

## POINTS ON SOME SHIMURA VARIETIES OVER FINITE FIELDS

ROBERT E. KOTTWITZ

The Hasse-Weil zeta functions of varieties over number fields are conjecturally products (and quotients) of automorphic  $L$ -functions. For a Shimura variety  $S$  associated to a connected reductive group  $G$  over  $\mathbb{Q}$  one can hope to be more specific about which automorphic  $L$ -functions appear in the zeta function. In fact Eichler, Shimura, Kuga, Sato, and Ihara, who studied  $GL_2$  and its inner forms, found in those cases that it was enough to use automorphic  $L$ -functions for the group  $G$  itself. In the general case Langlands [L2–L4] has given a conjectural description of the zeta function in terms of automorphic  $L$ -functions for  $G$  and its endoscopic groups [L5] (see also [K5] for the contribution of non-tempered representations), and a description of this type has been verified in certain cases, beginning with [L3].

For  $GL_2$  it was possible to use the Eichler-Shimura congruence relation in order to make the connection between the zeta function and automorphic  $L$ -functions. In general one needs more information than the Eichler-Shimura congruence relation gives, and it seems to be necessary to describe the points on  $S$  over finite fields in terms of group-theoretical data (for the group  $G$ ), in a way that is adapted to an eventual comparison of the number of points modulo  $p$  with the Selberg trace formula for  $G$  (actually with the stable trace formulas for  $G$  and its endoscopic groups), as is explained in [L2, L3, K5]. Ihara [I1, I2] gave such a group-theoretical description of points modulo  $p$  in the case of  $GL_2(\mathbb{Q})$  and its inner forms, and Deligne [D1] gave a related description of the category of ordinary abelian varieties over a finite field.

Langlands [L1] conjectured a group-theoretical description in the general case, based on a detailed though incomplete study of Shimura varieties of PEL type [S]; Milne [Mi1] gave a simplified exposition of this work of Langlands in a special case, using the description of the category of abelian varieties up to isogeny over a finite field due to Honda [H] and Tate [T2, T3]. Zink [Z2] gave complete proofs for part of Langlands's conjectures for Shimura varieties of PEL type, but by that time it was clear that a new idea was needed to give a complete proof for the full conjecture, even for the case of the group of symplectic similitudes. In fact the conjecture itself needed some refinement; this was one of the objects of some work by Langlands-Rapoport [LR], whose main goal, however, was to put the conjecture into a Tannakian framework, in which it became conceptually clearer. The final step was taken independently by

---

Received by the editors July 9, 1991.

1991 *Mathematics Subject Classification*. Primary 11G18.

Partially supported by NSF Grant DMS-8913971.

©1992 American Mathematical Society  
0894-0347/92 \$1.00 + \$.25 per page

Reimann-Zink [RZ1] and myself, the main result of [RZ1] being a stronger form of Lemma 13.1 of this paper (except that Reimann-Zink exclude the prime 2). At this point Langlands's conjecture had essentially been proved for Shimura varieties of PEL type in Cases A and C (see the explanation of Cases A and C below); it just remained to write out all the details. For the group of symplectic similitudes this was done in [K5] and again in [Mi2], from a slightly different point of view. The general case is treated in this paper, which is written in the same spirit as [Mi1] in that it relies heavily on Honda-Tate theory. Recently Reimann-Zink [RZ2] have treated some Shimura varieties for  $G = D^\times$ , with  $D$  a quaternion algebra over a totally real number field  $F$ ; these are not of PEL type but are related to ones that are.

Now we begin to give a precise formulation of the main result of this paper. Let  $p$  be a prime number and write  $\mathbb{Z}_{(p)}$  for the localization of  $\mathbb{Z}$  at the prime ideal generated by  $p$ . Let  $B$  be a finite-dimensional simple  $\mathbb{Q}$ -algebra with center  $F$ , let  $\mathcal{O}_B$  be a  $\mathbb{Z}_{(p)}$ -order in  $B$ , and let  $*$  be a positive involution on  $B$  that preserves  $\mathcal{O}_B$ . Let  $V$  be a nondegenerate skew-Hermitian  $B$ -module (a finitely generated left  $B$ -module together with a nondegenerate  $\mathbb{Q}$ -valued alternating form  $(\cdot, \cdot)$  such that  $(bv, w) = (v, b^*w)$  for all  $v, w \in V$  and all  $b \in B$ ). Let  $G$  be the group of automorphisms of the skew-Hermitian  $B$ -module  $V$ . In fact  $G$  is a group of similitudes since in this paper an automorphism or isomorphism of skew-Hermitian  $B$ -modules is only required to preserve the alternating form up to an invertible element of the ground ring, which is  $\mathbb{Q}$  at the moment. We impose conditions on  $B, \mathcal{O}_B, V$  (see §5 for details) that ensure that the group  $G_{\mathbb{Q}_p}$  is unramified. Let  $K^p$  be a compact open subgroup of  $G(\mathbb{A}_f^p)$ , and let  $h : \mathbb{C} \rightarrow \text{End}_B(V_{\mathbb{R}})$  be an  $\mathbb{R}$ -algebra homomorphism such that  $h(\bar{z}) = h(z)^*$  and the symmetric bilinear form  $(v, h(i)w)$  on  $V_{\mathbb{R}}$  is positive definite, where we have written  $*$  for the involution on  $\text{End}_B(V)$  obtained from the alternating form on  $V$ .

The homomorphism  $h$  determines a decomposition  $V_{\mathbb{C}} = V_1 \oplus V_2$ , where  $V_1$  (respectively,  $V_2$ ) is the subspace of  $V_{\mathbb{C}}$  on which  $h(z)$  acts by  $z$  (respectively, by  $\bar{z}$ ). The field of definition of the isomorphism class of the complex representation  $V_1$  of  $B$  is a number field  $E$ , whose ring of integers we denote by  $\mathcal{O}_E$ .

We consider the following moduli problem over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ . For a locally noetherian scheme  $S$  over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  the  $S$ -valued points on the moduli problem are the isomorphism classes of quadruples  $(A, \lambda, i, \bar{\eta})$  of the following type:  $A \rightarrow S$  is a projective abelian scheme over  $S$  up to prime-to- $p$  isogeny,  $\lambda : A \rightarrow \widehat{A}$  is a polarization of  $A$  (a prime-to- $p$  isogeny from  $A$  to its dual abelian scheme  $\widehat{A}$ , which at every geometric point  $s$  of  $S$  is a polarization of  $A_s$ ),  $i : \mathcal{O}_B \rightarrow \text{End}(A)$  is a  $*$ -homomorphism for  $*$  on  $\mathcal{O}_B$  and the Rosati involution on  $\text{End}(A)$  obtained from  $\lambda$ , and  $\bar{\eta}$  is a level structure (see §5) of type  $K^p$  on  $A$ . Moreover we require that  $(A, \lambda, i, \bar{\eta})$  satisfy the “determinant condition” (see §5), which depends on  $h$  and is the reason the moduli problem must be formulated over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  rather than  $\mathbb{Z}_{(p)}$ .

Over an algebraic closure of  $F$  the  $F$ -algebra  $\text{End}_B(V)$  with involution is

of one of the three following types:

- (1)  $\mathbf{M}_n \times \mathbf{M}_n^{\text{opp}}$  with  $(x, y)^* = (y, x)$ ,
- (2)  $\mathbf{M}_{2n}$  with  $x^*$  equal to the adjoint of  $x$  for a nondegenerate alternating form in  $2n$  variables,
- (3)  $\mathbf{M}_{2n}$  with  $x^*$  equal to the adjoint of  $x$  for a nondegenerate symmetric bilinear form in  $2n$  variables.

We refer to these as Cases A, C, D respectively, since the corresponding isometry groups  $\{x | xx^* = 1\}$  are of types  $A_{n-1}, C_n, D_n$  respectively.

From now on in this introduction we exclude Case D and assume that  $K^p$  is sufficiently small. Then our moduli problem is representable by a smooth quasi-projective scheme  $S_{K^p}$  over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ . If  $\text{End}_B(V)$  is a division algebra, then  $S_{K^p}$  is projective over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ . The group  $G(\mathbb{A}_f^p)$  acts on the right of the projective system  $S_{K^p}$  (vary  $K^p$ ). The variety over  $E$  obtained from  $S_{K^p}$  is a disjoint union of  $|\ker^1(\mathbb{Q}, G)|$  copies of the canonical model for the Shimura variety associated to  $(G, h^{-1}, K^p)$ , where  $h$  now denotes the restriction of  $h: \mathbb{C} \rightarrow \text{End}_B(V_{\mathbb{R}})$  to  $\mathbb{C}^\times$ , viewed as a homomorphism  $h: \mathbb{C}^\times \rightarrow G_{\mathbb{R}}$  of algebraic groups over  $\mathbb{R}$ .

Let  $\xi$  be a finite-dimensional representation of  $G$  on a vector space over a number field  $L$ , and let  $\lambda$  be a place of  $L$  lying over a prime  $l$  different from  $p$ . Then  $\xi$  gives rise to a smooth  $\lambda$ -adic sheaf  $\mathcal{F}_{K^p}$  on  $S_{K^p}$  and the group  $G(\mathbb{A}_f^p)$  acts naturally on the system of sheaves  $\mathcal{F}_{K^p}$  over the projective system of spaces  $S_{K^p}$ .

Let  $g \in G(\mathbb{A}_f^p)$  and put  $K_g^p := K^p \cap gK^pg^{-1}$ . Then we get a Hecke correspondence  $f$  from  $S_{K^p}$  to itself by taking

$$S_{K^p} \xleftarrow{a} S_{K_g^p} \xrightarrow{b} S_{K^p},$$

where  $a$  is induced by  $g$  and  $b$  is the covering map for the inclusion of  $K_g^p$  in  $K^p$ . The Hecke correspondence extends naturally to  $\mathcal{F}_{K^p}$ .

Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_E$  lying over  $p$ , let  $k$  denote the residue field at  $\mathfrak{p}$ , and let  $\bar{k}$  be an algebraic closure of  $k$ . Suppose that  $S_{K^p}$  is proper over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ , and abbreviate  $S_{K^p}$  and  $\mathcal{F}_{K^p}$  to  $S$  and  $\mathcal{F}$ . We are interested in the commuting representations of  $\text{Gal}(\bar{E}_{\mathfrak{p}}/E_{\mathfrak{p}})$  and  $\mathcal{H}$  on  $H^\bullet(S_{\bar{E}}, \mathcal{F})$ , where  $\mathcal{H}$  denotes the Hecke algebra of compactly supported  $L$ -valued functions on  $G(\mathbb{A}_f^p)$ , bi-invariant under  $K^p$ , and  $H^\bullet$  indicates that we consider the Euler characteristic. Since  $S$  is proper and smooth over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  and  $\mathcal{F}$  is a smooth  $\lambda$ -adic sheaf, the representations  $H^i(S_{\bar{E}}, \mathcal{F})$  are unramified and equal to  $H^i(S_{\bar{k}}, \mathcal{F})$ . Therefore it is enough to calculate the trace of  $\Phi_{\mathfrak{p}}^j \circ f$  on  $H^\bullet(S_{\bar{k}}, \mathcal{F})$  for all positive integers  $j$ , where  $f$  is our Hecke correspondence and  $\Phi_{\mathfrak{p}}$  is the Frobenius morphism from  $S_{\bar{k}}$  to itself.

By the Lefschetz formula this trace is a sum over the fixed points  $x' \in S'(\bar{k})$  of the trace of the endomorphism induced by the correspondence on the stalk of  $\mathcal{F}$  at the point  $x \in S(\bar{k})$  that is the common image of  $x'$  under the two

maps  $a$  and  $c := \Phi_p^j \circ b$  that make up our correspondence  $\Phi_p^j \circ f$ ; we have written  $S'$  for  $S_{K_g^p}$  in order to simplify notation. In fact even when  $S_{K_g^p}$  is not proper over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  we still want to consider the same sum, although it will be only a part of the full story. The main result of the paper is the expression (19.5) for this sum, which is denoted by  $T(j, f)$  in §19,

$$|\ker^1(\mathbb{Q}, G)| \sum_{(\gamma_0; \gamma, \delta)} c(\gamma_0; \gamma, \delta) O_\gamma(f^p) T O_\delta(\phi_r) \operatorname{tr} \xi(\gamma_0).$$

The number  $\operatorname{tr} \xi(\gamma_0)$  gives the trace of our correspondence on the stalk  $\mathcal{F}_x$  (see the end of §16), so that what we must show is that

$$|\ker^1(\mathbb{Q}, G)| \sum_{(\gamma_0; \gamma, \delta)} c(\gamma_0; \gamma, \delta) O_\gamma(f^p) T O_\delta(\phi_r)$$

is the number of fixed points of  $\Phi_p^j \circ f$  in  $S'(\bar{k})$ .

Let  $\sigma$  be the Frobenius automorphism  $x \mapsto x^p$  of  $\bar{k}$ , let  $r = j[k : \mathbb{F}_p]$  and write  $k_r$  for the fixed field of  $\sigma^r$  on  $\bar{k}$ , so that  $k_r$  is a field with  $p^r$  elements. If the Hecke operator  $f$  is trivial (in other words  $g = 1$ ), then a fixed point of our correspondence is simply a  $k_r$ -valued point of  $S$ . The general case is similar: if a  $\bar{k}$ -point  $(\bar{A}, \lambda, i, \bar{\eta})$  of  $S'$  is a fixed point, then there exists a prime-to- $p$  isogeny  $u : \sigma'(\bar{A}) \rightarrow \bar{A}$ , commuting with the action of  $\mathcal{O}_B$ , carrying  $\sigma'(\bar{\eta})$  into  $\bar{\eta} \bar{g}$ , and carrying  $\sigma'(\lambda)$  into a scalar multiple of  $\lambda$ ; moreover  $u$  is unique since  $K^p$  is sufficiently small. Giving a prime-to- $p$  isogeny  $u : \sigma'(\bar{A}) \rightarrow \bar{A}$  is analogous to giving a  $k_r$ -structure on  $\bar{A}$ , and, in fact, we call such a pair  $(\bar{A}, u)$  a virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny.

In §10 we develop the theory of virtual abelian varieties  $A = (\bar{A}, u)$  over  $k_r$  up to isogeny. As usual there is a Frobenius endomorphism  $\pi_A \in \operatorname{End}(A)$  and  $\operatorname{End}(A)$  is the centralizer of  $\pi_A$  in  $\operatorname{End}(\bar{A})$ . Let  $c$  be a rational number. We say that a polarization  $\lambda$  of  $\bar{A}$  is a  $c$ -polarization of  $A$  if  $\pi_A \pi_A^* = c$ , where  $*$  denotes the Rosati involution for  $\lambda$  on  $\operatorname{End}(\bar{A})_{\mathbb{Q}}$ ; if  $A$  is  $c$ -polarizable then  $c$  must be positive and of the form  $p' c_0$  for a  $p$ -adic unit  $c_0$ . All of Honda-Tate theory goes through for  $c$ -polarizable virtual abelian varieties over  $k_r$  up to isogeny (see §10), the role of Weil  $q$ -numbers being played by  $c$ -numbers, by which we mean algebraic numbers  $\alpha \in \bar{\mathbb{Q}}$  such that the image of  $\alpha$  under any embedding  $\bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}_p$  lies in the valuation ring of  $\bar{\mathbb{Q}}_p$  and the image of  $\alpha$  under any embedding  $\bar{\mathbb{Q}} \rightarrow \mathbb{C}$  has absolute value  $c^{1/2}$ .

Our fixed point  $(\bar{A}, \lambda, i, \bar{\eta})$  gives us a  $c$ -polarized virtual abelian variety  $A$  over  $k_r$  up to prime-to- $p$  isogeny, together with a level structure and an action of  $\mathcal{O}_B$  compatible with the polarization. We can forget the level structure and consider isogeny classes rather than prime-to- $p$  isogeny classes; in this way our problem divides into two parts: counting the fixed points isogenous to a given one and describing the isogeny classes of  $c$ -polarized virtual  $B$ -abelian varieties over  $k_r$ .

In both parts a key role is played by the construction (see §14) of a triple  $(\gamma_0; \gamma, \delta)$  from a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  up to isogeny.

