{\times} \to G(\mathbb{R})$  such that (G, X) satisfies the axioms for a Shimura variety (Deligne 1979, 2.1.1). Assume that Sh(G, X) has a canonical model  $(M(G, X), \varphi: Sh(G, X) \to M(G, X)_{\mathbb{C}})$  in the sense of Deligne 1979, 2.2.5, defined over its reflex field E = E(G, X). We begin this section by showing how to derive from M(G, X) a canonical model in the sense of Shimura 1970.

4.2. Let  $\ell = \ell_{G,X}$  be the map

$$\pi_0 N_{E/\mathbb{Q}} q_M : \operatorname{Gal}(\overline{\mathbb{Q}}/E)^{\operatorname{ab}} = \pi_0 \pi(\mathbb{G}_{mE}) \to \overline{\pi}_0 \pi(G)$$

explicitly defined in Deligne 1979, 2.6.2.1. According to Deligne (ibid., 2.6.3),  $\sigma \epsilon = \ell(\sigma)\epsilon \stackrel{\text{def}}{=} \epsilon \ell(\sigma)^{-1}$  for  $\epsilon \in \pi_0(M(G, X)_{\overline{\mathbb{Q}}})$ . Let  $\mathfrak{k}$  be the subfield of  $\overline{\mathbb{Q}}$  corresponding to the kernel of  $\ell$  and define  $\overline{\mathcal{E}}(G, X)$  to make the following diagram exact and commutative,

Thus  $\overline{\mathcal{E}}(G, X)$  is a quotient of  $\mathcal{E}(G^{\mathrm{ad}}, G^{\mathrm{der}}, X^+)$ . Let  $\mathfrak{z}$  be the set of open compact subgroups of  $\overline{\mathcal{E}}(G, X)$  and for any  $S \in \mathfrak{z}$ , let  $k_S$  be the subfield of  $\mathfrak{k}$  defined by  $\sigma(S)$ . Let  $\Gamma_S =$ 

 $S \cap G^{ad}(\mathbb{Q})^+$ , and choose a connected component  $X^+$  of X. We shall construct a family  $(V_S, \varphi_S), S \in \mathfrak{z}$ , of models for the varieties  $\Gamma_S \setminus X^+$ , and a family of maps  $(J_{TS}(x)), x \in \overline{\mathcal{E}}(G, X)$  analogous to those constructed in special cases by Shimura (1970, 2.5), K. Miyake (1971, 4.1), and Shih (1979, 2.4; 1981, 3).

4.3. The group  $\Gamma_S$  is open relative to the topology on  $G^{ad}(\mathbb{Q})$  defined by  $G^{der}$ , and is torsion free (and so belongs to  $\Sigma$ ) if *S* is sufficiently small. Set  $S_0 = S \cap G^{ad}(\mathbb{Q})^+$  (rel *G'*). Let  $Sh(G, X)^\circ$  be the connected component of Sh(G, X) containing the image of  $X^+ \times \{1\}$ . Thus  $\Gamma_S \setminus X^+ \xrightarrow{\simeq} S_0 \setminus Sh(G, X)^\circ$ . For some connected component  $M(G, X)^\circ$ of  $M(G, X)_{\overline{\mathbb{Q}}}$ ,  $\varphi$  induces an isomorphism  $Sh(G, X)^\circ \xrightarrow{\simeq} M(G, X)_{\mathbb{C}}^\circ$ , and we let *e* denote  $M(G, X)^\circ$  regarded as a point on the pro-finite scheme  $\pi_0(M(G, X))$ . As *e* is fixed by  $Gal(\overline{\mathbb{Q}}/\mathfrak{k}), M(G, X)^\circ$  is defined over  $\mathfrak{k}$ . The group  $\overline{\mathcal{E}}(G, X)$  acts on  $M(G, X)^\circ$  compatibly with the action of its quotient  $Gal(\mathfrak{k}/E)$  on  $\mathfrak{k}$ . Thus  $V_S \stackrel{\text{def}}{=} S \setminus M(G, X)^\circ$  is a model of  $S_0 \setminus M(G, X)^\circ$  rational over  $k_S$ . Define  $\varphi_S$  to be the composite,

$$\Gamma_S \setminus X^+ \xrightarrow{\simeq} S_0 \setminus \operatorname{Sh}(G, X)^\circ \xrightarrow{\simeq} S_0 \setminus M(G, X)^\circ_{\mathbb{C}} \xrightarrow{\simeq} (V_S)_{\mathbb{C}}.$$

4.4. The compatibility of the actions of  $\overline{\mathcal{E}}(G, X)$  on  $M(G, X)^{\circ}$  and  $\mathfrak{k}$  means that, for any  $\alpha \in \overline{\mathcal{E}}(G, X)$ ,



commutes. We therefore have a map of  $\mathfrak{k}$ -schemes  $J(\alpha): M(G, X)^{\circ} \to \sigma(\alpha)^{-1} M(G, X)^{\circ}$  such that  $\sigma(\alpha) \circ J(\alpha) = \alpha$ ,

If  $S, T \in \mathfrak{z}$  are such that  $\alpha S \alpha^{-1} \subset T$ , then  $J(\alpha)$  defines a map on the quotients,

$$J_{TS}(\alpha): V_S \to T \setminus (\sigma(\alpha)^{-1} M(G, X)^{\circ}) = \sigma(\alpha)^{-1} V_T.$$
  
Thus, for  $f \in k_T(V_T)$ ,  $(\sigma(\alpha)^{-1} f) \circ J_{TS}(\alpha) = {}^{\alpha^{-1}} f \stackrel{\text{def}}{=} \sigma(\alpha)^{-1} \cdot f \circ \alpha.$ 

4.5. Let  $h \in X^+$  be special, so that *h* factors through  $H(\mathbb{R})$  for some  $\mathbb{Q}$ -rational torus  $H \subset G$ , and let  $\mu$  be the cocharacter of  $G_{\mathbb{C}}$  defined *h*. By definition, the reflex field E(h) is the smallest field over which  $\mu$  is defined. Let  $\eta$  be the homomorphism of algebraic groups

$$E(h)^{\times} \xrightarrow{NR(\mu)} H \hookrightarrow G,$$

where, as in Deligne 1979, 2.2.2,  $NR(\mu)$  is the composite

$$E(h)^{\times} = \operatorname{Res}_{E(h)/\mathbb{Q}}(\mathbb{G}_{mE(h)}) \xrightarrow{\operatorname{Res}(\mu)} \operatorname{Res}_{E(h)/\mathbb{Q}}(H_{E(h)}) \xrightarrow{N_{E(h)/\mathbb{Q}}} H.$$

Let *M* be the  $G(\mathbb{C})$ -conjugacy class of maps  $\mathbb{C}^{\times} \to G(\mathbb{C})$  associated with *X*, and let  $q_m: \pi(\mathbb{G}_{mE}) \to \pi(G_E)$  and  $N_{E/\mathbb{Q}}: \pi(G_E) \to \pi(G)$  be the maps defined in Deligne 1979, 2.4. It follows directly from the definitions that

$$\begin{array}{ccc} \mathbb{A}_{E(h)}^{\times} & \xrightarrow{\eta} & G(\mathbb{A}) \\ & & & \downarrow \\ \mathbb{A}_{E}^{\times} & \longrightarrow \pi(\mathbb{G}_{mE}) \xrightarrow{N_{E/\mathbb{Q}} \circ q_{m}} \pi(G) & \longrightarrow \overline{\pi}_{0}\pi(G) \end{array}$$

commutes. Let  $v \in \mathbb{A}_{E(h)}^{\times}$  and let [v] and  $[\eta(v)]$  denote respectively the images of v and  $\eta(v)$  in  $\operatorname{Gal}(E(h)^{\operatorname{ab}}/E(h))$  and  $\overline{\pi}_0\pi(G)$ . The above diagram and Deligne 1979, 2.6.3, show that  $[\eta(v)]\epsilon = \ell_{G,X}(N_{E(h)/E}(v)) \cdot \epsilon = [v]\epsilon$  for  $\epsilon \in \pi_0(M(G,X)_{\overline{\mathbb{Q}}})$ . The element  $\eta(v) * 1 \in G(\mathbb{A}_f)/Z(\mathbb{Q})^{\wedge} * \cdots$  maps to  $\ell_{G,X}(N_{E(h)/E}(v))$  and therefore lies in  $\overline{\mathcal{E}}(G,X)$ ; we have therefore a map  $\overline{\eta} = (v \mapsto \eta(v) * 1) : \mathbb{A}_{E(h)}^{\times} \to \overline{\mathcal{E}}(G,X)$ . Moreover,  $\sigma(\overline{\eta}(v)) = [v]^{-1}|_{\mathfrak{k}}$ .

THEOREM 4.6. (a) For each  $S \in \mathfrak{z}$ ,  $(V_S, \varphi_S)$  is a model of  $\Gamma_S \setminus X^+$  over  $k_S$ .

(b) For any  $\alpha \in \overline{\mathcal{E}}(G, X)$  and  $S, T \in \mathfrak{z}$  such that  $\alpha S \alpha^{-1} \subset T$ ,  $J_{TS}(\alpha)$  is a map  $V_S \rightarrow \sigma(\alpha)^{-1} V_T$  defined over  $k_S$ . The following hold:

$$J_{SS}(\alpha) \text{ is the identity map if } \alpha \in S;$$
  

$$(\sigma(\alpha)^{-1}J_{TS}(\beta)) \circ J_{SR}(\alpha) = J_{TR}(\beta\alpha);$$
  

$$J_{TS}(\alpha) \circ \varphi_S = \varphi_T \circ \alpha \text{ for all } \alpha \in G(\mathbb{Q})_+ \text{ such that } \alpha S \alpha^{-1} \subset T.$$

(c) Let  $z \in X^+$  be special; for each  $S \in \mathfrak{z}$ ,  $\varphi_S(z)$  is rational over  $E(z)^{ab}$ , and for every  $\nu \in \mathbb{A}_{f,E(z)}^{\times}$ ,

$$[\nu]\varphi_S(z) = J_{ST}(\overline{\eta}(\nu))\varphi_T(z),$$

where [v] is the element of  $\operatorname{Gal}(E(z)^{\operatorname{ab}}/E(z))$  corresponding to v and  $T = \overline{\eta}(v)^{-1}S\overline{\eta}(v)$ .

PROOF. Both (a) and (b) follow directly from the definitions. Let  $z \in X^+$  be special and let  $\nu \in \mathbb{A}_{f,E(z)}^{\times}$ . One of the conditions for M(G,X) to be a canonical model is that  $[\nu][z,1] = [z,\eta(\nu)^{-1}]$ , where [z,1] is regarded as a point on  $M(G,X)_{\overline{\mathbb{Q}}}$  (Deligne 1979, 2.2.5). Therefore,

$$\overline{\eta}(\nu)[z,1] \stackrel{\text{\tiny def}}{=} \sigma(\eta(\nu))[z,\eta(\nu)^{-1}] \stackrel{\text{\tiny 4.5}}{=} [\nu]^{-1}[z,\eta(\nu)^{-1}] = [z,1],$$

and so  $J(\overline{\eta}(\nu))[z, 1] = [\nu][z, 1]$ , which implies (c).