The element  $\gamma_0$  is a semisimple element of  $G(\mathbb{Q})$ , elliptic in  $G(\mathbb{R})$ , well defined up to conjugacy in  $G(\mathbb{Q})$ ; the element  $\gamma$  is an element of  $G(\mathbb{A}_f^p)$ , well defined up to conjugacy; and  $\delta$  is an element of  $G(L_r)$ , well defined up to twisted conjugacy, where  $L_r$  is the fraction field of the Witt ring of  $k_r$ . The element  $\gamma$  is easy to define: pick an isomorphism  $V_{\mathbb{A}_f^p} \simeq H_1(\bar{A}, \mathbb{A}_f^p)$  of skew-Hermitian  $B$ -modules and use it to transport  $\pi_A^{-1}$  over to an automorphism  $\gamma$  of  $V_{\mathbb{A}_f^p}$ . The element  $\delta$  arises from an analogous  $p$ -adic construction. The  $G(\mathbb{Q})$ -conjugacy class of  $\gamma_0$  is determined uniquely by the requirement that  $\gamma_0$  be conjugate in  $G(\mathbb{Q}_l)$  to the  $l$ -adic component of  $\gamma$  for all primes  $l$  different from  $p$ .

Fix a  $c$ -polarized virtual  $B$ -abelian variety  $(A_0, \lambda_0, i_0)$  over  $k_r$  up to isogeny, and assume that this triple satisfies three assumptions imposed in §14. Then the number of fixed points that are isogenous to  $(A_0, \lambda_0, i_0)$  is equal to

$$\text{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f)) O_\gamma(f^p) T O_\delta(\phi_r).$$

Here  $O_\gamma(f^p)$  denotes the orbital integral of a certain function  $f^p$  on  $G(\mathbb{A}_f^p)$  over the conjugacy class of  $\gamma$ , and  $T O_\delta(\phi_r)$  denotes the twisted orbital integral of a certain function  $\phi_r$  on  $G(L_r)$  over the twisted conjugacy class of  $\delta$ ; the group  $I$  is a certain inner form of the centralizer  $I_0$  of  $\gamma_0$  in  $G$ . The formula above (see §16 for its derivation) just reflects the fact that giving an object  $(A, \lambda, i, \eta)$  plus an isogeny to  $(A_0, \lambda_0, i_0)$  is the same as giving a pair of lattices, one in  $H_1(\bar{A}_0, \mathbb{A}_f^p)$  and the other in the isocrystal associated to  $A_0$  in §10 (the lattices must satisfy certain requirements, of course); the functions  $f^p$  and  $\phi_r$  are such that their orbital integrals count such lattices.

It remains to describe the isogeny classes  $(A, \lambda, i)$ . For this we again use the map  $(A, \lambda, i) \mapsto (\gamma_0; \gamma, \delta)$ . Two triples  $(A, \lambda, i), (A', \lambda', i')$  give rise to the same  $(\gamma_0; \gamma, \delta)$  (the same up to equivalence, that is) if and only if  $(A, \lambda, i)$  and  $(A', \lambda', i')$  differ by an element of  $\ker^1(\mathbb{Q}, I)$ , where  $I$  denotes the group of automorphisms of  $(A, \lambda, i)$  (see §17). Therefore  $|\ker^1(\mathbb{Q}, I)|$  (which is also equal to  $|\ker^1(\mathbb{Q}, I_0)|$ ) gives the number of triples  $(A', \lambda', i')$  for which  $(\gamma_0; \gamma, \delta)$  is the same as it is for  $(A, \lambda, i)$ .

The final point is to determine the image of the map  $(A, \lambda, i) \mapsto (\gamma_0; \gamma, \delta)$ ; this is done in Lemma 18.1. Suppose that  $(\gamma_0; \gamma, \delta)$  comes from some  $(A, \lambda, i)$ . It is then immediate that conditions (1) and (3) of Lemma 18.1 hold; however, it is much harder to see that (2) holds. Condition (2) states that a certain invariant  $\alpha(\gamma_0; \gamma, \delta)$  attached to  $(\gamma_0; \gamma, \delta)$  vanishes. This vanishing is proved in §15, which in turn relies on §§12 and 13. Conversely, suppose that  $(\gamma_0; \gamma, \delta)$  satisfies the three conditions of Lemma 18.1. Then one uses the analog of Honda-Tate theory developed in §10 to see that  $(\gamma_0; \gamma, \delta)$  comes from some  $(A, \lambda, i)$ .

Putting all this together, one finally arrives at the formula (19.5), in which  $c(\gamma_0; \gamma, \delta)$  denotes the product of  $\text{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f^p))$  and

$$|\ker[\ker^1(\mathbb{Q}, I_0) \rightarrow \ker^1(\mathbb{Q}, G)]|.$$

The factor  $|\ker^1(\mathbb{Q}, G)|$  in (19.5) disappears when we replace  $S_{K^p}$  by the

canonical model for the Shimura variety associated to  $(G, h^{-1}, K^p)$  since  $S_{K^p}$  is a disjoint union of  $|\ker^1(\mathbb{Q}, G)|$  copies of this canonical model. As is explained in §19, the formula (19.6) agrees with the formula (3.1) of [K5], except for the following mistake in [K5]: the formula (3.1) of [K5] is not valid for  $(G, h, K)$ , as stated in [K5], but rather for  $(G, h^{-1}, K)$ .

The main lines of the argument leading to (19.5) are given in §§14–19, and the reader may want to start with §§5 and 6, which establish notation, and then skip directly to §14. There are important auxiliary results in §§9–13, especially in §§10, 12, 13; these will have to be read along with §§14–19. The remaining sections give various lemmas, most of which are more-or-less well known, but that may help to make the paper more readable; they should be consulted only as needed.

The paper is self-contained with a few notable exceptions. The reader should be familiar with §§2 and 3 of [K5], which it seemed pointless to rewrite, and with the results concerning Galois cohomology in [K2–K4] (our notational conventions concerning Galois cohomology and Langlands dual groups are taken from these papers). Moreover the reader is expected to be familiar with abelian varieties (see [M2] for example), their Dieudonné modules (see §3 of [Mi1] for a short review of this material), and the comparison isomorphism of Fontaine–Messing [FM] and Faltings [Fa]. The reader may also find it useful to look at part III of [K5], which concerns the case  $B = \mathbb{Q}$ .

There remains the pleasant task of thanking R. P. Langlands, who introduced me to Shimura varieties by suggesting that I write up his lectures on this topic at the 1977 AMS Summer Research Institute in Corvallis, and M. Rapoport, who has taught me a great deal about Shimura varieties over the years.

## 1. INVOLUTIONS ON SEMISIMPLE ALGEBRAS

Let  $B$  be a finite-dimensional semisimple algebra over a field  $F$  of characteristic zero. An involution  $*$  on  $B$  is a linear isomorphism from  $B$  to itself such that  $(xy)^* = y^*x^*$  and  $x^{**} = x$ . Suppose that  $F$  is algebraically closed. Since the involution permutes the simple factors of  $B$ , the algebra  $B$  with involution is a product of semisimple algebras with involution, with each factor either simple or else the product of two simple algebras interchanged by  $*$ . Thus, in classifying semisimple algebras with involution, we may as well suppose that we are in one of these two irreducible cases. In the first case  $B$  is a matrix algebra over  $F$  and the involution differs from the standard transpose involution by an inner automorphism  $x \mapsto yxy^{-1}$ . The equality  $x^{**} = x$  implies that  $y$  is either symmetric or alternating, hence that the pair consisting of  $B$  and  $*$  is isomorphic to the algebra of endomorphisms of a finite-dimensional nondegenerate quadratic or symplectic vector space over  $F$  with involution given by the adjoint map for the given bilinear form. In the second case  $B$  is isomorphic to a product  $M \times M^{\text{opp}}$  with involution given by  $(x, y) \mapsto (y, x)$ , where  $M$  is a matrix algebra and  $M^{\text{opp}}$  denotes the opposite algebra.

Let  $B_{\text{sym}}$  denote the subspace of  $B$  consisting of elements that are fixed by the involution and let  $B_{\text{sym}}^\times$  denote the subset consisting of all elements of  $B_{\text{sym}}$  that are invertible in  $B$ . The group  $B^\times$  of invertible elements in

$B$  acts on  $B_{\text{sym}}$ , the action of an invertible element  $b$  of  $B$  being given by  $x \mapsto bxb^*$  (for  $x$  in  $B_{\text{sym}}$ ). This action preserves the subset  $B_{\text{sym}}^\times$ . When  $F$  is algebraically closed, the action is transitive on this subset, as one sees by examining the three irreducible cases from the previous discussion, keeping in mind that over an algebraically closed field of characteristic different from 2 any two nondegenerate symmetric bilinear forms are equivalent.

Let  $G$  denote the algebraic group whose points in any algebra  $R$  over  $F$  are given by the set of elements  $x$  in  $B \otimes_F R$  such that  $xx^* = 1$ . The discussion above shows that when  $F$  is algebraically closed,  $G$  is a product of orthogonal, symplectic, and general linear groups over  $F$ .

## 2. POSITIVE INVOLUTIONS

In this section  $B$  denotes a finite-dimensional semisimple algebra over  $\mathbb{R}$  with involution  $*$ . By a  $B$ -module we mean finitely generated left  $B$ -module. A Hermitian form on a  $B$ -module  $V$  is a symmetric real-valued bilinear form  $(v, w)$  on  $V$  such that  $(bv, w) = (v, b^*w)$  for all  $b \in B$  and all  $v, w \in V$ . A Hermitian  $B$ -module is a  $B$ -module  $V$  together with a Hermitian form on  $V$ . We say that a Hermitian  $B$ -module is positive definite if  $(v, v) > 0$  for all nonzero  $v \in V$ .

**Lemma 2.1.** *Any positive definite Hermitian  $B$ -module  $V$  can be written as a direct sum of positive definite Hermitian  $B$ -modules that are irreducible as  $B$ -modules.*

Use induction on the length of  $V$ . If the length is 0, there is nothing to do. Otherwise choose an irreducible submodule  $W$  of  $V$ . Then a Hermitian  $B$ -module  $V$  is the direct sum of  $W$  and its orthogonal complement. Now apply the induction hypothesis to this orthogonal complement.

**Lemma 2.2.** *The following are equivalent conditions on the involution  $*$ .*

- (1) *Every  $B$ -module carries some positive definite Hermitian form.*
- (2) *For every faithful  $B$ -module  $V$  we have  $\text{tr}(xx^*; V) > 0$  for all nonzero  $x \in B$ .*
- (3)  *$\text{tr}_{B/\mathbb{R}}(xx^*) > 0$  for all nonzero  $x \in B$ .*
- (4) *There exists a  $B$ -module  $V$  such that  $\text{tr}(xx^*; V) > 0$  for all nonzero  $x \in B$ .*
- (5) *There exists a faithful positive definite Hermitian  $B$ -module.*

First show that (1) implies (2). Let  $V$  be a faithful  $B$ -module. By (1) there exists a positive definite Hermitian form on  $V$ . Then  $\text{tr}(xx^*; V)$  is the Hilbert-Schmidt norm of the endomorphism of  $V$  given by multiplication by  $x$ . Since  $V$  is faithful, this norm is positive if  $x$  is nonzero.

It is obvious that (2) implies (3) and (3) implies (4). Next show that (4) implies (5). By (4) there exists a  $B$ -module  $V$  such that  $\text{tr}(xx^*; V) > 0$  for all nonzero  $x \in B$ . Define a bilinear form  $(x, y)_0$  on  $B$  by  $(x, y)_0 = \text{tr}(xy^*; V)$  and consider its symmetrization  $(x, y) := (x, y)_0 + (y, x)_0$ . Then  $(x, y)$  is a positive definite Hermitian form on the faithful  $B$ -module  $B$ .

Finally show that (5) implies (1). Let  $V$  be a faithful positive definite Hermitian  $B$ -module. By Lemma 2.1  $V$  is a direct sum of positive definite Hermitian

$B$ -modules that are irreducible as  $B$ -modules. Since  $V$  is faithful, every irreducible  $B$ -module is isomorphic to one of these direct summands and hence carries some positive definite Hermitian form. This proves (1) because any  $B$ -module can be written as a direct sum of irreducible  $B$ -modules.

**Definition.** An involution is said to be positive if it satisfies the equivalent conditions of Lemma 2.2.

**Lemma 2.3.** (1) *If  $*$  is a positive involution of  $B$ , then it is also a positive involution of  $B^{\text{opp}}$ .*

(2) *The tensor product (respectively, direct product) of positive involutions on semisimple algebras  $B_1$  and  $B_2$  is a positive involution on  $B_1 \otimes_{\mathbb{R}} B_2$  (respectively,  $B_1 \times B_2$ ).*

(3) *If  $*$  is a positive involution of  $B$  leaving stable a semisimple subalgebra  $C$  of  $B$ , then  $*$  induces a positive involution of  $C$ .*

For (1) simply note that  $*$  is an isomorphism of algebras with involution from  $B$  to  $B^{\text{opp}}$ . To prove (2) we choose for  $i = 1, 2$  a faithful positive definite Hermitian  $B_i$ -module  $V_i$ . Then the tensor product (respectively, direct sum) of  $V_1$  and  $V_2$  is a faithful positive definite Hermitian module for  $B_1 \otimes B_2$  (respectively,  $B_1 \times B_2$ ). To prove (3) choose a faithful positive definite Hermitian  $B$ -module. Then  $V$  is a faithful positive definite Hermitian  $C$ -module.

**Lemma 2.4.** *Let  $*$  be a positive involution of  $B$ . Then  $*$  leaves stable each simple factor of  $B$ , and as an algebra with involution  $B$  is the direct product of simple algebras with positive involution.*

Obviously the involution permutes the simple factors of  $B$ . It cannot interchange two factors; if it did, then  $xx^*$  would be zero for any element  $x$  belonging to one of these factors, which would contradict (3) in Lemma 2.2. Therefore the involution preserves the simple factors and is positive on them by (3) of Lemma 2.3.

**Definition.** We say that an element  $x \in B$  is symmetric if  $x^* = x$ . We write  $B_{\text{sym}}$  for the set of symmetric elements of  $B$ .

**Lemma 2.5.** *Let  $B$  be a finite-dimensional division algebra over  $\mathbb{R}$ , and suppose that  $*$  is a positive involution of  $B$ . Then  $B_{\text{sym}} = \mathbb{R}$ .*

Let  $x$  belong to  $B_{\text{sym}}$ . Then  $F := \mathbb{R}[x]$  is a commutative field stable under  $*$ , and  $*$  acts by the identity on  $F$ . Therefore by Lemma 2.3 the identity is a positive involution of  $F$ . Therefore by Lemma 2.2  $\text{tr}_{F/\mathbb{R}}(x^2)$  is positive for all nonzero  $x$  in  $F$ . This would not be the case if  $F$  were isomorphic to  $\mathbb{C}$ ; therefore  $F = \mathbb{R}$ .

**Lemma 2.6.** *Suppose that  $*$  is a positive involution of  $B$ .*

- (1) *Let  $V$  be an irreducible  $B$ -module. Then the real vector space of Hermitian forms on  $V$  is one-dimensional.*
- (2) *Two positive definite Hermitian  $B$ -modules are isomorphic as Hermitian  $B$ -modules if and only if they are isomorphic as  $B$ -modules.*

First we prove (1). Choose a positive definite Hermitian form  $(x, y)_0$  on  $V$ . Let  $(x, y)$  be any Hermitian form on  $V$ . Thinking of Hermitian forms on  $V$  as  $B$ -module maps from  $V$  to the dual of  $V$ , we see that there exists a unique  $B$ -module endomorphism  $f$  of  $V$  such that  $(v, w) = (v, fw)_0$  for all  $v, w \in V$ . Let  $\iota$  be the involution of  $\text{End}_{\mathbb{R}}(V)$  obtained from the bilinear form  $(x, y)_0$ , so that  $(fv, w)_0 = (v, \iota(fw))_0$  for all  $f \in \text{End}_{\mathbb{R}}(V)$  and all  $v, w \in V$ . Then  $(x, y)_0$  is a positive definite Hermitian form on the faithful  $\text{End}_{\mathbb{R}}(V)$ -module  $V$ . Therefore  $\iota$  is positive. It leaves  $\text{End}_B(V)$  stable, hence induces a positive involution of  $\text{End}_B(V)$ . Since  $(x, y)$  is symmetric,  $f$  is a symmetric element of  $\text{End}_B(V)$ . By Lemma 2.5  $f$  is a real scalar.

Next we prove (2). By Lemma 2.1 it is enough to show that any two positive definite Hermitian forms on an irreducible  $B$ -module yield isomorphic Hermitian  $B$ -modules. By the first part of the lemma the second form is a real multiple of the first. Since both forms are positive definite, this multiple must be positive, hence is a square in  $\mathbb{R}$ . Therefore the second form is isomorphic to the first by multiplication by a real number.

**Lemma 2.7.** *For all  $b \in B$  there are equalities  $\text{tr}_{B/\mathbb{R}} b = \text{tr}_{B^{\text{opp}}/\mathbb{R}} b = \text{tr}_{B/\mathbb{R}} b^*$ .*

Since  $B$  is semisimple,  $\text{tr}_{B/\mathbb{R}}(xy)$  is a nondegenerate bilinear form on  $B$ . Right multiplication by  $b$  and left multiplication by  $b$  are adjoint for this form. Therefore  $\text{tr}_{B/\mathbb{R}} b = \text{tr}_{B^{\text{opp}}/\mathbb{R}} b$ . Since  $*$  is an isomorphism from  $B^{\text{opp}}$  to  $B$ , we have  $\text{tr}_{B/\mathbb{R}} b^* = \text{tr}_{B^{\text{opp}}/\mathbb{R}} b$ .

*Notation.* For  $b \in B$  we write  $(x, y)_b$  for the bilinear form  $(x, y)_b = \text{tr}_{B/\mathbb{R}} xby^*$  on  $B$ .

In this way we get an isomorphism from  $B$  to the real vector space of all bilinear forms  $(x, y)$  on  $B$  such that  $(bx, y) = (x, b^*y)$  for all  $b, x, y \in B$ . Using Lemma 2.7 we see that  $(x, y)_b$  is symmetric (respectively, alternating) if and only if  $b$  is symmetric (respectively, antisymmetric, that is,  $b^* = -b$ ). It is easy to see that  $(x, y)_b$  is nondegenerate if and only if  $b$  is an invertible element of  $B$ .

**Definition.** We say that a symmetric element  $b$  of  $B$  is positive if the form  $(x, y)_b$  is positive definite. We write  $B_+$  for the set of positive elements in  $B_{\text{sym}}$ .

**Lemma 2.8.** *Suppose that  $*$  is a positive involution of  $B$ . Then  $B_+$  is a nonempty open convex cone in  $B_{\text{sym}}$ . Moreover the group  $B^\times$  acts transitively on  $B_+$ , the action of  $b \in B^\times$  on  $x \in B_+$  being given by  $x \mapsto bxb^*$ . Finally, the set  $B_+$  is equal to  $\{bb^* | b \in B^*\}$ .*

The set of positive definite Hermitian forms on  $B$  is an open convex cone in the vector space of Hermitian forms on  $B$ . This implies the corresponding statement for  $B_+$ . The transitivity of the action of  $B^\times$  follows from the second part of Lemma 2.6. The last statement follows from this transitivity and the fact that  $1 \in B_+$  (by the third part of Lemma 2.2).

**Lemma 2.9.** *Suppose that  $*$  is a positive involution leaving stable a semisimple subalgebra  $C$  of  $B$ . Then  $C_+ = C \cap B_+$ .*

Let  $c \in C_+$ . Then  $c = dd^*$  for some  $d \in C^\times$ . Therefore  $c \in B_+$ . To prove the reverse inclusion we start with an element  $c \in C \cap B_+$ . We want to show that  $c \in C_+$ ; for this it is enough to check that  $\text{tr}_{C/\mathbb{R}} xcx^*$  is positive for all nonzero  $x \in C$ . Since  $c$  is invertible in  $B$ , it is invertible in  $C$ ; therefore,  $\text{tr}_{C/\mathbb{R}} xcy^*$  is a nondegenerate symmetric bilinear form, and it is enough to show that  $\text{tr}_{C/\mathbb{R}} xcx^*$  is nonnegative for all  $x \in C$ . Let  $y = xcx^*$ . There exists  $b \in B^\times$  such that  $c = bb^*$ . Therefore  $y = xb(xb)^*$ . It follows that left multiplication by  $y$  on  $B$  is selfadjoint with nonnegative eigenvalues (take the adjoint with respect to the form  $\text{tr}_{B/\mathbb{R}}(xy^*)$  on  $B$ ). Moreover left multiplication by  $y$  preserves the subspace  $C$  of  $B$ , and hence has nonnegative eigenvalues on  $C$ . Therefore  $\text{tr}_{C/\mathbb{R}} y$  is nonnegative.

Let  $(B, *_B), (C, *_C)$  be two semisimple finite-dimensional  $\mathbb{R}$ -algebras with positive involution. We say that an  $\mathbb{R}$ -algebra homomorphism  $i$  from  $B$  to  $C$  is a  $*$ -homomorphism if  $i(b^*) = i(b)^*$  for all  $b \in B$ .

**Lemma 2.10.** *Any homomorphism  $i$  from  $B$  to  $C$  is conjugate under  $C^\times$  to a  $*$ -homomorphism. If two  $*$ -homomorphisms  $i_1, i_2$  from  $B$  to  $C$  are conjugate under  $C^\times$ , then they are conjugate by an element  $c$  of  $C$  satisfying  $cc^* = 1$ .*

First we prove the first statement. Using  $i$ , we make  $C$  into a  $C \otimes_{\mathbb{R}} B^{\text{opp}}$ -module. Since the tensor product of  $*_B$  and  $*_C$  is a positive involution of  $C \otimes_{\mathbb{R}} B^{\text{opp}}$ , there exists a positive definite Hermitian form on the  $C \otimes_{\mathbb{R}} B^{\text{opp}}$ -module  $C$ . This form can be written as  $(x, y)_c$  for some  $c \in C_+$ , and since  $(x, y)_c$  is Hermitian for  $B^{\text{opp}}$ , we have  $i(b)c = ci(b^*)^*$  for all  $b \in B$ . Write  $c = dd^*$  for some  $d \in C^\times$ . Then  $\text{Int}(d)^{-1} \circ i$  is a  $*$ -homomorphism.

Next we prove the second statement. Consider the positive definite Hermitian  $C \otimes_{\mathbb{R}} C^{\text{opp}}$ -module  $(C, \text{tr}_{C/\mathbb{R}}(xy^*))$ . Using  $i_1$  and  $i_2$ , we regard  $C$  as a positive definite Hermitian  $C \otimes_{\mathbb{R}} B^{\text{opp}}$ -module in two ways. These two Hermitian modules are isomorphic as modules since  $i_1$  and  $i_2$  are conjugate under  $C^\times$ ; therefore by Lemma 2.6 they are isomorphic as Hermitian modules. Therefore there exists  $c \in C^\times$  that conjugates  $i_1$  into  $i_2$  and has the property that right multiplication by  $c$  preserves the form  $\text{tr}_{C/\mathbb{R}} xy^*$ , or in other words,  $cc^* = 1$ .

**Lemma 2.11.** *Let  $*, i$  be two positive involutions on  $B$ . Then there exists  $b \in B^\times$  such that  $\text{Int}(b)$  is a  $*$ -homomorphism from  $(B, i)$  to  $(B, *)$ . Moreover we have  $x^i = c^{-1}x^*c$  for the element  $c = b^*b$ .*

Apply Lemma 2.10 to the identity map from  $B$  to  $B$  in order to get the first statement. The second statement follows from the first.

*Remark.* The standard involutions on  $\mathbf{M}_n(\mathbb{R}), \mathbf{M}_n(\mathbb{C}), \mathbf{M}_n(\mathbb{H})$  are positive. This fact, together with Lemmas 2.4 and 2.11, shows that every semisimple algebra with positive involution is isomorphic to a product of these standard examples.

### 3. SEMISIMPLE CATEGORIES

Let  $\mathcal{C}$  be an abelian category in which every object has finite length. The endomorphism ring of any simple object is a division ring, and the endomor-

phism ring of any semisimple object is a semisimple ring. Recall that  $\mathcal{C}$  is said to be semisimple if all its objects are semisimple. If  $\mathcal{C}$  is semisimple, then for every object  $X$  of  $\mathcal{C}$  the endomorphism ring  $\text{End}(X)$  is semisimple. There is also a converse.

**Lemma 3.1.** *Suppose that for every object  $X$  of  $\mathcal{C}$  the endomorphism ring  $\text{End}(X)$  is semisimple. Then  $\mathcal{C}$  is semisimple.*

We prove that any object  $Y$  of  $\mathcal{C}$  is semisimple by induction on the length of  $Y$ . If the length is 0 or 1, there is nothing to do; so we assume that the length is strictly greater than 1. Let  $Z$  be a subobject of  $Y$  such that the quotient  $X := Y/Z$  is simple, and let  $p$  be the canonical map from  $Y$  to  $X$ . By the induction hypothesis  $Z$  is semisimple. We will assume that  $Y$  is not semisimple and get a contradiction. Every simple subobject of  $Y$  must be contained in  $Z$  (otherwise we could write  $Y$  as the direct sum of  $Z$  and the simple subobject). Therefore  $Z$  can be characterized as the sum of all the simple subobjects of  $Y$ . Therefore any endomorphism of  $Y$  preserves  $Z$ . Hence we get a homomorphism from  $\text{End}(Y)$  to  $\text{End}(Z) \times \text{End}(X)$ , whose kernel is  $\text{Hom}(X, Z)$  with multiplication given by  $f g = 0$  for all  $f, g \in \text{Hom}(X, Z)$ . On the other hand this kernel is a two-sided ideal in the semisimple ring  $\text{End}(Y)$ , and therefore  $\text{Hom}(X, Z) = 0$ .

Our next step is to show that  $\text{Hom}(X, Y) = 0$ . Let  $f \in \text{Hom}(X, Y)$ . If  $p \circ f \neq 0$ , then since  $\text{End}(X)$  is a division ring, we could modify  $f$  on the right so as to get a new  $f$  with  $p \circ f = \text{id}_X$ . Then  $Y$  would be the direct sum of  $Z$  and  $X$ , and hence would be semisimple, a contradiction. Therefore  $p \circ f = 0$ , which just says that  $f$  factors through the subobject  $Z$  of  $Y$ . Since we already know that  $\text{Hom}(X, Z) = 0$ , we conclude that  $f = 0$ , as desired.

Now consider the ring  $\text{End}(X \oplus Y)$ . Since  $\text{Hom}(X, Y) = 0$ , the semisimple ring  $\text{End}(X \oplus Y)$  has as two-sided ideal the group  $\text{Hom}(Y, X)$  with the zero multiplication law, and therefore  $\text{Hom}(Y, X) = 0$ . This is a contradiction, since  $p$  is a nonzero element of  $\text{Hom}(Y, X)$ .

Let  $L$  be a field of characteristic 0, and let  $\mathcal{C}$  be a semisimple  $L$ -linear abelian category in which  $\text{Hom}(X, Y)$  is finite-dimensional over  $L$  for every pair  $X, Y$  of objects in  $\mathcal{C}$  (in particular, every object in  $\mathcal{C}$  has finite length). Let  $B$  be a finite-dimensional semisimple  $L$ -algebra and let  $\mathcal{C}_B$  be the category of  $B$ -objects in  $\mathcal{C}$ : the objects of  $\mathcal{C}_B$  are pairs  $(X, i)$  consisting of an object  $X$  in  $\mathcal{C}$  and an  $L$ -algebra homomorphism  $i: B \rightarrow \text{End}(X)$ , and a morphism from  $(X, i)$  to  $(Y, j)$  is a morphism  $f: X \rightarrow Y$  in  $\mathcal{C}$  such that  $f \circ i(b) = j(b) \circ f$  for all  $b \in B$ . Let  $F$  be the center of  $B$ , a finite product of finite extensions of  $L$ . The category  $\mathcal{C}_B$  has a natural structure of  $F$ -linear category, and it is clear that  $\text{Hom}(X, Y)$  is finitely generated over  $F$  for any pair  $X, Y$  of objects in  $\mathcal{C}_B$ .

**Lemma 3.2.** *The category  $\mathcal{C}_B$  is abelian and semisimple. The functor  $\mathcal{C}_B \rightarrow \mathcal{C}$  taking  $(X, i)$  to  $X$  is faithful and exact. Moreover, if  $(X, i)$  is simple in  $\mathcal{C}_B$ , then  $X$  is isotypic in  $\mathcal{C}$ .*

The category  $\mathcal{C}$  is a direct sum  $\bigoplus_{X \in S} \mathcal{C}_X$ , where  $S$  is a set of representatives for the isomorphism classes of simple objects in  $\mathcal{C}$  and  $\mathcal{C}_X$  denotes the full

subcategory of  $\mathcal{C}$  consisting of isotypic objects of type  $X$ . The category of  $B$ -objects in  $\mathcal{C}$  is the direct sum over  $X \in S$  of the categories of  $B$ -objects in the categories  $\mathcal{C}_X$ . Therefore it is enough to prove the lemma in the case that  $\mathcal{C}$  has only one simple object  $X$  (up to isomorphism), in which case  $\mathcal{C}$  is equivalent to the category of finitely generated left  $D^{\text{opp}}$ -modules, where  $D = \text{End}(X)$ , and  $\mathcal{C}_B$  is equivalent to the category of finitely generated left  $B \otimes_L D^{\text{opp}}$ -modules. The ring  $B \otimes_L D^{\text{opp}}$  is semisimple, which implies that  $\mathcal{C}_B$  is semisimple. The rest of the lemma is obvious.

It is easy to describe the simple objects in  $\mathcal{C}_B$  in terms of the simple objects in  $\mathcal{C}$ . Let  $Y$  be a simple object in  $\mathcal{C}$ , denote by  $D$  the division algebra  $\text{End}(Y)$  and by  $M$  its center, and define a positive integer  $n$  by the equality  $n^2 = \dim_M D$ . Let  $(X, i)$  be a simple object of  $\mathcal{C}_B$  such that  $X$  is isotypic of type  $Y$ , say  $X \approx Y^s$ . Denote by  $C$  the division algebra  $\text{End}_{\mathcal{C}_B}(X, i)$  and by  $E$  its center, and define a positive integer  $m$  by the equality  $m^2 = \dim_E C$ . The field  $M$  is canonically isomorphic to the center of  $\text{End}_{\mathcal{C}}(X)$  and hence maps into the  $F$ -algebra  $E$ , yielding an  $L$ -algebra map  $\rho: F \otimes_L M \rightarrow E$ . Write  $F \otimes_L M = M_1 \times \cdots \times M_r$  where  $M_1, \dots, M_r$  are fields. Then  $\rho$  induces an isomorphism  $M_j \simeq E$  for a unique value of the index  $j \in \{1, \dots, r\}$  (for the surjectivity of  $\rho$  see the first part of the proof of the lemma below). Thus we have associated to  $(X, i)$  a factor  $M_j$  of  $F \otimes_L M$ .

**Lemma 3.3.** *This construction sets up a bijection between the set of isomorphism classes of simple objects  $(X, i)$  in  $\mathcal{C}_B$  such that  $X$  is isotypic of type  $Y$  and the set of factors  $M_j$  of  $F \otimes_L M$ . The class  $[C]$  of  $C$  in the Brauer group of  $E$  is equal to  $[D \otimes_M E] - [B \otimes_F E]$ . The numbers  $n, m, s$  are related by the equality  $sn = d[E : M]m$ , where  $d$  is the positive integer such that  $d^2 = \dim_E(B \otimes_F E)$ .*

As in the proof of the previous lemma it is enough to consider the case in which  $\mathcal{C}$  is the category of finitely generated left modules over the division algebra  $D^{\text{opp}}$ . Then  $\mathcal{C}_B$  is equivalent to the category of finitely generated left  $D' := B \otimes_L D^{\text{opp}}$ -modules. The center of  $D'$  is  $F \otimes_L M = M_1 \times \cdots \times M_r$ , and  $D'$  factors in a parallel way as  $D_1 \times \cdots \times D_r$  where  $D_j$  is a simple algebra with center  $M_j$ . The first statement of the lemma is now clear.

Fix one of the factors  $M_j$ , call it  $E$ ; the corresponding factor  $D_j$  of  $D'$  is isomorphic to  $(B \otimes_F E) \otimes_E (D^{\text{opp}} \otimes_M E) \approx \mathbf{M}_t(C^{\text{opp}})$  with  $t = dn/m$  ( $\mathbf{M}_t$  denotes  $t \times t$ -matrices). This proves the statement regarding the class of  $C$  in the Brauer group of  $E$ . The statement regarding the numbers  $n, m, s$  follows by calculating the rank of  $D_j$  as a left  $D^{\text{opp}}$ -module. On the one hand its rank is  $s \cdot \text{rank}_{D_j}(D_j) = st = sdn/m$ . On the other hand, using the fact that  $D_j = (B \otimes_F E) \otimes_E (D^{\text{opp}} \otimes_M E)$ , we see that its rank is  $d^2[E : M]$ . Equating these two expressions for the rank gives  $sn = d[E : M]m$ .