4.7. It is sometimes possible to strengthen this theorem by enlarging  $\overline{\mathcal{E}}(G, X)$  and  $\mathfrak{Z}$ . Let A be the algebraic group associated with  $G^{ad}$  as in §1, and assume that the action of A on  $G^{ad}$  extends to an action on G (cf. 3.7). Since  $G = \widetilde{G} *_{Z(\widetilde{G})} Z(G)$  it is only necessary for this that the action of  $A/A^\circ$  on  $Z(\widetilde{G})$  extend to Z(G). Under this assumption, we can construct, as in 3.5 and 4.2, extensions

Let 3 be the set of compact open subgroups of  $\overline{\mathcal{E}^e}(G, X)$ . Then, exactly as before, we can construct a family  $(V_S, \varphi_S, J_{ST}(\alpha))$  with the same properties as the family in 4.6 except that now *S* and *T* are allowed to lie in 3 and  $\alpha$  in  $\overline{\mathcal{E}}(G, X)$ . For example, if  $G^{ad}$  is Q-simple of type *C* or *A* and we take (G, X) to be the pair denoted  $(G_0, X_0)$  in the appendix of Milne and Shih 1981, then we obtain the families constructed in Shimura 1970, 5.2, and K. Miyake 1971, 4.1.

4.8. We return to the situation of 4.6. For any  $S \in \mathfrak{z}$ , the function field F(S) of  $V_S$  is a subfield of the function field  $\mathcal{F}(\Gamma_S)$  of  $\Gamma_S \setminus M(G, X)^\circ$  linearly disjoint from  $\mathbb{C}$  over  $\overline{\mathbb{Q}}$  and such that  $\mathbb{C} \cdot F(S) = \mathcal{F}(\Gamma_S)$ . We define F', the *field of arithmetic automorphic functions* on  $X^+$  relative to G to be  $\bigcup F(S) \subset \mathcal{F}$ . Thus  $f \in \mathcal{F}$  is in F' if and only if there is an  $S \in \mathfrak{z}$  such that  $f = g \circ \varphi_S$  for some  $g \in k_S(V_S)$ . We define an action of  $\overline{\mathcal{E}}(G, X)$  on F' as follows: for  $\alpha \in \overline{\mathcal{E}}(G, X)$ ,  $f \in F'$ , and  $z \in M(G, X)^\circ$ , we set  ${}^{\alpha}f(z) = \sigma(\alpha) \circ f \circ \alpha^{-1}(z)$ . Thus, if  $f = g \circ \varphi_S$ , then  ${}^{\alpha}f = {}^{\alpha}g \circ \varphi_S = (\sigma(\alpha)g) \circ J_{ST}(\alpha^{-1}) \circ \varphi_T$  (cf. 4.4).

THEOREM 4.9. If  $G^{ad}$  is classical, then  $\overline{\mathcal{E}}(G, X)$  is isomorphic to an open subgroup of  $\operatorname{Aut}(F'/E)$  of finite index.

PROOF. The proof is the same as that of 3.4.

4.10. There is a reciprocity law at the special points: with the notation of 4.5, for any special  $z \in X^+$  and  $f \in F'$  defined at z,  $f(z) \in E(z)^{ab}$ ; moreover, for any  $v \in \mathbb{A}_{f,E(z)}^{\times}$ , the function  $\overline{\eta}(v)^{-1}f$  is also defined at z, and  $[v]f(z) = \overline{\eta}(v)^{-1}f(z)$  (because  $\overline{\eta}(v)^{-1}f \stackrel{\text{def}}{=} [v] \circ f \circ \overline{\eta}(v)$ , and  $\overline{\eta}(v)z = z$ ; cf. the proof of 4.6c).

4.11. In the case that (as in 4.7) the action of A on  $G^{ad}$  extends to G, we can replace  $\overline{\mathcal{E}}(G, X)$  with  $\overline{\mathcal{E}}^e(G, X)$  and  $(V_S, \varphi_S), S \in \mathfrak{z}$ , with the larger family  $(V_S, \varphi_S), S \in \mathfrak{z}$ . The field  $F' = \bigcup F(S)$  is unchanged. If further  $G^{ad}$  is classical, then there is an isomorphism  $\mathcal{E}^e(G, X) \xrightarrow{\simeq} \operatorname{Aut}(F'/E)$  of topological groups.

4.12. In the special case that  $G^{der}$  is simply connected and the centre Z of G is a cohomologically trivial torus, the above results can be made more explicit. This will be so, for example, if  $G^{ad}$  is Q-simple of type A, B, or C and (G, X) is taken to be the pair denoted  $(G_0, X_0)$  in the appendix to Milne and Shih 1981. (These are the cases studied in K. Miyake 1971, Shih 1979, and Shimura 1970 respectively.)