The following special case of Lemma 3.3 will be used later. Let  $L$  be a local field and let  $B$  be a central simple algebra of dimension  $d^2$  over  $L$ . Let  $\mathcal{C}$  be the category of pairs  $(V, \gamma)$ , where  $V$  is a finite-dimensional  $L$ -vector space and  $\gamma$  is a semisimple automorphism of  $V$ . A  $B$ -object in  $\mathcal{C}$  is a finite-

dimensional  $B$ -module  $V$  together with a semisimple automorphism  $\gamma$  of the  $B$ -module  $V$ . For  $\alpha \in L^\times$  the pair  $(L[\alpha], \text{multiplication by } \alpha)$  is a simple object  $Y_\alpha$  in  $\mathcal{C}$ , and this construction sets up a bijection between elements of  $L^\times$  up to conjugacy over  $L$  and isomorphism classes of simple objects in  $\mathcal{C}$ . Clearly  $\text{End}(Y_\alpha) = L[\alpha]$  and the  $L$ -dimension of the vector space underlying  $Y_\alpha$  is  $[L[\alpha] : L]$ . For  $\alpha \in L^\times$  let  $X_\alpha$  be a simple object in  $\mathcal{C}_B$  such that the object of  $\mathcal{C}$  underlying  $X_\alpha$  is isotypic of type  $Y_\alpha$ .

**Corollary 3.4.** *The construction  $\alpha \mapsto X_\alpha$  sets up a bijection between elements of  $L^\times$  up to conjugacy over  $L$  and isomorphism classes of simple objects in  $\mathcal{C}_B$ . The endomorphism algebra  $\text{End}(X_\alpha)$  is a central division algebra  $C$  over  $L[\alpha]$  whose Hasse invariant is given by  $\text{inv}(C) = -[L[\alpha] : L]\text{inv}(B)$ . Moreover the dimension of the  $L$ -vector space underlying  $X_\alpha$  is  $d[L[\alpha] : L](\dim_{L[\alpha]} C)^{1/2}$ .*

The corollary is an immediate consequence of the lemma. Using the corollary, we will analyze the objects in  $\mathcal{C}_B$  having a given  $L$ -dimension. Let  $V$  be an object in  $\mathcal{C}_B$ ; in other words, a  $B$ -module together with an automorphism  $\gamma$ . The characteristic polynomial of  $\gamma$  (as  $L$ -linear map) is a monic polynomial in  $L[T]$  whose degree is equal to  $\dim_L(V)$ . The characteristic polynomial determines the isomorphism class of  $V$  (since it determines the multiplicities of the simple constituents of  $V$ ). Let  $f \in L[T]$  be monic of degree  $m$  and for  $\alpha \in L^\times$  denote by  $m(\alpha)$  the multiplicity of  $\alpha$  as a root of  $f$ .

**Lemma 3.5.** *The polynomial  $f$  arises as the characteristic polynomial of an  $m$ -dimensional object in  $\mathcal{C}_B$  if and only if the following statement holds for all  $\alpha \in L^\times$ : the number  $m(\alpha)$  is divisible by  $d$  and the quotient  $m(\alpha)/d$  kills the class of  $\text{End}(X_\alpha)$  in the Brauer group of  $L[\alpha]$ .*

Clearly  $f$  arises as a characteristic polynomial if and only if the following statement holds for all  $\alpha \in L^\times$ : the number  $m(\alpha)$  is divisible by the multiplicity of  $\alpha$  in the characteristic polynomial for the simple object  $X_\alpha$ . By the corollary the latter multiplicity is  $d(\dim_{L[\alpha]} C)^{1/2}$  where  $C = \text{End}(X_\alpha)$ . The lemma now follows from the fact that  $(\dim_{L[\alpha]} C)^{1/2}$  is the order of  $C$  in the Brauer group of  $L[\alpha]$ .

#### 4. HERMITIAN SYMMETRIC SPACES OF PEL TYPE

Let  $C$  be a semisimple finite-dimensional  $\mathbb{R}$ -algebra with involution  $*$ . Let  $h: \mathbb{C} \rightarrow C$  be an  $\mathbb{R}$ -algebra homomorphism such that  $h(z)^* = h(\bar{z})$  for all  $z \in \mathbb{C}$ . Then  $h(i)$  is antisymmetric for  $*$ , and therefore  $\iota(x) := h(i)^{-1}x^*h(i)$  ( $x \in C$ ) is an involution of  $C$ . Assume that  $\iota$  is a positive involution. Let  $G$  be the algebraic group over  $\mathbb{R}$  whose points in an  $\mathbb{R}$ -algebra  $R$  are given by  $G(R) = \{x \in C \otimes_{\mathbb{R}} R | xx^* \in R^\times\}$ , and let  $G_1$  be the closed subgroup such that  $G_1(R) = \{x \in C \otimes_{\mathbb{R}} R | xx^* = 1\}$ . We abuse notation by also using  $h$  to denote the restriction of  $h$  to  $\mathbb{C}^\times$ , regarded as a homomorphism of real algebraic groups  $\mathbb{C}^\times \rightarrow G$ .

**Lemma 4.1.** *The pair  $(G, h)$  satisfies the following three conditions.*

- (1) *The image under  $h$  of  $\mathbb{R}^\times$  is central in  $G$ .*
- (2) *Define  $\mu_h: \mathbb{G}_m \rightarrow G_{\mathbb{C}}$  by restricting  $h_{\mathbb{C}}: (R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m)_{\mathbb{C}} \rightarrow G_{\mathbb{C}}$  to the factor of  $(R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m)_{\mathbb{C}} = \mathbb{G}_m \times \mathbb{G}_m$  indexed by the identity map from  $\mathbb{C}$  to  $\mathbb{C}$  (the two factors of  $\mathbb{G}_m$  are indexed by the two  $\mathbb{R}$ -algebra maps from  $\mathbb{C}$  to  $\mathbb{C}$ ). Then  $\mathbb{G}_m$ , acting on the Lie algebra  $\text{Lie}(G_{\mathbb{C}})$  by means of  $\mu_h$  and the adjoint action of  $G_{\mathbb{C}}$  on  $\text{Lie}(G_{\mathbb{C}})$ , has weights  $1, 0, -1$ .*
- (3) *The  $\mathbb{R}$ -form of  $G_1$  obtained by twisting  $G_1$  by the inner automorphism  $\text{Int}(h(i))$  is the compact form of  $G_1$ .*

Statement (1) is obvious. We prove (2) by choosing a faithful finitely generated left  $C$ -module  $V$ . Note that  $h: \mathbb{C} \rightarrow C$  makes  $V$  into a complex vector space. Therefore (2) follows from the following easily verified fact: Let  $V$  be a finite-dimensional complex vector space, let  $h: \mathbb{C}^\times \rightarrow GL_{\mathbb{R}}(V)$  be the restriction of  $C \rightarrow \text{End}_{\mathbb{R}}(V)$  to  $\mathbb{C}^\times$ , and let  $\mu_h: \mathbb{G}_m \rightarrow GL_{\mathbb{C}}(V_{\mathbb{C}})$  be obtained from  $h$  as before. Then  $\mathbb{G}_m$ , acting on the Lie algebra of  $GL_{\mathbb{C}}(V_{\mathbb{C}})$  by means of  $\mu_h$  and the adjoint action, has weights  $1, 0, -1$ .

To prove (3) we must show that the group

$$\{x \in C \otimes_{\mathbb{R}} \mathbb{C} \mid xx^* = 1 \text{ and } h(i)^{-1}\bar{x}h(i) = x\}$$

is compact. This group is a closed subgroup of the group  $\{x \in C \otimes_{\mathbb{R}} \mathbb{C} \mid xx' = 1\}$ , where  $x \mapsto x'$  is the tensor product of  $i$  on  $C$  and complex conjugation on  $\mathbb{C}$ ; the involution  $x \mapsto x'$  is positive (Lemma 2.3), and therefore the group  $\{x \in C \otimes_{\mathbb{R}} \mathbb{C} \mid xx' = 1\}$  is compact, since by choosing a faithful positive definite Hermitian  $C \otimes_{\mathbb{R}} \mathbb{C}$ -module, we can embed this group as a closed subgroup of the orthogonal group of a positive definite symmetric bilinear form.

Lemma 4.1 says that  $(G, h)$  satisfies the conditions (1.5.1), (1.5.2), (1.5.3) of [D3]. Therefore (see [D2, D3]) the set  $X_\infty$  of conjugates of  $h$  under  $G(\mathbb{R})$  is a finite union of copies of the symmetric space for the identity component of  $G(\mathbb{R})$ , and this symmetric space is of Hermitian type.

It is easy to classify the isomorphism classes of triples  $(C, *, h)$  satisfying the conditions above. First note that  $*$  can be reconstructed from  $i$  and  $h$ , and that  $*$  and  $i$  agree on  $h(\mathbb{C})$ . Therefore it is equivalent to classify triples  $(C, i, h)$ , where  $i$  is a positive involution on  $C$  and  $h$  is an  $\mathbb{R}$ -algebra homomorphism  $C \rightarrow C$  such that  $h(z)^i = h(\bar{z})$  for all  $z \in \mathbb{C}$ . By Lemma 2.4 the algebra with positive involution  $(C, i)$  is a product of simple  $\mathbb{R}$ -algebras with positive involution. Therefore we may as well assume that  $C$  is simple. By the remark at the end of §2  $(C, i)$  is isomorphic to one of  $\mathbf{M}_n(\mathbb{R}), \mathbf{M}_n(\mathbb{C}), \mathbf{M}_n(\mathbb{H})$  with the standard involution.

By Lemma 2.10, classifying  $*$ -homomorphisms  $\mathbb{C} \rightarrow C$  up to inner automorphisms of  $(C, i)$  is the same as classifying  $\mathbb{R}$ -algebra homomorphisms  $\mathbb{C} \rightarrow C$  up to conjugacy by  $C^\times$ . With  $D = \mathbb{R}, \mathbb{C}, \mathbb{H}$  as the case may be, this is the same as classifying isomorphism classes of  $\mathbb{C} \otimes_{\mathbb{R}} D$ -modules that are of rank  $n$  as  $D$ -modules.

If  $D = \mathbb{R}$  then  $\mathbb{C} \otimes_{\mathbb{R}} D = \mathbb{C}$ , and no  $h$  exists unless  $n$  is even, in which case it is unique up to inner automorphisms of  $(C, i)$ . If  $D = \mathbb{C}$ , then  $\mathbb{C} \otimes_{\mathbb{R}} D = \mathbb{C} \times \mathbb{C}$ , and up to inner automorphisms of  $(C, i)$ , there is a  $*$ -homomorphism  $\mathbb{C} \rightarrow C$

for each pair  $(p, q)$  of nonnegative integers such that  $p + q = n$ . If  $D = \mathbb{H}$ , then  $\mathbb{C} \otimes_{\mathbb{R}} D$  is isomorphic to  $\mathbf{M}_2(\mathbb{C})$ , and up to inner automorphisms of  $(C, \iota)$ , there exists a unique  $*$ -homomorphism  $h: \mathbb{C} \rightarrow C$ . If  $D = \mathbb{R}$  or  $D = \mathbb{H}$ , then every automorphism of  $C$  is inner and our classification is complete. If  $D = \mathbb{C}$ , then, up to inner automorphisms,  $x \mapsto \bar{x}$  is the unique outer automorphism of  $\mathbf{M}_n(\mathbb{C})$ , and since this outer automorphism commutes with the standard involution  $x \mapsto \bar{x}^t$ , it gives an automorphism of  $(C, \iota)$ ; its effect on  $h$  is to replace  $(p, q)$  by  $(q, p)$ .

In PEL moduli problems, triples  $(C, *, h)$  arise in the following way. Let  $B$  be a semisimple finite-dimensional  $\mathbb{R}$ -algebra with positive involution  $*$ . Let  $V$  be a finitely generated left  $B$ -module, and let  $(v, w)$  be a nondegenerate skew-Hermitian form on  $V$  (in other words, a nondegenerate real-valued alternating bilinear form on  $V$  such that  $(bv, w) = (v, b^*w)$  for all  $v, w \in V$  and all  $b \in B$ ). Let  $h: \mathbb{C} \rightarrow \text{End}_B(V)$  be an  $\mathbb{R}$ -algebra homomorphism such that  $(h(z)v, w) = (v, h(\bar{z})w)$  for all  $v, w \in V$  and all  $z \in \mathbb{C}$ . Assume that the symmetric bilinear form  $(v, h(i)w)$  on  $V$  is positive definite. Now let  $C = \text{End}_B(V)$ . The adjoint map for  $(v, w)$  gives an involution  $*$  on  $C$ , characterized by  $(cv, w) = (v, c^*w)$  for all  $v, w \in V$  and all  $c \in C$ . Clearly  $h$  is an  $\mathbb{R}$ -algebra homomorphism from  $\mathbb{C}$  to  $C$  satisfying  $h(\bar{z}) = h(z)^*$  (in other words, a  $*$ -homomorphism for  $*$  on  $C$  and complex conjugation on  $\mathbb{C}$ ). The involution  $\iota$  of  $C$  defined by  $\iota(x) := h(i)^{-1}x^*h(i)$  is positive since the  $\iota$ -Hermitian form  $(v, h(i)w)$  is positive definite on the faithful  $C$ -module  $V$ . Thus  $(B, *, V, (\cdot, \cdot), h)$  gives rise to  $(C, *, h)$  and hence to  $G, G_1$ , and  $X_\infty$  as before.

Any  $(C, *, h)$  comes from some  $(B, *, V, (\cdot, \cdot), h)$ . If fact we can take  $B = C^{\text{opp}}$  with involution  $\iota$  (the usual  $\iota$  obtained from  $*$  and  $h$ ); for  $V$  we can take  $C$  viewed as a left  $C^{\text{opp}}$ -module using right multiplications, with skew-Hermitian form given by  $(x, y) = \text{tr}_{C/\mathbb{R}} x h(i) y^*$ ; we can take  $h: \mathbb{C} \rightarrow C$  to be the given one. Note, however, that there are other choices for  $(B, *, V, (\cdot, \cdot), h)$  giving rise to the same  $(C, *, h)$ .

**Lemma 4.2.** *Let  $(B, *, V, (\cdot, \cdot), h)$  be as before and assume that  $(\cdot, \cdot)'$  and  $h'$  satisfy the same conditions as  $(\cdot, \cdot)$  and  $h$ . Assume further that the two  $B \otimes_{\mathbb{R}} \mathbb{C}$ -module structures on  $V$  obtained from  $h$  and  $h'$  are isomorphic. Then  $(V, (\cdot, \cdot), h)$  and  $(V, (\cdot, \cdot)', h')$  are isomorphic as skew-Hermitian  $B \otimes_{\mathbb{R}} \mathbb{C}$ -modules. Moreover the set  $X_\infty$  for  $(B, *, V, (\cdot, \cdot), h)$  is equal to the set of  $*$ -homomorphisms  $h'$  from  $\mathbb{C}$  to  $C = \text{End}_B(V)$  satisfying the following two conditions.*

- (1) *The form  $(v, h'(i)w)$  is positive or negative definite.*
- (2) *The two  $B \otimes_{\mathbb{R}} \mathbb{C}$ -module structures on  $V$  obtained from  $h$  and  $h'$  are isomorphic.*

First we prove the first statement. The positive definite form  $(v, h(i)w)$  is  $B \otimes_{\mathbb{R}} \mathbb{C}$ -Hermitian for the positive involution on  $B \otimes_{\mathbb{R}} \mathbb{C}$  obtained by taking the tensor product of  $*$  on  $B$  and complex conjugation on  $\mathbb{C}$ , where we have used  $h$  to regard  $V$  as  $B \otimes_{\mathbb{R}} \mathbb{C}$ -module. We have the analogous assertion for  $(\cdot, \cdot)'$  and  $h'$  as well. By Lemma 2.6 the two Hermitian  $B \otimes_{\mathbb{R}} \mathbb{C}$ -modules we

get from  $(\cdot, \cdot)$ ,  $h$  and  $(\cdot, \cdot)', h'$  are isomorphic. Concretely this says that there exists  $c \in C^\times$  such that  $h' = \text{Int}(c) \circ h$  and  $(v, h(i)w) = (cv, h'(i)cw)'$  for all  $v, w \in V$ . It follows that  $(v, w) = (cv, cw)'$  for all  $v, w \in V$ , which means that  $c$  is an isomorphism from the skew-Hermitian  $B$ -module  $(V, (\cdot, \cdot), h)$  to  $(V, (\cdot, \cdot)', h')$ .

As for the second statement, it is easy to see that any  $h' \in X_\infty$  satisfies (1) and (2). Conversely, if  $h'$  satisfies (1) and (2), it follows from the first statement of the lemma that there exists a nonzero real number  $r$  and an isomorphism  $g$  of skew-Hermitian  $B \otimes_{\mathbb{R}} \mathbb{C}$ -modules from  $(V, (\cdot, \cdot), h)$  to  $(V, r(\cdot, \cdot), h')$ . Concretely,  $g$  is an element of  $G(\mathbb{R})$  conjugating  $h$  into  $h'$ , which shows that  $h' \in X_\infty$ .

**Lemma 4.3.** *Suppose that  $B, *, V, (\cdot, \cdot), h$  are as before and that  $h': \mathbb{C} \rightarrow C$  is another \*-homomorphism such that  $(v, h(i)w)$  is positive definite. Then  $h'$  and  $h$  are conjugate under  $G_1(\mathbb{R})$ .*

We begin by checking that it is enough to prove that  $h, h'$  are conjugate under  $C^\times$ , or, equivalently, that the  $B \otimes_{\mathbb{R}} \mathbb{C}$ -module structures on  $V$  obtained from  $h, h'$  are isomorphic. Indeed, by the proof of the first statement of the previous lemma it would then follow that there exists  $c \in C^\times$  conjugating  $h$  into  $h'$  and such that  $(v, w) = (cv, cw)$  for all  $v, w \in V$ , which means that  $c \in G_1(\mathbb{R})$ .

It remains to show that  $h, h'$  are conjugate under  $C^\times$ . By decomposing  $(B, *)$  as a product of simple  $\mathbb{R}$ -algebras with positive involution, we may without loss of generality assume that  $B$  is simple. Then  $C$  is also simple and has the same center as  $B$ . If this center is  $\mathbb{R}$ , then  $h$  and  $h'$  are conjugate under  $C^\times$  by the Skolem-Noether theorem, and we are done.

It remains to treat the case that the center of  $B$  is  $\mathbb{C}$ . What we must show is that the  $B \otimes_{\mathbb{R}} \mathbb{C}$ -module structures on  $V$  obtained from  $h, h'$  are isomorphic. These two modules are isomorphic if and only if they are isomorphic as modules over the center of  $B \otimes_{\mathbb{R}} \mathbb{C}$ , namely,  $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ . Therefore it is enough to treat the case  $B = \mathbb{C}$  ( $*$  is then automatically complex conjugation).

At this point our situation is as follows. We are given a complex vector space  $V$  together with a nondegenerate real-valued alternating form  $(v, w)$  on  $V$  such that  $(zv, w) = (v, \bar{z}w)$  for all  $v, w \in V$  and all  $z \in \mathbb{C}$ . We want to show that there is a unique  $\mathbf{GL}_{\mathbb{C}}(V)$ -conjugacy class of  $\mathbb{R}$ -algebra homomorphisms  $h: \mathbb{C} \rightarrow \text{End}_{\mathbb{C}}(V)$  such that  $(h(z)v, w) = (v, h(\bar{z})w)$  for all  $v, w \in V$  and all  $z \in \mathbb{C}$  and such that  $(v, h(i)w)$  is positive definite. Any such  $h$  decomposes  $V$  as  $V_1 \oplus V_2$  where  $V_1$  (respectively,  $V_2$ ) is the subspace consisting of vectors  $v$  such that  $h(z)v = zv$  for all  $z \in \mathbb{C}$  (respectively,  $h(z)v = \bar{z}v$  for all  $z \in \mathbb{C}$ ). Put  $p = \dim(V_1)$  and  $q = \dim(V_2)$ . Then two homomorphisms  $h, h'$  are conjugate by  $\mathbf{GL}_{\mathbb{C}}(V)$  if and only if  $p, q$  have the same values for  $h'$  as they have for  $h$ . Thus we need to show that the pair  $(p, q)$  is uniquely determined by the two conditions imposed on  $h$ . The alternating form  $(\cdot, \cdot)'$  on  $V$  is the imaginary part of a complex-valued Hermitian form  $(\cdot, \cdot)'$  on  $V$ :

$$(v, w)' = (v, iw) + i(v, w).$$

It is enough to show that  $(p, q)$  is the signature of  $(\cdot, \cdot)'$ . The subspaces  $V_1$  and  $V_2$  are orthogonal to each other for the alternating form  $(\cdot, \cdot)$  and hence for the Hermitian form  $(\cdot, \cdot)'$ . Since  $(v, h(i)w)$  is positive definite and  $h(i)$  acts by  $i$  (respectively,  $-i$ ) on  $V_1$  (respectively,  $V_2$ ), the restriction of  $(\cdot, \cdot)'$  to  $V_1$  (respectively,  $V_2$ ) is positive definite (respectively, negative definite), and it follows that the signature of  $(\cdot, \cdot)'$  is indeed  $(p, q)$ .

### 5. MODULI SPACES OF PEL TYPE

We are interested in PEL moduli problems having good reduction at all places of the reflex field lying over a given rational prime  $p$ . We write  $\mathbb{Z}_{(p)}$  for the localization of  $\mathbb{Z}$  at the prime ideal generated by  $p$ . Our starting point is the following long list of data. Let  $B$  be a finite-dimensional simple  $\mathbb{Q}$ -algebra with center  $F$ , and assume that  $B_{\mathbb{Q}_p}$  is a product of matrix algebras over unramified extensions of  $\mathbb{Q}_p$  (in particular, the number field  $F$  must be unramified at  $p$ ). Let  $\mathcal{O}_B$  be a  $\mathbb{Z}_{(p)}$ -order in  $B$  whose  $p$ -adic completion is a maximal order in  $B_{\mathbb{Q}_p}$ . Let  $*$  be a positive involution on  $B$  over  $\mathbb{Q}$  (recall that this means that  $*$  induces a positive involution on  $B_{\mathbb{R}}$ ) that preserves the order  $\mathcal{O}_B$ . Denote by  $F_0$  the fixed field of  $*$  on  $F$ . Let  $V$  be a nonzero finitely generated left  $B$ -module. Let  $(\cdot, \cdot)$  be a nondegenerate  $\mathbb{Q}$ -valued alternating form on  $V$  such that  $(bv, w) = (v, b^*w)$  for all  $v, w \in V$  and all  $b \in B$ . Assume that there exists a lattice  $\Lambda_0$  in  $V_{\mathbb{Q}_p}$  that is self-dual for  $(\cdot, \cdot)$  and is preserved by  $\mathcal{O}_B$ . Let  $C$  be the  $\mathbb{Q}$ -algebra  $\text{End}_B(V)$ ; it is a simple  $\mathbb{Q}$ -algebra with center  $F$  and has an involution  $*$  coming from the form  $(\cdot, \cdot)$ . Let  $G$  be the algebraic group over  $\mathbb{Q}$  whose points in any  $\mathbb{Q}$ -algebra  $R$  are given by  $\{x \in C \otimes_{\mathbb{Q}} R \mid xx^* \in R^\times\}$ , and let  $G_1$  be the subgroup whose  $R$ -points are given by  $\{x \in C \otimes_{\mathbb{Q}} R \mid xx^* = 1\}$ . We need two more data in order to formulate our PEL moduli problem. The first is a compact open subgroup  $K^p$  of  $G(\mathbb{A}_f^p)$ , where  $\mathbb{A}_f^p$  denotes the ring of finite adeles of  $\mathbb{Q}$  with trivial  $p$ -adic component. The second is a  $*$ -homomorphism  $h : \mathbb{C} \rightarrow C_{\mathbb{R}}$  (a  $*$ -homomorphism for complex conjugation on  $\mathbb{C}$  and  $*$  on  $C_{\mathbb{R}}$ ) such that the symmetric real-valued bilinear form  $(v, h(i)w)$  on  $V_{\mathbb{R}}$  is positive definite.

This concludes the list of necessary data, but we need to introduce some more objects before stating the moduli problem. Decompose the  $B_{\mathbb{C}}$ -module  $V_{\mathbb{C}}$  as  $V_{\mathbb{C}} = V_1 \oplus V_2$ , where  $V_1$  (respectively,  $V_2$ ) is the subspace of  $V_{\mathbb{C}}$  on which  $h(z)$  acts by  $z$  (respectively, by  $\bar{z}$ ). Since  $h$  centralizes  $B$ , the subspaces  $V_1$  and  $V_2$  are  $B_{\mathbb{C}}$ -submodules of  $V_{\mathbb{C}}$ . Let  $E \subset \mathbb{C}$  be the field of definition of the isomorphism class of the complex representation  $V_1$  of  $B$ ; the number field  $E$  is called the reflex field. Choose a basis  $\alpha_1, \dots, \alpha_t$  for the free  $\mathbb{Z}_{(p)}$ -module  $\mathcal{O}_B$ , and let  $X_1, \dots, X_t$  be indeterminates. Then

$$f(X_1, \dots, X_t) := \det(X_1\alpha_1 + \dots + X_t\alpha_t; V_1)$$

is a homogeneous polynomial of degree  $\dim_{\mathbb{C}}(V_1)$  in  $X_1, \dots, X_t$  with coefficients in  $\mathbb{C}$ ; since the isomorphism class of  $V_1$  is defined over  $E$ , these coefficients lie in  $E$ . In fact they lie in  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ , where  $\mathcal{O}_E$  denotes the ring of integers in  $E$ . For this it is enough to check that they lie in  $\mathcal{O}_{E'} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$

for some finite extension field  $E'$  of  $E$  over which  $V_1$  can be defined. But then, in a suitable basis, the matrix entries of  $\alpha_1, \dots, \alpha_t$  (acting on  $V_1$ ) are in  $\mathcal{O}_{E'} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ , and it follows that  $f(X_1, \dots, X_t)$  has coefficients in  $\mathcal{O}_{E'} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ .

We can finally formulate the moduli problem. We consider the set-valued contravariant functor from the category of locally noetherian schemes  $S$  over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  that associates to  $S$  the set of isomorphism classes of quadruples  $(A, \lambda, i, \bar{\eta})$  of the following type:  $A \rightarrow S$  is a projective abelian scheme over  $S$  up to prime-to- $p$  isogeny,  $\lambda: A \rightarrow \hat{A}$  is a polarization of  $A$  (a prime-to- $p$  isogeny from  $A$  to its dual abelian scheme  $\hat{A}$ , which at every geometric point  $s$  of  $S$  is a polarization of  $A_s$ ),  $i: \mathcal{O}_B \rightarrow \text{End}(A)$  is a \*-homomorphism for \* on  $\mathcal{O}_B$  and the Rosati involution on the  $\mathbb{Z}_{(p)}$ -algebra  $\text{End}(A)$  obtained from the polarization  $\lambda$ , and  $\bar{\eta}$  is a level structure of type  $K^p$  on  $A$  (see the explanation below).

We require that the quadruple  $(A, \lambda, i, \bar{\eta})$  satisfy the “determinant condition.” The Lie algebra  $\text{Lie}(A)$  is a locally free  $\mathcal{O}_S$ -module on which  $\mathcal{O}_B$  acts. Let  $\alpha_1, \dots, \alpha_t; X_1, \dots, X_t$  be as before. Then the determinant of the  $\mathcal{O}_S$ -linear endomorphism  $X_1\alpha_1 + \dots + X_t\alpha_t$  of  $\text{Lie}(A)$  is a homogeneous polynomial  $g(X_1, \dots, X_t)$  of degree  $\dim_S(A)$  with coefficients in the global sections of  $\mathcal{O}_S$ . Since  $S$  is a scheme over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ , it makes sense to require that  $g(X_1, \dots, X_t)$  be equal to the polynomial  $f(X_1, \dots, X_t)$  constructed earlier; this equality  $g = f$  is what we mean by the determinant condition. The significance of the determinant condition is explained by the following remark. Let  $E$  be a finite-dimensional semisimple algebra over a field  $k$ , and let  $\alpha_1, \dots, \alpha_t$  be a  $k$ -basis for  $E$ . For any finite-dimensional  $E$ -module  $V$  define a polynomial  $\det_V \in k[X_1, \dots, X_t]$  by

$$\det_V = \det(X_1\alpha_1 + \dots + X_t\alpha_t; V \otimes_k k[X_1, \dots, X_t]).$$

Then  $V$  is isomorphic to  $W$  if and only if  $\det_V = \det_W$ . This explains why we use the determinant rather than the trace, since the analogous assertion regarding the trace is false when the characteristic of  $k$  is finite. The proof is easy: replacing  $E$  by its center and  $k$  by its algebraic closure, it is enough to prove the statement for  $E = k \times \dots \times k$ , in which case it is obvious.

Two quadruples  $(A, \lambda, i, \bar{\eta})$  and  $(A', \lambda', i', \bar{\eta}')$  are said to be isomorphic if there is a prime-to- $p$  isogeny from  $A$  to  $A'$ , commuting with the action of  $\mathcal{O}_B$ , carrying  $\bar{\eta}$  into  $\bar{\eta}'$ , and carrying  $\lambda$  into a scalar multiple of  $\lambda'$  (a scalar in  $\mathbb{Z}_{(p)}^\times$ ).

Here is what is meant by a level structure of type  $K^p$  on  $A$ . It is enough to consider the case in which  $S$  is connected. The Tate  $\mathbb{A}_f^p$ -module of  $A$  is a smooth  $\mathbb{A}_f^p$ -sheaf on  $S$ . Choosing a geometric point  $s$  of  $S$ , we can think of the Tate  $\mathbb{A}_f^p$ -module of  $A$  as the Tate  $\mathbb{A}_f^p$ -module  $H_1(A_s, \mathbb{A}_f^p)$  of the abelian variety  $A_s$ , viewed as  $\pi_1(S, s)$ -module. A level structure of type  $K^p$  on  $A$  is a  $K^p$ -orbit  $\bar{\eta}$  of isomorphisms  $\eta: V_{\mathbb{A}_f^p} \rightarrow H_1(A_s, \mathbb{A}_f^p)$  of skew-Hermitian  $B$ -modules such that  $\bar{\eta}$  is fixed by  $\pi_1(S, s)$ . Here we are using the  $B$ -action (respectively, alternating form) on  $H_1(A_s, \mathbb{A}_f^p)$  obtained from  $i$  (respectively,

$\lambda$ ); since the alternating form actually takes values in the Tate twist  $\mathbb{A}_f^p(1)$  of  $\mathbb{A}_f^p$ , when it is viewed as an alternating form with values in  $\mathbb{A}_f^p$  it is only well defined up to a scalar, and thus by an isomorphism of skew-Hermitian  $B$ -modules we mean a  $B$ -module isomorphism carrying one alternating form into a scalar multiple of the other. Thus the similitude group  $G(\mathbb{A}_f^p)$  acts on the right of the set of isomorphisms  $\eta$ , simply transitively if this set is nonempty; this explains what was meant by a  $K^p$ -orbit of isomorphisms  $\eta$ . The group  $\pi_1(S, s)$  acts by similitudes on the skew-Hermitian  $B$ -module  $H_1(A_s, \mathbb{A}_f^p)$  and hence acts on the left of the set of  $K^p$ -orbits  $\bar{\eta}$ ; this explains the meaning of the condition that  $\bar{\eta}$  be fixed by  $\pi_1(S, s)$ . Because of this condition the notion of level structure of type  $K^p$  is essentially independent of the choice of geometric point  $s$  of  $S$ .

For sufficiently small  $K^p$  this moduli problem is representable by a quasi-projective scheme  $S_{K^p}$  over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ . For  $B = \mathbb{Q}$  this was proved by Mumford [M1] using geometric invariant theory. By forgetting the homomorphism  $i: \mathcal{O}_B \rightarrow \text{End}(A)$  we get a morphism from our moduli problem to one considered by Mumford, and therefore it is enough to show that our moduli problem is relatively representable over his. This is not hard, the key point being the following consequence of Grothendieck's theory of Hilbert schemes: For any projective abelian scheme  $A$  over a locally noetherian scheme  $S$  the functor  $T \mapsto \text{End}(A_T)$  on the category of locally noetherian  $S$ -schemes  $T$  is representable by a disjoint union of projective schemes over  $S$ .

Before discussing the smoothness of  $S_{K^p}$  we need to observe that our moduli problems fall into three families (Cases A, C, and D). The involution  $*$  is positive on the center  $F$  of the simple  $\mathbb{Q}$ -algebra  $B$ . Therefore the fixed field  $F_0$  of  $*$  on  $F$  is totally real, and either  $F = F_0$ , in which case  $*$  is said to be of the first kind, or else  $F$  is a totally complex quadratic extension of  $F_0$ , in which case  $*$  is said to be of the second kind. The group  $G_1$  is obtained from an algebraic group  $G_0$  over  $F_0$  by restriction of scalars from  $F_0$  to  $\mathbb{Q}$ , and we have  $G_0(F_0) = G_1(\mathbb{Q}) = \{x \in C \mid xx^* = 1\}$ .