Let T be the torus defined by the exact sequence

 $1 \to G^{\mathrm{der}} \to G \xrightarrow{\nu} T \to 1.$ 

Since  $G^{der}$  is simply connected, the map

$$\pi_0\pi(G) = \pi_0(G(\mathbb{Q})\backslash G(\mathbb{A})) \to \pi_0(T(\mathbb{Q})\backslash T(\mathbb{A}))$$

induced by  $\nu$  is an isomorphism (Deligne 1971, 2.4). As

$$G(\mathbb{R})_{+} = \{g \in G(\mathbb{R}) \mid \nu(g) \in \nu(Z(\mathbb{R}))\}$$

(see Milne and Shih 1981, 3.1), we see that

$$\overline{\pi}_0 \pi(G) \stackrel{\text{def}}{=} \pi_0(G(\mathbb{R})_+) \backslash \pi_0 \pi(G)$$
$$= \nu(Z(\mathbb{R}) \backslash \pi_0(T(\mathbb{Q}) \backslash T(\mathbb{A}))$$
$$= T(\mathbb{A}) / T^c \nu(Z(\mathbb{R})),$$

where  $T^c$  is the closure of  $T(\mathbb{R})^+T(\mathbb{Q})$  in  $T(\mathbb{A})$ . In many cases,  $\nu(Z(\mathbb{R})) \subset T(\mathbb{R})^+$  and so  $\overline{\pi}_0\pi(G) = T(\mathbb{A})/T^c$ .

The map  $\ell$ : Gal $(E^{ab}/E) = \pi_0(\mathbb{A}_E^{\times}/E^{\times}) \to \overline{\pi}_0\pi(G)$  of 4.2 can be described as follows. Let  $\mu_h: \mathbb{G}_m \to G_{\mathbb{C}}$  correspond to  $h \in X$ . The composite  $\mu_X = v \circ \mu_h$  is independent of h, and is therefore defined over E. We have therefore a map

$$\lambda = (\operatorname{Res}_{E/\mathbb{Q}} \mathbb{G}_m \xrightarrow{\operatorname{Res}(\mu_X)} \operatorname{Res}_{E/\mathbb{Q}} T \xrightarrow{N_{E/\mathbb{Q}}} T).$$

This gives a map  $\pi_0(\mathbb{A}_E^{\times}/E^{\times}) \to \pi_0(T(\mathbb{A})/T(\mathbb{Q}))$  that, when composed with  $\pi_0(T(\mathbb{A})/T(\mathbb{Q})) \to \pi_0(T(\mathbb{A})/T(\mathbb{Q}))/\nu(Z(\mathbb{R}))$ , equals  $\ell$ .

As Z is cohomologically trivial,  $G(\mathbb{Q}) \to G^{\mathrm{ad}}(\mathbb{Q})$  is surjective. Thus,

$$\frac{G(\mathbb{A}_f)}{Z(\mathbb{Q})^{\wedge}} *_{G(\mathbb{Q})_+/Z(\mathbb{Q})} G^{\mathrm{ad}}(\mathbb{Q})^+ = \frac{G(\mathbb{A}_f)}{Z(\mathbb{Q})^{\wedge}} = \frac{G(\mathbb{A})_+}{Z(\mathbb{Q})^{\wedge} \cdot G(\mathbb{R})_+}$$

There is a diagram

which, when the four left-most terms are divided by  $Z(\mathbb{Q})^{\wedge} \cdot G(\mathbb{R})^+$ , becomes the diagram in 4.2. By definition,

$$\mathcal{G}(G, X) = \{ g \in G(\mathbb{A})_+ \mid \nu(g) \in T^c \cdot \lambda(\mathbb{A}_E^{\times}) \cdot \nu(Z(\mathbb{R})) \}.$$

Note that, for any special  $h \in X$ , the map  $\eta$  of 4.5 defines a homomorphism  $\mathbb{A}_{E(h)}^{\times} \to \mathcal{G}(G, X)$ .

We can now identify  $\mathfrak{z}$  with the set of subgroups S of  $\mathcal{G}(G, X)$  such that  $Z(\mathbb{Q})^{\wedge}G(\mathbb{Q})_{+} \subset S$  and  $S/Z(\mathbb{Q})^{\wedge}G(\mathbb{R})^{+}$  is open and compact in  $\mathcal{G}(G, X)/Z(\mathbb{Q})^{\wedge}G(\mathbb{R})_{+} (= \mathcal{E}'(G, X))$ , and we can substitute  $\mathcal{G}(G, X)$  for  $\overline{\mathcal{E}}(G, X)$  in the statement of Theorem 4.6. From 4.6, 4.9, and 4.10 we can conclude the following statement.

THEOREM 4.13. There is a continuous homomorphism  $\tau: \mathcal{G}(G, X) \to \operatorname{Aut}(F'/E)$  with the following properties.

- (a) The kernel of  $\tau$  is  $Z(\mathbb{Q})^{\wedge} \cdot G(\mathbb{R})_+$ .
- (b) For all  $\alpha \in \mathcal{G}(G, X)$ ,  $\tau(\alpha)|_{\mathfrak{k}} = \sigma(\alpha)$ .
- (c) For  $\alpha \in G(\mathbb{Q})^{\wedge}_{+} \subset \mathcal{G}(G, X), f \in F'$ , and  $z \in M(G, X)^{\circ}$

$$\tau^{(\alpha)}f(z) = f(\alpha^{-1}z).$$

- (d) For all special  $z \in X^+$  and  $f \in F'$  defined at z,  $f(z) \in E(z)^{ab}$ ; if  $v \in \mathbb{A}_{E(h)}^{\times}$  and  $u = \eta(v)^{-1}$ , then  $\tau^{(u)}f$  is also defined at z, and  $\tau^{(u)}f(z) = [v]f(z)$ .
- (e) The map τ defines a topological isomorphism of G(G, X)/(Z(Q)<sup>∧</sup> · G(R)<sub>+</sub>) onto an open subgroup of Aut(F'/E). For every S ∈ 3, F' is an infinite Galois extension of k<sub>S</sub> and τ(S) = Gal(F'/k<sub>S</sub>).

4.14. In, in addition to the assumptions of 4.12, we suppose that the action of A on  $G^{ad}$  extends to an action on G, then we can extend  $\mathcal{G}(G, X)$  to a group  $\mathcal{G}^{e}(G, X)$  having  $\overline{\mathcal{E}^{e}}(G, X)$  as a quotient group. In this case, there is an exact sequence

$$1 \to Z(\mathbb{Q})^{\wedge} \cdot G(\mathbb{R})_+ \to \mathcal{G}^e(G, X) \to \operatorname{Aut}(F'/E) \to 1$$

of topological groups.

4.15. Unlike Deligne's connected canonical model, Shimura's canonical model depends on the pair (G, X) with G a reductive group and not merely the associated triple  $(G^{ad}, G^{der}, X^+)$ (because the field  $\mathfrak{k}$  depends on G; consider the example the case of a torus). It would perhaps be most natural to define the canonical model associated with a triple  $(G, G', X^+)$ to be a family  $(V_S, \varphi_S, J_{ST}(\alpha))$  in which S is an open compact subgroup of  $\mathcal{E}(G, G', X^+)$ ,  $\alpha \in \mathcal{E}(G, G', X^+)$ , and  $V_S = S \setminus M^{\circ}(G, G', X^+)$  is a model for  $\Gamma_S \setminus X^+$ , where  $\Gamma_S = S \cap G(\mathbb{Q})^+$ .

# 5 Non-abelian reciprocity laws and solutions to Hilbert's twelfth problem

5.1. Throughout this section, (G, X) satisfies the axioms for a Shimura variety and is of abelian type in the sense of Milne and Shih 1981, §1. We also assume that the weight w of any  $h \in X$  is defined over  $\mathbb{Q}$  and that adh(i) is a Cartan involution of  $(G/w(\mathbb{G}_m))_{\mathbb{R}}$  (see Deligne 1979, 2.1.1.4, 2.1.1.5). These conditions ensure that, for all special  $h \in X$ , the cocharacter  $\mu$  associated with h factors through the Serre group,

$$\mathbb{G}_m \xrightarrow{\mu_{\operatorname{can}}} S_{\mathbb{C}} \xrightarrow{\rho_{\mu}} G_{\mathbb{C}} \quad (\rho_{\mu} \ \mathbb{Q}\text{-rational}).$$

See Milne and Shih 1982a, §1.

5.2. Let *h* be a special element of *X*, and let  $T \subset G$  be a  $\mathbb{Q}$ -rational torus such that *h* factors through  $T_{\mathbb{R}}$ . Fix a field  $E \subset \overline{\mathbb{Q}}$  of finite degree over E(G, X), and let  $E'(h) = E(h) \cdot E$ . We define  $\eta'$  to be the composite

$$E'(h)^{\times} = \operatorname{Res}_{E'(h)/\mathbb{Q}}(\mathbb{G}_m) \xrightarrow{\operatorname{Res}(\mu)} \operatorname{Res}_{E'(h)/\mathbb{Q}}(T_{E(h)}) \xrightarrow{N_{E(h)/\mathbb{Q}}} T \hookrightarrow G$$

(so  $\eta' = \eta$  if E'(h) = E; see 4.5). Let  $W_{E'(h)/E}$  be the Weil group of E'(h) over E (see Tate 1979). There is an exact commutative diagram

For  $\alpha = (\alpha_{\infty}, \alpha_f) \in G(\mathbb{Q})$ , the element  $[\operatorname{ad} \alpha_{\infty} \circ h, \alpha_f] \in \operatorname{Sh}(G, X)$  depends only on the class of  $\alpha$  in  $G(\mathbb{Q}) \setminus G(\mathbb{A}) / C(\mathbb{R})$ , where *C* is the centralizer of *h* in  $G_{\mathbb{R}}$ . Let M(G, X) be a weakly canonical model for  $\operatorname{Sh}(G, X)$ , and identify  $\operatorname{Sh}(G, X)$  with  $M(G, X)_{\mathbb{C}}$ . Then, as [h, 1] is rational over  $E(h)^{\operatorname{ab}}, \sigma[h, 1]$  is well-defined for  $\sigma \in \operatorname{Hom}_E(E'(h)^{\operatorname{ab}}, \overline{\mathbb{Q}})$ .

THEOREM 5.3. There is a map  $\xi: W_{E'(h)/E} \to G(\mathbb{Q}) \setminus G(\mathbb{A})/C(\mathbb{R})$  with the following properties:

(a) for any  $v \in W_{E'(h)/E}$ ,

$$[ad(\xi(v)_{\infty}) \circ h, \xi(v)_f] = [v^{-1}][h, 1],$$

where [v] is the image of v in Hom<sub>*E*</sub> ( $E'(h)^{ab}, \overline{\mathbb{Q}}$ );

(b) the following diagram commutes,



(c) for all  $\nu \in W_{E'(h)/E}$  and  $\epsilon \in \pi_0(M(G, X)_{\overline{\mathbb{O}}})$ ,

$$\xi(v)_f \epsilon \equiv [v]\epsilon$$

in 
$$G(\mathbb{Q})\setminus \pi_0(M(G,X)_{\overline{\mathbb{Q}}})$$
.