Let  $m$  be the positive integer defined by  $[F : F_0](\dim_F C)^{1/2}$ . The existence of  $h: \mathbb{C} \rightarrow C_{\mathbb{R}}$  forces  $m$  to be even, say  $m = 2n$ . If  $*$  is of the second kind, then  $G_0$  is an inner form of the quasi-split unitary group over  $F_0$  obtained from the quadratic extension  $F$ ; we refer to this as Case A since over an algebraic closure of  $F_0$  the group  $G_0$  is of type  $A_{n-1}$ . If  $*$  is of the first kind, then over an algebraic closure of  $F_0$ , the group  $G_0$  is either an orthogonal group in  $2n$  variables (a group of type  $D_n$ ) or a symplectic group in  $2n$  variables (a group of type  $C_n$ ); of course we refer to these as Cases D and C respectively. Using that  $*$  is a positive involution and that our form  $(\cdot, \cdot)$  is skew-Hermitian, one sees easily that in Case C the algebra  $C_{\mathbb{R}}$  is a product of  $[F_0 : \mathbb{Q}]$  copies of  $\mathbf{M}_{2n}(\mathbb{R})$ , and that in Case D it is a product of  $[F_0 : \mathbb{Q}]$  copies of  $\mathbf{M}_n(\mathbb{H})$ ; of course in Case A it is a product of  $[F_0 : \mathbb{Q}]$  copies of  $\mathbf{M}_n(\mathbb{C})$ .

Now assume that  $p \neq 2$  if we are in Case D. Then for sufficiently small  $K^p$  the scheme  $S_{K^p}$  is smooth over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ . This can be proved using the deformation theory of Grothendieck-Messing [Me], as is done in [LR, Z1]

for Cases A and C. Case D is similar and will be left to the reader, who may, however, prefer to skip this exercise, since we will in fact exclude Case D starting with §14.

Continue to assume that  $p \neq 2$  if we are in Case D. Since  $S_{K^p}$  is smooth over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ , and since  $S_{K^p}(\mathbb{C})$  has only finitely many connected components (this follows easily from the description of  $S_{K^p}(\mathbb{C})$  given in §8), it follows that  $S_{K^p}$  is a finite disjoint union of projective schemes over Mumford's space; in particular  $S_{K^p}$  is of finite type over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ . Suppose that  $C = \text{End}_B(V)$  is a division algebra. In this case we will show that  $S_{K^p}$  is projective over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ , using the valuative criterion of properness. Let  $R$  be a discrete valuation ring over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  with fraction field  $K$  and residue field  $k$ , and let  $(A, \lambda, i, \bar{\eta})$  be a  $K$ -valued point of  $S_{K^p}$ . Consider the Néron model of  $A$  over  $R$ , which we still denote by  $A$ . We are free to replace  $K$  by a finite extension, so we may assume by Grothendieck's semistable reduction theorem that the identity component of the special fiber of  $A$  is an extension of an abelian variety by a torus  $T$ . The  $\mathbb{Q}$ -vector space  $X_*(T)_{\mathbb{Q}}$  is a  $B$ -module whose  $\mathbb{Q}$ -dimension is no bigger than half the  $\mathbb{Q}$ -dimension of  $V$  (since  $2 \dim(A) = \dim(V)$ ). Since the hypothesis that  $\text{End}_B(V)$  be a division algebra is equivalent to the hypothesis that  $V$  be a simple  $B$ -module, it follows that  $T$  is trivial and hence that the Néron model  $A$  is an abelian scheme over  $R$  (see Lemma 3 in §1 of [SeT]). It is immediate that  $\lambda$  and  $i$  extend to the Néron model, since  $\text{End}(A)$  and  $\text{Hom}(A, \widehat{A})$  are the same for  $R$  as they are for  $K$ ; clearly the extended  $\lambda$  is compatible with the extended  $i$ . In fact  $\lambda$  is a polarization of the Néron model. Indeed, we may suppose that  $\lambda$  comes from a line bundle  $\mathcal{L}$  on the Néron model of  $A$ , and that this line bundle is very ample on the general fiber. By Grothendieck's semicontinuity theorem the group of global sections of the pullback  $\mathcal{L}$  of  $\mathcal{L}$  to the geometric special fiber  $A_k$  does not vanish, and therefore the index of  $\mathcal{L}$  (in the sense of §16 of [M2]) is 0. But the results of §16 of [M2] imply that any nondegenerate line bundle of index 0 is ample (use the usual cohomological criterion for ampleness), which shows that  $\lambda$  is a polarization. The old  $\bar{\eta}$  still serves as a level structure on  $(A, \lambda, i)$  over  $R$ . Finally, it is obvious that  $(A, \lambda, i)$  satisfies the determinant condition over  $R$  (two polynomials over  $R$  are equal if and only if they are equal as polynomials over  $K$ ). Thus we have shown that  $(A, \lambda, i, \bar{\eta})$  extends to an  $R$ -valued point of  $S_{K^p}$ , which concludes the proof of properness.

## 6. HECKE CORRESPONDENCES AND $\lambda$ -ADIC SHEAVES

We retain the notation of §5. We only consider compact open subgroups  $K^p$  of  $G(\mathbb{A}_f^p)$  that are small enough so that the objects in the moduli problem have no nontrivial automorphisms. For any compact open subgroup  $K_1^p$  of  $K^p$  there is an étale covering  $S_{K_1^p} \rightarrow S_{K^p}$ , sending  $(A, \lambda, i, (\bar{\eta})_1)$  to  $(A, \lambda, i, \bar{\eta})$ , where  $(\bar{\eta})_1$  denotes the  $K_1^p$ -orbit of  $\bar{\eta}$ , and this covering map is Galois with Galois group  $K^p/K_1^p$  if  $K_1^p$  is normal in  $K^p$ . For  $g \in G(\mathbb{A}_f^p)$  there is an isomorphism  $S_{K^p} \rightarrow S_{g^{-1}K^p g}$  sending  $(A, \lambda, i, \bar{\eta})$  to  $(A, \lambda, i, \overline{\eta g})$ .

Let  $l$  be a prime different from  $p$ . Then any continuous  $l$ -adic repre-

sentation of  $G(\mathbb{A}_f^p)$  gives rise to smooth  $l$ -adic sheaves  $\mathcal{F}_{K^p}$  on  $S_{K^p}$  (use the restriction of the  $l$ -adic representation to  $K^p$  and the tower over  $S_{K^p}$  with Galois group  $K^p$  to construct  $\mathcal{F}_{K^p}$ ), and the pullback of  $\mathcal{F}_{K^p}$  under  $S_{K_1^p} \rightarrow S_{K^p}$  is canonically isomorphic to  $\mathcal{F}_{K_1^p}$  and the pullback of  $\mathcal{F}_{g^{-1}K^p g}$  under  $S_{K^p} \rightarrow S_{g^{-1}K^p g}$  is canonically isomorphic to  $\mathcal{F}_{K^p}$ ; of course this isomorphism depends on the element  $g$  and not just the subgroup  $g^{-1}K^p g$ .

We apply the construction above to the following  $l$ -adic representations. Let  $\xi$  be a finite-dimensional representation of  $G$  on a vector space over a number field  $L$ , and let  $\lambda$  be a place of  $L$  lying over  $l$ . Then  $\xi$  gives a  $\lambda$ -adic representation of  $G(\mathbb{Q}_l)$  and hence of  $G(\mathbb{A}_f^p)$  (use the projection map from  $G(\mathbb{A}_f^p)$  to  $G(\mathbb{Q}_l)$ ). We denote by  $\mathcal{F}$  the corresponding system of smooth  $\lambda$ -adic sheaves on the spaces  $S_{K^p}$ .

Let  $K^p$  be a sufficiently small compact open subgroup of  $G(\mathbb{A}_f^p)$  and let  $g \in G(\mathbb{A}_f^p)$ . Put  $K_g^p = K^p \cap gK^p g^{-1}$ . Then we get a Hecke correspondence from  $S_{K^p}$  to itself by taking

$$S_{K^p} \xleftarrow{a} S_{K_g^p} \xrightarrow{b} S_{K^p},$$

where the map  $a$  is the composition of the covering map  $S_{K^p} \leftarrow S_{g^{-1}(K_g^p)g}$  for the inclusion  $g^{-1}(K_g^p)g \subset K^p$  and the canonical isomorphism  $S_{g^{-1}(K_g^p)g} \xleftarrow{\sim} S_{K_g^p}$  induced by  $g$  and the map  $b$  is the covering map for the inclusion  $K_g^p \subset K^p$ .

This Hecke correspondence extends naturally to the sheaf  $\mathcal{F}_{K^p}$ . For this we need a canonical map from  $b^*\mathcal{F}_{K^p}$  to  $a^*\mathcal{F}_{K^p}$ ; since both pullbacks are canonically isomorphic to  $\mathcal{F}_{K_g^p}$ , we simply take the canonical isomorphism between the two pullbacks as our map.

## 7. STRUCTURE OF THE GROUPS $G$ AND $G_1$

We retain the notation of §5. In this section we discuss the structure of the groups  $G$  and  $G_1$ ; of course their structure depends on whether we are in Case A, C, or D (see §5 for this case division). In Cases A and C the group  $G$  is connected and reductive, while in Case D it is reductive with  $2^{[F_0 : \mathbb{Q}]}$  connected components. Moreover in Cases A and C the derived group of  $G$  is simply connected.

Later we will need information about the Hasse principle for  $H^1(\mathbb{Q}, G)$ . We write  $\ker^1(\mathbb{Q}, G)$  for the locally trivial elements in  $H^1(\mathbb{Q}, G)$ . In Case D the Hasse principle fails. In Cases A and C, we write  $D$  for the torus obtained as the quotient of  $G$  by its derived group and use the fact that  $\ker^1(\mathbb{Q}, G) = \ker^1(\mathbb{Q}, D)$  (see Lemma 4.3.1 of [K2]). In Case C the torus  $D$  is isomorphic to  $\mathbb{G}_m$ , and therefore  $G$  satisfies the Hasse principle. In Case A the group  $G_1$  is the restriction of scalars from  $F_0$  to  $\mathbb{Q}$  of an inner form of a quasi-split unitary group over  $F_0$  determined by the quadratic extension  $F/F_0$ ; we write  $n$  for the dimension of the Hermitian vector space giving rise to this unitary group. Then the torus  $D$  is the subtorus of  $F^\times \times \mathbb{Q}^\times$  defined by the condition  $N_{F/F_0}x = t^n$

( $x \in F^\times$ ,  $t \in \mathbb{Q}^\times$ ). If  $n$  is even, say  $n = 2k$ , then the torus  $D$  is isomorphic to  $D_1 \times \mathbb{Q}^\times$ , where  $D_1$  is the kernel of the norm homomorphism from  $F^\times$  to  $F_0^\times$ , the isomorphism being given by  $(x, t) \mapsto (xt^{-k}, t)$  for  $(x, t) \in D$ . Since the tori  $D_1$  and  $\mathbb{Q}^\times$  both satisfy the Hasse principle, the group  $G$  satisfies the Hasse principle in Case A if  $n$  is even. If  $n$  is odd, say  $n = 2k + 1$ , then  $D$  is isomorphic to the subtorus of  $F^\times$  consisting of elements whose norm down to  $F_0$  belongs to  $\mathbb{Q}^\times$ , the isomorphism being given by  $(x, t) \mapsto xt^{-k}$ . This torus need not satisfy the Hasse principle, and therefore  $G$  need not satisfy the Hasse principle in Case A if  $n$  is odd.

We now concentrate on Case A with  $n$  odd and show that the failure of the Hasse principle is of a harmless nature, in that it comes from the failure of the Hasse principle for the center  $Z$  of  $G$ . In fact we will show that the canonical map  $\ker^1(\mathbb{Q}, Z) \rightarrow \ker^1(\mathbb{Q}, G)$  is a bijection. We write  $Z_0$  for the center of the derived group of  $G$ . Then we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & Z_0 & \longrightarrow & Z & \longrightarrow & D & \longrightarrow 1 \\ & & \parallel & & \uparrow & & \uparrow \\ 1 & \longrightarrow & Z_0 & \longrightarrow & D_1 & \xrightarrow{n} & D_1 & \longrightarrow 1 \end{array}$$

the bottom row being the analog for  $G_1$  of the top row, the  $n$  over the arrow from  $D_1$  to  $D_1$  signifying that this map is given by  $x \mapsto x^n$ .

Let  $v$  be any place of  $\mathbb{Q}$ . Then  $H^1(\mathbb{Q}_v, D_1) = (F_0)_v^\times / N_{F/F_0}(F_v^\times)$ , which is killed by 2, and since  $n$  is odd, it follows that  $D_1 \xrightarrow{n} D_1$  induces an isomorphism  $H^1(\mathbb{Q}_v, D_1) \xrightarrow{n} H^1(\mathbb{Q}_v, D_1)$ . Therefore the map  $H^1(\mathbb{Q}_v, Z_0) \rightarrow H^1(\mathbb{Q}_v, D_1)$  is trivial, which implies that the map  $H^1(\mathbb{Q}_v, Z_0) \rightarrow H^1(\mathbb{Q}_v, Z)$  is trivial, which implies that  $H^1(\mathbb{Q}_v, Z) \rightarrow H^1(\mathbb{Q}_v, D)$  is injective. Moreover, since  $D_1$  satisfies the Hasse principle, the map  $H^1(\mathbb{Q}, Z_0) \rightarrow H^1(\mathbb{Q}, D_1)$  is also trivial, which implies that the map  $H^1(\mathbb{Q}, Z) \rightarrow H^1(\mathbb{Q}, D)$  is injective. This shows that  $\ker^1(\mathbb{Q}, Z) \rightarrow \ker^1(\mathbb{Q}, D)$  is injective.

It remains to show that  $\ker^1(\mathbb{Q}, Z) \rightarrow \ker^1(\mathbb{Q}, D)$  is surjective. Let  $d \in \ker^1(\mathbb{Q}, D)$ . The group  $\ker^2(\mathbb{Q}, Z_0)$  is trivial, since it is dual [T1] to  $\ker^1(\mathbb{Q}, X^*(Z_0))$ , which by Shapiro's lemma is isomorphic to a group of the form  $\ker^1(F_0, X)$ , where  $X$  is a  $\text{Gal}(\mathbb{Q}/F_0)$ -module on which  $\text{Gal}(\mathbb{Q}/F)$  acts trivially (as usual, use a place of  $F_0$  that remains prime in  $F$  to see that  $\ker^1(F_0, X) = \ker^1(F/F_0, X)$  is trivial). Therefore the image of  $d$  in  $H^2(\mathbb{Q}, Z_0)$  is trivial, which implies that there exists  $z \in H^1(\mathbb{Q}, Z)$  such that  $z \mapsto d$ . The injectivity of  $H^1(\mathbb{Q}_v, Z) \rightarrow H^1(\mathbb{Q}_v, D)$  shows that  $z \in \ker^1(\mathbb{Q}, Z)$ , as desired.

We will also need to understand conjugacy classes in  $G(K)$ , where  $K$  is an algebraically closed field containing  $\mathbb{Q}$ . For this we consider the obvious embedding  $i : G \hookrightarrow H$ , where  $H$  denotes the  $\mathbb{Q}$ -group  $C^\times$  (recall that  $C =$

$\text{End}_B(V)$ , as well as the homomorphism  $c: G \rightarrow \mathbb{G}_m$  that associates to  $g \in G(K)$  the scalar  $c(g) \in K^\times$  such that  $(gv, gw) = c(v, w)$  for all  $v, w \in V$ .

**Lemma 7.1.** *Two elements  $x, y$  of  $G(K)$  are conjugate if and only if  $c(x) = c(y)$  and  $i(x), i(y)$  are conjugate in  $H(K)$ .*

Suppose that  $c(x) = c(y)$  and that  $i(x), i(y)$  are conjugate in  $H(K)$ . We want to show that  $x, y$  are conjugate. Modifying  $x, y$  by the same scalar, we may assume that  $c(x) = c(y) = 1$ , so that  $x, y \in G_1(K)$ . Over  $K$  the groups  $G_1$  and  $H$  decompose as products of factors indexed by the embeddings of  $F_0$  in  $K$ . Thus we may reduce to the case in which  $G_1 \hookrightarrow H$  is of one of the three following types:

- (A)  $\mathbf{GL}_n \hookrightarrow \mathbf{GL}_n \times \mathbf{GL}_n$  (diagonal map),
- (C)  $\mathbf{Sp}_{2n} \hookrightarrow \mathbf{GL}_{2n}$ ,
- (D)  $\mathbf{O}_{2n} \hookrightarrow \mathbf{GL}_{2n}$ .