PROOF. To construct  $\xi$  we shall need to use the motivic Galois group attached to the category of abelian varieties over  $\mathbb{Q}$  that are of potential CM-type (see Deligne and Milne 1982). This is an extension

$$1 \to S \to M \xrightarrow{\pi} \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to 1$$

of  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  by the Serre group *S* together with a splitting  $M(\mathbb{A}_f) \xleftarrow{sp} \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  over  $\mathbb{A}_f$ . For  $\tau \in \operatorname{Gal}(\overline{\mathbb{Q}}/E)$ , let  ${}^{\tau}S$  be the *S*-torsor  $\pi^{-1}(\tau)$  and let  ${}^{\tau}G$  be the *G*-torsor  ${}^{\tau}S \times {}^{S}G$ . According to Milne and Shih 1982b, 7.2, §10,  ${}^{\tau}G$  is trivial. Choose an  $a(\tau) \in {}^{\tau}S(\overline{\mathbb{Q}})$  and  $c(\tau) \in {}^{\tau}G(\mathbb{Q})$  and set

$$\rho(a(\tau)) = c(\tau)\nu, \quad \nu \in G(\mathbb{Q}),$$
  
$$\rho(sp(\tau)) = c(\tau)\alpha, \quad \alpha \in G(\mathbb{A}_f)$$

with  $\rho = \rho_{\mu}$  as in 5.1. Let  $\omega_{\tau} \in G(\mathbb{C})$  normalize  $T(\mathbb{C})$  and be such that  $\mathrm{ad} \omega_{\tau} \circ \mu = \tau \mu$ . Then  $\nu \omega_{\tau} \in G(\mathbb{R})$  (ibid., 7.7, §10) and  $\tau[h, 1] = [\mathrm{ad}(\nu \omega_{\tau}) \circ h, \alpha]$  (ibid., 7.11, §10). For  $\nu \in W_{E'(h)/E}$ , we choose a  $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/E)$  whose restriction to  $E'(h)^{\mathrm{ab}}$  is  $[\nu^{-1}]$ , and we set  $\xi(\nu)$  equal to the class of  $(\nu \omega_{\tau}, \alpha)$  in  $G(\mathbb{Q}) \setminus G(\mathbb{A}) / C(\mathbb{R})$ . Obviously  $\xi(\nu)$  is well-defined, and  $[\nu^{-1}][h, 1] = [\mathrm{ad}\xi(\nu)_{\infty}) \circ h, \xi(\nu)_f]$ .

Let  $\nu \in \mathbb{A}_{E(h)}^{\times}$  and identify  $\tau = [\nu^{-1}]$  with an element of  $\operatorname{Gal}(E'(h)^{ab}/E'(h))$ . Then  $\tau \mu = \mu$  because  $E(h) \subset E'(h)$  is the field of definition of  $\mu$ , and we can take  $\omega_{\tau} = 1$ . According to Milne and Shih 1982a, 3.10,  $\tau S$  is trivial, so that we can take  $a(\tau) \in \tau S(\mathbb{Q})$  and  $c(\tau) \in \rho(a(\tau))$ . Moreover,  $\alpha = \eta'(\nu_f)$ , and so  $\xi(\nu) \stackrel{\text{def}}{=} (1, \eta'(\nu_f)) \equiv (\eta'(\nu_{\infty}), \eta'(\nu_f))$  because  $\eta'(\nu_{\infty}) \in C(\mathbb{R})$ .

As  $G(\mathbb{A}_f)$  acts transitively on  $\pi_0(M(G, X)_{\overline{\mathbb{Q}}})$  and its action factors through an abelian quotient and commutes with the action of  $\operatorname{Gal}(\overline{\mathbb{Q}}/E)$ , it suffices to check (c) for a single  $\epsilon \in \pi_0(M(G, X)_{\overline{\mathbb{Q}}})$ . But if we take  $\epsilon$  to be the class of [h, 1], then the formula follows from (a).

5.4. Let  $\tilde{\xi}(v) \in G(\mathbb{A})$  represent  $\xi(v)$ . The real approximation theorem allows us to assume that  $\tilde{\xi}(v)_{\infty} \in G(\mathbb{R})_+$ . Part (c) of the theorem can be strengthened to read:  $\tilde{\xi}(v)_f \epsilon = [v]\epsilon$ . From this it follows that  $\overline{\xi}(v)_f \stackrel{\text{def}}{=} \tilde{\xi}(v)_f * 1 \in G(\mathbb{A}_f)/Z(\mathbb{Q})^{\wedge} * \cdots$  lies in  $\overline{\mathcal{E}}(G, X)$ , and that  $\sigma(\overline{\xi}(v)_f) = [v]|_{\mathfrak{k}}$ .

COROLLARY 5.5. Part (c) of Theorem 4.6 can be replaced by the following: let  $h \in X^+$  be special; for each  $S \in \mathfrak{z}, \varphi_S(h)$  is rational over  $E(h)^{ab}$ , and for every  $\nu \in W_{k_S}E(h)/k_S$ ,

$$[\nu]\varphi_S(\mathrm{ad}\,\widetilde{\xi}(\nu)_{\infty}\circ h) = J_{ST}(\overline{\xi}(\nu)_f)(\varphi_T(h)),$$

where  $T = \overline{\xi}(v)_f^{-1}S\overline{\xi}(v)_f$  and  $\widetilde{\xi}(v)_{\infty}$  and  $\overline{\xi}(v)_f$  correspond to some lifting  $\widetilde{\xi}(v)$  of  $\xi(v)$  with  $\widetilde{\xi}(v)_{\infty} \in G(\mathbb{R})_+$ .

PROOF. We have  $\overline{\xi}(\nu)_f[h,1] \stackrel{\text{def}}{=} \sigma(\overline{\xi}(\nu)_f)[h,\overline{\xi}(\nu)_f^{-1}]$ , and  $\sigma(\overline{\xi}(\nu)_f) = [\nu]$  and  $[\nu][h,1] = ad\xi(\nu)_{\infty} \circ h, \xi(\nu)_f]$ . Thus  $\overline{\xi}(\nu)_f^{-1}[ad\xi(\nu)_{\infty} \circ h, 1] = [h,1]$  and so

$$J(\overline{\xi}(\nu)_f)[h,1] = [\nu][\mathrm{ad}\,\xi(\nu)_{\infty} \circ h,1],$$

which implies the formula.

COROLLARY 5.6. Let  $z \in X^+$  be special and let  $f \in F'$  be defined at z; then, for any  $\nu \in W_{E(h)/E}$ ,  ${}^{u}f$ , where  $u = \overline{\xi}(\nu)_{f}^{-1}$ , is defined at z and

$${}^{\mu}f(z) = [\nu]f(\mathrm{ad}\,\widetilde{\xi}(\nu)_{\infty}\circ z).$$

PROOF. We have

$${}^{u}f(z) = [v] \circ f \circ \overline{\xi}(v)_{f}(z) = [v] f(\mathrm{ad}\,\widetilde{\xi}(v)_{\infty} \circ z)$$

because  $\overline{\xi}(\nu)_f[z,1] = [\operatorname{ad} \widetilde{\xi}(\nu)_{\infty} \circ z, 1]$  (see the above proof).

5.7. The last corollary can be regarded as a non-abelian solution to Hilbert's twelfth problem: it describes the action of the Weil group on the special values of certain functions and therefore determines the fields they generate; this field is an abelian extension of a finite extension of the base field.

5.8. We shall prove a non-abelian version of the reciprocity law stated in Deligne 1979, 2.7.10c. Let  $h \in X$  be special and let  $\rho = \rho_{\mu}$  be the map  $S \to G$  associated with h as in 5.1. Let  $_EM$  be the pullback of the motivic Galois group relative to  $\text{Gal}(\overline{\mathbb{Q}}/E) \hookrightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . Then we have an extension

$$1 \to S \longrightarrow {}_{E}M \xrightarrow{\pi} \operatorname{Gal}(\overline{\mathbb{Q}}/E) \to 1$$

together with a splitting  ${}_{E}M(\mathbb{A}_{f}) \xleftarrow{sp} \operatorname{Gal}(\overline{\mathbb{Q}}/E)$ . Write M for  ${}_{E}M$  and let S act on  $M \times G$ by  $s(m,g) = (ms^{-1}, \rho(s)g)$  and define MG to be the quotient scheme  $S \setminus M \times G$ . The splitting sp allows us to define a map  $MG(\mathbb{A}^{f}) \to G(\mathbb{A}^{f}) \times \operatorname{Gal}(\mathbb{Q}/E)$ : we send [m,g]to  $(\rho(sp(\tau)^{-1}m)g, \tau)$ , where  $\tau$  is the image of m in  $\operatorname{Gal}(\overline{\mathbb{Q}}/E)$ . If  $q \in MG(\mathbb{Q})$  maps to  $(\alpha, \tau) \in G(\mathbb{A}_{f}) \times \operatorname{Gal}(\overline{\mathbb{Q}}/E)$ , we define  $q[h, 1] = \tau[h, \alpha]$ .

PROPOSITION 5.9. Let  $h \in X$  be special, and let  $q = [m, g] \in MG(\mathbb{Q})$ . If  $\tau$  is the image of *m* in Gal( $\overline{\mathbb{Q}}/E$ ), then  ${}^{q}h \stackrel{\text{def}}{=} \operatorname{ad} g^{-1} \circ {}^{\tau}h$  is in *X*, and  $q[h, 1] = [{}^{q}h, 1]$ .

PROOF. Let L be some large finite Galois extension of  $\mathbb{Q}$  containing E(h). Using that the motivic Galois group, and therefore  $_E M$ , is a pro-system, we have an extension

$$1 \to S^L \to {}_E M^L \to \operatorname{Gal}(L^{\operatorname{ab}}/E) \to 1$$

with a splitting  ${}_{E}M^{L}(\mathbb{A}_{f}) \xleftarrow{sp} \operatorname{Gal}(L^{ab}/E)$ , see Milne and Shih 1982a, §2. Replace  ${}_{E}M$ in the above discussion by its quotient  ${}_{E}M^{L}$ . Choose a section  $\tau \mapsto a(\tau)$  to  ${}_{E}M^{L}(L) \to$  $\operatorname{Gal}(L^{ab}/E)$  that is a morphism of pro-algebraic schemes. After possibly multiplying gby an element of  $S^{L}(L)$ , we can assume  $q = [a(\tau), g]$ . Let  $\sigma(a(\tau)) = a(\tau)\gamma_{\sigma}(\tau)$  with  $\gamma_{\sigma}(\tau) \in S^{L}(L)$ ; since  $\sigma g = [\sigma a(\tau), \sigma g] = q$ , we have  $\sigma g = \rho(\gamma_{\sigma}(\tau))g$ . The formula of Milne and Shih 1982b, 7.13, §10, states that  $\tau[h, 1] = [ad \nu \circ^{\tau} h, \nu\rho(sp(\tau)^{-1}a(\tau))^{-1}]$ , where  $\nu$  is any element of G(L) such that  $\sigma \nu = \nu\rho(\gamma_{\sigma}(\tau))$ . Clearly,  $g^{-1}$  is such an element, and so  $\tau[h, 1] = [{}^{q}h, g^{-1}\rho(sp(\tau)^{-1}a(\tau))^{-1}]$ . On multiplying on the right with  $\rho(sp(\tau)^{-1}a(\tau))g$ , we obtain the formula  $q[h, 1] = [{}^{q}h, 1]$ .