Case A is trivial and Cases C and D are dealt with in the fourth chapter of the article by Springer and Steinberg in [B] (for semisimple  $x, y$  one can simply look at Weyl group orbits on maximal tori of the groups  $G_1$  and  $H$ ).

Finally, we will also need several facts about the  $p$ -adic group  $G_{\mathbb{Q}_p}$ . To simplify notation we will temporarily write  $F, F_0, B, V, C$  for the objects over  $\mathbb{Q}_p$  obtained by extension of scalars from the previously considered objects over  $\mathbb{Q}$ , and we will also write  $\mathcal{O}_B$  for the  $p$ -adic completion of the previously considered  $\mathcal{O}_B$ . Because of the conditions imposed in §5 the  $\mathbb{Q}_p$ -algebra  $F$  is a finite product of finite unramified extensions of  $\mathbb{Q}_p$ , the algebra  $B$  is a matrix algebra over  $F$ , the order  $\mathcal{O}_B$  is a maximal order in  $B$  (hence is a matrix algebra over  $\mathcal{O}_F$ ), the involution  $*$  of  $B$  preserves  $\mathcal{O}_B$ , and there exists a self-dual  $\mathcal{O}_B$ -lattice  $\Lambda$  in  $V$  (by  $\mathcal{O}_B$ -lattice in  $V$  we mean a lattice that is an  $\mathcal{O}_B$ -submodule).

**Lemma 7.2.** *Let  $(V', (\cdot, \cdot)')$  be a nondegenerate skew-Hermitian  $B$ -module such that  $V'$  is isomorphic to  $V$  as  $B$ -module. Suppose that  $\Lambda'$  is a self-dual  $\mathcal{O}_B$ -lattice in  $V'$ . In Case D assume further that  $p \neq 2$  and that under the map*

$$H^1(\mathbb{Q}_p, G) \rightarrow H^1(\mathbb{Q}_p, G/G^0),$$

*the element of  $H^1(\mathbb{Q}_p, G)$  that measures the difference between  $V$  and  $V'$  is sent to the trivial element of  $H^1(\mathbb{Q}_p, G/G^0)$ . Then there exists an isomorphism  $\phi: V \rightarrow V'$  of skew-Hermitian  $B$ -modules such that  $\phi(\Lambda) = \Lambda'$ .*

Assume for the moment that the skew-Hermitian  $\mathcal{O}_B/p\mathcal{O}_B$ -modules  $\Lambda/p\Lambda$  and  $\Lambda'/p\Lambda'$  are isomorphic; later in the proof we will see that this assumption holds automatically. Choose an isomorphism  $\bar{\phi}: \Lambda/p\Lambda \rightarrow \Lambda'/p\Lambda'$  of skew-Hermitian  $\mathcal{O}_B/p\mathcal{O}_B$ -modules. Modifying the alternating form  $(\cdot, \cdot)'$  by a unit, we may assume that  $\bar{\phi}$  carries the alternating form on  $\Lambda'/p\Lambda'$  into the alternating form on  $\Lambda/p\Lambda$  (not just a scalar multiple of that form). Since the  $\mathcal{O}_B$ -module  $\Lambda$  is projective, there exists an  $\mathcal{O}_B$ -module map  $\phi_0: \Lambda' \rightarrow \Lambda$  whose reduction modulo  $p$  is  $\bar{\phi}$ , and it follows from Nakayama's lemma that  $\phi_0$  is

an isomorphism of  $\mathcal{O}_B$ -modules. We use  $\phi_0$  to identify  $V'$  with  $V$  and  $\Lambda'$  with  $\Lambda$ ; thus  $(\cdot, \cdot)'$  is now a second nondegenerate skew-Hermitian form on  $V$  for which  $\Lambda$  is self-dual, and the reduction of  $(\cdot, \cdot)'$  modulo  $p$  coincides with the reduction of  $(\cdot, \cdot)$  modulo  $p$ . Let  $C_0$  denote the maximal order  $\text{End}_{\mathcal{O}_B}(\Lambda)$  of  $C$ ; the involution  $*$  on  $C$  obtained from  $(\cdot, \cdot)$  preserves  $C_0$ . We want to find  $\psi \in C_0$  such that  $\text{id}_\Lambda + p\psi$  induces an isomorphism of skew-Hermitian  $\mathcal{O}_B/p^2\mathcal{O}_B$ -modules from  $(\Lambda/p^2\Lambda, (\cdot, \cdot))$  to  $(\Lambda/p^2\Lambda, (\cdot, \cdot)')$ . Let  $\rho$  be the unique element of  $C_0$  such that  $(v, w)' = (\rho v, w)$  for all  $v, w \in \Lambda$ . Of course  $\rho^* = \rho$ . The condition on  $\psi$  can be expressed as

$$(\rho - 1)/p \equiv \psi + \psi^* \pmod{p}.$$

If  $p \neq 2$ , it is obvious that this equation can be solved (take  $\psi$  to be  $\frac{1}{2}$  times the symmetric element  $(\rho - 1)/p$  of  $C_0$ ). If  $p = 2$  and we are in Case A, it is again obvious that this equation can be solved (use that the trace map from  $\mathbb{F}_{p^2}$  to  $\mathbb{F}_p$  is surjective). If  $p = 2$  and we are in Case C, it is not true that the map  $x \mapsto x + x^*$  from  $C_0/pC_0$  to  $(C_0/pC_0)_{\text{sym}}$  is surjective; however, it is true that its image contains  $(C_0)_{\text{sym}}/p(C_0)_{\text{sym}}$  (just look at dimensions, noting that the involution  $*$  on  $C_0/pC_0$  gives rise to a product of groups of type C over  $\mathbb{F}_p$ ).

Continuing this process for  $p^3, p^4, \dots$ , we eventually get  $\psi \in C_0$  such that  $\text{id}_\Lambda + p\psi$  is an isomorphism of skew-Hermitian  $\mathcal{O}_B$ -modules from  $(V, (\cdot, \cdot))$  to  $(V, (\cdot, \cdot)')$ . This proves the lemma under the assumption made at the beginning of the proof. In Cases A and C Lang's theorem implies that any two nondegenerate skew-Hermitian forms on  $\Lambda/p\Lambda$  are equivalent, and therefore the assumption we made holds automatically. In Case D we are dealing with a disconnected group, and we are not yet in a position to use Lang's theorem. However, applying what has been done already with  $\mathbb{Q}_p$  replaced by a sufficiently large finite unramified extension  $K$  of  $\mathbb{Q}_p$ , we see that the difference between  $V'$  and  $V$  can be represented by a 1-cocycle with values in  $G(\mathcal{O}_K)$ , where we are using the  $\mathbb{Z}_p$ -form of  $G$  determined by  $\Lambda$ . Since  $G(\mathcal{O}_K)$  meets every connected component of  $G(\mathbb{Q}_p)$ , the group  $G(\mathcal{O}_K)/G^0(\mathcal{O}_K)$  is isomorphic both to  $G(\mathbb{Q}_p)/G^0(\mathbb{Q}_p)$  and  $G(\mathbb{F}_p)/G^0(\mathbb{F}_p)$ , and the additional hypothesis we made in Case D implies that the difference between the skew-Hermitian  $\mathcal{O}_B$ -modules  $\Lambda/p\Lambda$  and  $\Lambda'/p\Lambda'$  comes from an element of  $H^1(\mathbb{F}_p, G^0(\mathbb{F}_p))$ , and this cohomology set is trivial by Lang's theorem. Therefore  $\Lambda/p\Lambda$  and  $\Lambda'/p\Lambda'$  are indeed isomorphic, and the proof of the lemma is complete.

**Corollary 7.3.** *In Case D assume that  $p \neq 2$ . Then  $G(\mathbb{Q}_p)$  acts transitively on the set of  $\mathcal{O}_B$ -lattices  $\Lambda'$  in  $V$  that are self-dual up to a scalar in  $\mathbb{Q}_p^\times$ .*

Apply Lemma 7.2 to  $(V, (\cdot, \cdot), \Lambda)$  and  $(V, c(\cdot, \cdot), \Lambda')$ , where  $c \in \mathbb{Q}_p^\times$  is chosen so that  $\Lambda'$  is self-dual with respect to  $c(\cdot, \cdot)$ .

We continue to work with  $p$ -adic objects  $F, F_0, B, V, C$ , and we again consider the embedding  $i : G \hookrightarrow H := C^\times$ . Let  $\Lambda$  be a self-dual  $\mathcal{O}_B$ -lattice in

$V$  and let  $K$  (respectively,  $K_H$ ) denote its stabilizer in  $G(\mathbb{Q}_p)$  (respectively,  $H(\mathbb{Q}_p)$ ).

**Lemma 7.4.** *Let  $x, y \in G(\mathbb{Q}_p)$ , and assume that  $K_H i(x) K_H = K_H i(y) K_H$ . Then  $KxK = KyK$ .*

First consider Cases A and C, so that  $G$  is connected. Let  $S$  be a maximal  $\mathbb{Q}_p$ -split torus in the quasi-split group  $G$  and  $\Omega_{\mathbb{Q}_p}$  be the relative Weyl group of  $S$ . Then the double cosets of  $K$  in  $G(\mathbb{Q}_p)$  are in one-to-one correspondence with the orbits of  $\Omega_{\mathbb{Q}_p}$  on  $X_*(S)$ , and the analogous statement holds for  $H$  as well. From the proof of Lemma (1.1.3) of [K1] we see that  $X_*(S) \otimes \mathbb{R}$  modulo  $\Omega_{\mathbb{Q}_p}$  injects into  $X_*(T) \otimes \mathbb{R}$  modulo  $\Omega$ , where  $T$  is the unique maximal torus of  $G$  containing  $S$  and  $\Omega$  is the absolute Weyl group of  $T$ . Let  $T_H$  be a maximal torus of  $H$  containing  $i(T)$  and let  $\Omega_H$  be its absolute Weyl group. It is enough to prove that if two elements  $x, y \in X := X_*(T) \otimes \mathbb{R}$  are such that  $i(x), i(y)$  are in the same orbit of  $\Omega_H$  in  $X_H := X_*(T_H) \otimes \mathbb{R}$ , then  $x, y$  are in the same orbit of  $\Omega$  in  $X$ . Modifying  $x, y$  by an element of the form  $j(z)$ , where  $z \in X_*(\mathbb{G}_m) \otimes \mathbb{R}$  and  $j$  is the obvious inclusion of  $\mathbb{G}_m$  in the center of  $G$ , we may assume that  $x, y \in X_1 := X_*(T \cap G_1) \otimes \mathbb{R}$ . In other words we can work with  $G_1 \hookrightarrow H$  rather than  $G \hookrightarrow H$ , which means that our problem decomposes as a product of problems of the form  $\mathbf{GL}_n \hookrightarrow \mathbf{GL}_n \times \mathbf{GL}_n$  (diagonal map) in Case A and of the form  $\mathbf{Sp}_{2n} \hookrightarrow \mathbf{GL}_{2n}$  in Case C. Thus Case A is trivial. In Case C note that every positive root for  $\mathbf{Sp}_{2n}$  is the restriction of a positive root for  $\mathbf{GL}_{2n}$ , so that the positive Weyl chamber for  $\mathbf{Sp}_{2n}$  is contained in the positive Weyl chamber for  $\mathbf{GL}_{2n}$ . This gives what we want, since the closure of any Weyl chamber is a fundamental domain for the action of the Weyl group.

Case D is a little more complicated. Let  $K^0 = K \cap G^0(\mathbb{Q}_p)$ . Then  $K^0 \backslash G^0(\mathbb{Q}_p) / K^0$  is in one-to-one correspondence with the orbits of the relative Weyl group  $\Omega_{\mathbb{Q}_p}^0$  of  $G^0$  on  $X_*(S)$ , where  $S$  denotes a maximal  $\mathbb{Q}_p$ -split torus in  $G^0$ . Since  $K$  meets every connected component of  $G$ , the map  $G^0(\mathbb{Q}_p) / K^0 \rightarrow G(\mathbb{Q}_p) / K$  is bijective, which implies that  $K \backslash G(\mathbb{Q}_p) / K$  is the quotient of  $K^0 \backslash G^0(\mathbb{Q}_p) / K^0$  by the conjugation action of  $K / K^0$  on that set. Let  $T$  denote the unique maximal torus of  $G^0$  containing  $S$ , let  $N_T$  denote the normalizer of  $T$  in  $G(\mathbb{Q}_p)$ , and let  $\Omega_{\mathbb{Q}_p}$  denote the quotient  $N_T / T(\mathbb{Q}_p)$ . Since both  $N_T$  and  $K$  meet every connected component of  $G$ , the groups  $K / K^0$  and  $\Omega_{\mathbb{Q}_p} / \Omega_{\mathbb{Q}_p}^0$  are equal, and we see that the double cosets  $K \backslash G(\mathbb{Q}_p) / K$  are in one-to-one correspondence with the orbits of  $\Omega_{\mathbb{Q}_p}$  on  $X_*(S)$ .

It is again true that  $X_*(S) \otimes \mathbb{R}$  modulo  $\Omega_{\mathbb{Q}_p}$  injects into  $X_*(T) \otimes \mathbb{R}$  modulo the absolute analog  $\Omega$  of  $\Omega_{\mathbb{Q}_p}$ . It is enough to check this for  $G_1$  rather than  $G$ , and then the problem reduces to checking the following assertion: for a quasi-split orthogonal group  $G$  in  $2n$  variables over a field  $E$  the set  $X_*(S) \otimes \mathbb{R}$  modulo  $\Omega_E$  injects into  $X_*(T) \otimes \mathbb{R}$  modulo  $\Omega$ . If  $G^0$  is split, the assertion is trivial. Otherwise  $G^0$  splits over a quadratic extension  $E'$  of  $E$ , and the

nontrivial element of  $\text{Gal}(E'/E)$  acts on  $X_*(T) \otimes \mathbb{R}$  by the unique nontrivial element  $\omega_1$  of  $\Omega$  that preserves the positive Weyl chamber of  $X_*(T) \otimes \mathbb{R}$  (pick a Borel subgroup of  $G^0$  over  $E$  containing  $T$ ). The element  $\omega_1$  is of order 2, and  $\Omega$  is the semidirect product of  $\{1, \omega_1\}$  and  $\Omega^0$  (of course  $\Omega^0$  denotes the absolute Weyl group of  $T$  in  $G^0$ ). The subspace  $X_*(S) \otimes \mathbb{R}$  of  $X_*(T) \otimes \mathbb{R}$  is equal to the set of fixed points of  $\omega_1$ . Now let  $x, y \in X_*(S) \otimes \mathbb{R}$  and suppose that  $x, y$  are in the same orbit of  $\Omega$  on  $X_*(T) \otimes \mathbb{R}$ , say  $y = \omega \omega_1^j x$  for  $\omega \in \Omega^0$  and  $j = 0$  or 1. Since  $\omega_1$  fixes  $x$ , we have  $y = \omega x$ . Again from the proof of Lemma (1.1.3) of [K1] we see that  $y, x$  belong to the same orbit of  $\Omega_E^0$  on  $X_*(S) \otimes \mathbb{R}$ , as we wanted to show.

Thus we need to examine the embedding  $\mathbf{O}_{2n} \hookrightarrow \mathbf{GL}_{2n}$  over an algebraically closed field. Letting  $T$  (respectively,  $T_H$ ) denote a maximal torus in  $\mathbf{O}_{2n}$  (respectively, a maximal torus in  $\mathbf{GL}_{2n}$  containing  $T$ ), we must show that  $X_*(T) \otimes \mathbb{R}$  modulo the Weyl group  $\Omega$  of  $\mathbf{O}_{2n}$  injects into  $X_*(T_H) \otimes \mathbb{R}$  modulo the Weyl group  $\Omega_H$  of  $\mathbf{GL}_{2n}$ . But the map  $X_*(T) \rightarrow X_*(T_H)$  from the  $\Omega$ -module  $X_*(T)$  to the  $\Omega_H$ -module  $X_*(T_H)$  is isomorphic to the analogous map for  $\mathbf{Sp}_{2n} \hookrightarrow \mathbf{GL}_{2n}$  (the Weyl group for the disconnected group  $\mathbf{O}_{2n}$  is isomorphic to the Weyl group for  $\mathbf{Sp}_{2n}$ ), and for this map we have already seen that the desired injectivity holds.

*Remark 7.5.* In Lemma 7.2, Corollary 7.3, and Lemma 7.4 the base field  $\mathbb{Q}_p$  can be replaced by any unramified extension of  $\mathbb{Q}_p$ .