5.10. If we knew the conjecture of Langlands (1979, pp. 232–33) (equivalently, conjecture CM or D of Milne and Shih 1982b), it would be possible to replace the motivic Galois group by the Taniyama group. The above results would then be more explicit.<sup>4</sup>

5.11. Let N be the normalizer of T in G. It would be interesting to know under what conditions every element  $\xi(v)$  is representated by an element of  $N(\mathbb{A})$  and further that there exists a commutative diagram



with  $N' \subset N(\mathbb{A})$ . The existence of such a diagram would provide a partial answer to the problem mentioned in Tate 1967, p. 200.<sup>5</sup>

#### THE UNIVERSITY OF MICHIGAN

 $<sup>^4</sup>$ 27.03.23. We do know the conjecture, see the article in footnote 2.

<sup>&</sup>lt;sup>5</sup>The kernel of the map [from the Weil group  $\mathcal{E}$  of L/K to  $\operatorname{Gal}(L^{ab}/K)$ ] is the connected component  $D_L$  of  $C_L$ . As Weil remarks, the search for a Galois-like interpretation of  $\mathcal{E}$  (or even a "natural" construction, without recourse to factor systems, of a group  $\mathcal{E}$  furnished with a "natural" map  $W: \mathcal{E} \to \operatorname{Gal}(L^{ab}/K)$  seems to be one of the fundamental problems of number theory.

#### References

- BAILY, JR., W. L. AND BOREL, A. 1966. Compactification of arithmetic quotients of bounded symmetric domains. *Ann. of Math.* (2) 84:442–528.
- BOREL, A. 1966. Density and maximality of arithmetic subgroups. J. Reine Angew. Math. 224:78-89.
- BOREL, A. 1969. Introduction aux groupes arithmétiques. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris.
- BOREL, A. 1972. Some metric properties of arithmetic quotients of symmetric spaces and an extension theorem. J. Differential Geometry 6:543–560.
- DELIGNE, P. 1971. Travaux de Shimura, pp. Exp. No. 389, pp. 123–165. *In* Séminaire Bourbaki, 23ème année (1970/1971), Lecture Notes in Math., Vol. 244. Springer, Berlin.
- 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. Amer. Math. Soc., Providence, R.I.
- DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. *In* Hodge cycles, motives, and Shimura varieties, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York.
- KNESER, M. 1969. Lectures on Galois cohomology of classical groups. Tata Institute of Fundamental Research Lectures on Mathematics, No. 47. Tata Institute of Fundamental Research, Bombay. With an appendix by T. A. Springer, Notes by P. Jothilingam.
- LANGLANDS, R. P. 1979. Automorphic representations, Shimura varieties, and motives. Ein Märchen. 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. 205–246. Amer. Math. Soc., Providence, R.I.
- MILNE, J. AND SHIH, K.-Y. 1981. The action of complex conjugation on a Shimura variety. Ann. of Math. (2) 113:569–599.
- MILNE, J. AND SHIH, K.-Y. 1982a. Langlands's construction of the Taniyama group, pp. 229–260. In Hodge cycles, motives, and Shimura varieties, volume 900 of Lecture Notes in Mathematics. Springer-Verlag, Berlin-New York.
- MILNE, J. S. AND SHIH, K.-Y. 1982b. Conjugates of Shimura varieties, pp. 280–356. In Hodge cycles, motives, and Shimura varieties, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York.
- MIYAKE, K. 1971. Models of certain automorphic function fields. Acta Math. 126:245-307.
- MIYAKE, T. 1972. On automorphism groups of the fields of automorphic functions. *Ann. of Math.* (2) 95:243–252.
- SHAFAREVICH, I. R. 1994. Basic algebraic geometry. 2. Springer-Verlag, Berlin, second edition. Schemes and complex manifolds, Translated from the 1988 Russian edition by Miles Reid.
- SHIH, K.-Y. 1979. Construction of arithmetic automorphic functions for special Clifford groups. *Nagoya Math. J.* 76:153–171.

- SHIMURA, G. 1970. On canonical models of arithmetic quotients of bounded symmetric domains I,II. Ann. of Math. (2) pp. 91, 144–222; 92 528–549.
- SHIMURA, G. 1971a. Introduction to the arithmetic theory of automorphic functions. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo.
- SHIMURA, G. 1971b. On arithmetic automorphic functions, pp. 343–348. *In* Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 2. Gauthier-Villars, Paris.
- SHIMURA, G. 1975. On some arithmetic properties of modular forms of one and several variables. *Ann. of Math.* (2) 102:491–515.
- TATE, J. T. 1967. Global class field theory. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pp. 162–203. Thompson, Washington, D.C.
- TATE, J. T. 1979. Number theoretic background. 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. 3–26. Amer. Math. Soc., Providence, R.I.
- WEIL, A. 1960. Algebras with involutions and the classical groups. J. Indian Math. Soc. (N.S.) 24:589–623.