## 8. COMPLEX POINTS OF MODULI SPACES OF PEL TYPE

We retain the notation of §5. If we are in Case D we assume that  $p \neq 2$ . We consider the set of complex points  $S_{K^p}(\mathbb{C})$  of  $S_{K^p}$  relative to the map  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} \rightarrow \mathbb{C}$  induced by the inclusion  $E \subset \mathbb{C}$ . Thus we are interested in quadruples  $(A, \lambda, i, \bar{\eta})$  satisfying the determinant condition, where  $A$  is now an abelian variety over  $\mathbb{C}$  up to prime-to- $p$  isogeny. The homology group  $H := H_1(A, \mathbb{Q})$  is a skew-Hermitian  $B$ -module, the  $B$ -action coming from  $i$  and the alternating form coming from  $\lambda$ ; since it is necessary to choose a square root of  $-1$  in  $\mathbb{C}$  in order to regard the alternating form as being  $\mathbb{Q}$ -valued, the form is only well determined up to scalars.

We claim that for every place  $v$  of  $\mathbb{Q}$  the skew-Hermitian  $B_{\mathbb{Q}_v}$ -modules  $H_{\mathbb{Q}_v}$  and  $V_{\mathbb{Q}_v}$  are isomorphic. For finite places  $v$  different from  $p$  this is an immediate consequence of the existence of  $\bar{\eta}$ .

In particular, considering any single finite place  $v$  different from  $p$ , we see that the  $B$ -modules  $H$  and  $V$  are isomorphic. Therefore the  $B_{\mathbb{R}}$ -modules  $H_{\mathbb{R}}$  and  $V_{\mathbb{R}}$  are isomorphic, and the same is true of the  $B_{\mathbb{C}}$ -modules  $H_{\mathbb{C}}$  and  $V_{\mathbb{C}}$ . Recall that we have decomposed  $V_{\mathbb{C}}$  as  $V_1 \oplus V_2$ , a decomposition as  $B_{\mathbb{C}} \otimes_{\mathbb{R}} \mathbb{C}$ -module, where we use  $h$  to give  $V_{\mathbb{R}}$  a complex structure. The natural complex structure on  $H_{\mathbb{R}} = \text{Lie}(A)$  allows us to do the same for  $H_{\mathbb{C}}$ , obtaining a decomposition  $H_{\mathbb{C}} = H_1 \oplus H_2$ . The determinant condition  $f = g$  satisfied by  $(A, i)$  implies that  $H_1$  and  $V_1$  are isomorphic  $B_{\mathbb{C}}$ -modules; this, together with the

fact that  $H_{\mathbb{C}}$  and  $V_{\mathbb{C}}$  are isomorphic  $B_{\mathbb{C}}$ -modules, implies that  $H_{\mathbb{R}}$  and  $V_{\mathbb{R}}$  are isomorphic  $B_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}$ -modules. Lemma 4.2 then implies that  $H_{\mathbb{R}}$  and  $V_{\mathbb{R}}$  are isomorphic skew-Hermitian  $B_{\mathbb{R}}$ -modules.

It remains to consider the place  $v = p$ . In this case we simply apply Lemma 7.2. We must check that the hypotheses of that lemma are satisfied. First of all, note that the  $B_{\mathbb{Q}_p}$ -modules  $V_{\mathbb{Q}_p}$  and  $H_{\mathbb{Q}_p}$  are isomorphic. Next, since  $A$  is an abelian variety up to prime-to- $p$  isogeny, the  $\mathbb{Z}_p$ -module  $\Lambda' := H_1(A, \mathbb{Z}_p)$  is well defined and gives us a self-dual  $\mathcal{O}_B$ -lattice in  $H_{\mathbb{Q}_p}$ . Finally, if we are in Case D, there are two further conditions to check. One is that  $p \neq 2$ ; we made this assumption at the beginning of this section. To check the second condition, we consider the element  $g \in H^1(\mathbb{Q}, G)$  that measures the difference between  $V$  and  $H$ . We already know that  $g$  is locally trivial for all places  $v \neq p$ . Therefore the image of  $g$  in  $H^1(\mathbb{Q}, G/G^0)$  is locally trivial except possibly at  $v = p$ . But by Shapiro's lemma  $H^1(\mathbb{Q}, G/G^0)$  is equal to  $H^1(F_0, \{\pm 1\})$ , and the latter group is just the group of characters on the idele class group of  $F_0$  with values in  $\{\pm 1\}$ . By the weak approximation theorem for the ideles of  $F_0$  any such character that is trivial at all but a finite number of places of  $F_0$  is trivial. Therefore the image of  $g$  in  $H^1(\mathbb{Q}, G/G^0)$  is trivial, which implies that the last hypothesis of Lemma 7.2 is indeed satisfied.

Isomorphism classes of skew-Hermitian  $B$ -modules of the same dimension as  $V$  are classified by  $H^1(\mathbb{Q}, G)$ , and therefore by [BS] there are finitely many isomorphism classes of skew-Hermitian  $B$ -modules  $(V', (\cdot, \cdot)')$  such that  $V'_{\mathbb{Q}_v}$  and  $V_{\mathbb{Q}_v}$  are isomorphic for all places  $v$  of  $\mathbb{Q}$ ; we choose representatives  $V^{(1)}, \dots, V^{(m)}$  in these isomorphism classes, and for each one we fix local isomorphisms  $V_{\mathbb{Q}_v}^{(i)} \simeq V_{\mathbb{Q}_v}$  for all places  $v$  of  $\mathbb{Q}$ . We denote by  $G^{(i)}$  the group of automorphisms of  $V^{(i)}$ . The local isomorphisms we just chose induce local isomorphisms  $G_{\mathbb{Q}_v}^{(i)} \simeq G_{\mathbb{Q}_v}$  for all  $v$ . The set  $S_{K^p}(\mathbb{C})$  is a disjoint union  $\coprod_{i=1}^m S_{K^p}(\mathbb{C})^{(i)}$ , where  $S_{K^p}(\mathbb{C})^{(i)}$  consists of quadruples  $(A, \lambda, i, \bar{\eta})$  such that  $H$  is isomorphic to  $V^{(i)}$ , and it is enough to describe each set  $S_{K^p}(\mathbb{C})^{(i)}$ .

We may assume that  $V^{(1)}$  is  $V$  itself and start by describing  $S_{K^p}(\mathbb{C})^{(1)}$ . Consider a point  $(A, \lambda, i, \bar{\eta})$  of  $S_{K^p}(\mathbb{C})^{(1)}$  and choose an isomorphism between  $H$  and  $V$ . Then giving  $\bar{\eta}$  is equivalent to giving an element of  $G(\mathbb{A}_f^p)/K^p$ . The complex structure on  $H_{\mathbb{R}} = \text{Lie}(A)$  becomes a complex structure on  $V_{\mathbb{R}}$  and yields a homomorphism  $h' : \mathbb{C} \rightarrow C_{\mathbb{R}}$ . It follows from Lemma 4.2 that  $h'$  belongs to the set  $X_{\infty}$  of  $G(\mathbb{R})$ -conjugates of  $h$  (recall that we have already shown that  $H_{\mathbb{R}}$  and  $V_{\mathbb{R}}$  are isomorphic  $B_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}$ -modules). The self-dual  $\mathcal{O}_B$ -lattice  $\Lambda'$  becomes an  $\mathcal{O}_B$ -lattice (still denoted  $\Lambda'$ ) in  $V_{\mathbb{Q}_p}$ , and it is self-dual up to a scalar (in other words, it is self-dual for some scalar multiple of  $(\cdot, \cdot)$ ). Choose a self-dual  $\mathcal{O}_B$ -lattice  $\Lambda_0$  in  $V_{\mathbb{Q}_p}$ , and let  $K_p$  denote its stabilizer in  $G(\mathbb{Q}_p)$ . Corollary 7.3 tells us that there exists  $g \in G(\mathbb{Q}_p)$  such that  $\Lambda' = g\Lambda_0$ , and  $g$  determines a well-defined element of  $G(\mathbb{Q}_p)/K_p$ . Put  $K = K_p \cdot K^p$ , a compact open subgroup

of  $G(\mathbb{A}_f)$ . Then our choice of isomorphism between  $H$  and  $V$  has given us a well-defined element of  $(G(\mathbb{A}_f)/K) \times X_\infty$ . The group  $G(\mathbb{A}) = G(\mathbb{A}_f) \times G(\mathbb{R})$  acts in an obvious way on the left of  $(G(\mathbb{A}_f)/K) \times X_\infty$ , as does the subgroup  $G(\mathbb{Q})$  of  $G(\mathbb{A})$ . Any two isomorphisms between  $H$  and  $V$  differ by an automorphism of  $V$ , or in other words by an element of  $G(\mathbb{Q})$ , and the corresponding elements of  $(G(\mathbb{A}_f)/K) \times X_\infty$  are in the same  $G(\mathbb{Q})$ -orbit. Therefore  $(A, \lambda, i, \bar{\eta})$  gives rise to a well-defined element of the quotient  $G(\mathbb{Q}) \backslash ((G(\mathbb{A}_f)/K) \times X_\infty)$ . The theory of abelian varieties over  $\mathbb{C}$  shows that this construction yields a bijection from  $S_{K^p}(\mathbb{C})^{(1)}$  to  $G(\mathbb{Q}) \backslash ((G(\mathbb{A}_f)/K) \times X_\infty)$ . Replacing  $V$  by  $V^{(i)}$ , we get a bijection from  $S_{K^p}(\mathbb{C})^{(i)}$  to  $G^{(i)}(\mathbb{Q}) \backslash ((G(\mathbb{A}_f)/K) \times X_\infty)$  (of course we are using our local isomorphisms  $G_{\mathbb{Q}_v}^{(i)} \simeq G_{\mathbb{Q}_v}$  to make  $G^{(i)}(\mathbb{Q})$  act on  $(G(\mathbb{A}_f)/K) \times X_\infty$ ).

Now we apply the discussion at the beginning of §7; in particular in Case A we again have the integer  $n$  introduced in §7. In Case D the situation is complicated in two ways: the group  $G$  has  $2^{[F_0 : \mathbb{Q}]}$  connected components and does not satisfy the Hasse principle. In Case C and in Case A with  $n$  even, the situation is simple:  $G$  is connected and satisfies the Hasse principle.

It remains to discuss Case A with  $n$  odd. In this case we have seen in §7 that  $\ker^1(\mathbb{Q}, Z) \rightarrow \ker^1(\mathbb{Q}, G)$  is a bijection. Using that  $Z$  is the kernel of the map  $F^\times \times \mathbb{Q}^\times \rightarrow F_0^\times$  sending  $(x, t)$  to  $(N_{F/F_0}x)t^{-1}$ , we see that  $H^1(\mathbb{Q}, Z) = F_0^\times / \mathbb{Q}^\times N_{F/F_0}(F^\times)$  and that  $H^1(\mathbb{Q}, Z(\bar{\mathbb{A}})) = \mathbb{A}_{F_0}^\times / \mathbb{A}_{\mathbb{Q}}^\times N_{F/F_0}(\mathbb{A}_F^\times)$ . Let  $z$  belong to  $\ker^1(\mathbb{Q}, Z)$  and represent  $z$  by an element  $\alpha \in F_0^\times$ . Choose, for each place  $v$  of  $\mathbb{Q}$ , an element  $\beta_v \in F_v^\times$  such that  $\alpha N_{F/F_0} \beta_v \in \mathbb{Q}_v^\times$ . Modifying the representative  $\alpha$  by an element of  $\mathbb{Q}^\times N_{F/F_0}(F^\times)$ , we may assume that  $\alpha$  is totally positive and that it is a unit at every place of  $F$  lying over  $p$ . Define an automorphism of  $S_{K^p}$  by sending an  $S$ -valued point  $(A, \lambda, i, \bar{\eta})$  to the point  $(A, \lambda \circ i(\alpha), i, \overline{\beta \eta})$ , where  $\beta$  is the element of  $(\mathbb{A}_f^p \otimes_{\mathbb{Q}} F)^\times$  whose component in  $F_l$  is  $\beta_l$  for every prime  $l$  different from  $p$ . This automorphism of  $S_{K^p}$  depends on  $\beta$  as well as  $\alpha$ . Varying  $K^p$ , we get an automorphism of the projective system  $S_{K^p}$ , and this automorphism commutes with the action of  $G(\mathbb{A}_f^p)$  on the projective system. Since the  $\lambda$ -adic sheaves in §6 are constructed in a formal way from this projective system, the automorphism is compatible with these sheaves as well.

The subvarieties  $S_{K^p}^{(1)}, \dots, S_{K^p}^{(m)}$  of the  $E$ -variety  $S_{K^p}$  are defined over  $E$ ; in fact each one is a canonical model for the Shimura variety obtained from the data  $(G, h^{-1}, K^p)$ . Let  $z_i$  be the element of  $\ker^1(\mathbb{Q}, Z)$  mapping to the element of  $\ker^1(\mathbb{Q}, G)$  determined by the skew-Hermitian  $B$ -module  $V^{(i)}$ . Then any one of the automorphisms of  $S_{K^p}$  associated to  $z_i$  maps  $S_{K^p}^{(1)}$  isomorphically to  $S_{K^p}^{(i)}$ , compatibly with the action of  $G(\mathbb{A}_f^p)$  on the projective system  $S_{K^p}$  and with the  $\lambda$ -adic sheaves on these spaces. Therefore our moduli space over  $E$  is just a disjoint union of  $|\ker^1(\mathbb{Q}, G)|$  copies of the canonical model  $S_{K^p}^{(1)}$  for  $(G, h^{-1}, K^p)$ .

### 9. $R$ -ISOGENIES, SYMMETRIZATIONS, AND POLARIZATIONS

Let  $k$  be a field and consider the category of abelian varieties over  $k$ . For any commutative ring  $R$  with 1 we can also consider the  $R$ -linear category of abelian varieties up to  $R$ -isogeny: its objects are abelian varieties over  $k$  and the  $R$ -module of homomorphisms from  $A$  to  $B$  is  $\text{Hom}(A, B) \otimes_{\mathbb{Z}} R$ , where  $\text{Hom}(A, B)$  is the  $\mathbb{Z}$ -module of  $k$ -homomorphisms from  $A$  to  $B$ . An  $R$ -isogeny from  $A$  to  $B$  is an isomorphism in the category of abelian varieties up to  $R$ -isogeny. The functor  $A \mapsto \widehat{A}$  ( $\widehat{A}$  denotes the abelian variety dual to  $A$ ) extends to the category of abelian varieties up to  $R$ -isogeny. For any  $f \in \text{Hom}(A, B) \otimes R$  and any  $\lambda \in \text{Hom}(B, \widehat{B}) \otimes R$  we write  $f^*(\lambda)$  for  $\widehat{f}\lambda f \in \text{Hom}(A, \widehat{A}) \otimes R$ .

An  $R$ -symmetrization of an abelian variety  $A$  is a symmetric  $R$ -isogeny  $\lambda: A \rightarrow \widehat{A}$  (symmetric meaning that  $\widehat{\lambda} = \lambda$ ). Suppose that  $R$  is a subring of  $\mathbb{R}$ . An  $R$ -polarization of  $A$  is an  $R$ -symmetrization  $\lambda: A \rightarrow \widehat{A}$  that is positive in the following sense: the image of  $\lambda$  in  $\text{Hom}(A, \widehat{A}) \otimes \mathbb{R}$  is a linear combination with strictly positive coefficients of elements  $\phi_{\mathcal{L}} \in \text{Hom}(A, \widehat{A})$  coming from ample line bundles  $\mathcal{L}$  on  $A$  (see [M2] for the definition of  $\phi_{\mathcal{L}}$  and a discussion of its properties). Let  $E$  denote the  $\mathbb{R}$ -algebra  $\text{End}(A) \otimes \mathbb{R}$ . Then  $E^\times$  acts on the right of the  $\mathbb{R}$ -vector space  $V$  of symmetric elements in  $\text{Hom}(A, \widehat{A}) \otimes \mathbb{R}$  (for  $f \in E^\times$  and  $\lambda \in V$  the action is given by  $\lambda \mapsto f^*(\lambda)$ ). Looking at §21 of [M2] (especially Application III), we see that the set of  $\mathbb{R}$ -polarizations in  $V$  is a nonempty open convex cone in  $V$  and that  $E^\times$  preserves this cone and acts transitively on it.

Let  $B$  be a semisimple finite-dimensional  $\mathbb{Q}$ -algebra and let  $*$  be a positive involution on  $B$ . Let  $R$  be a  $\mathbb{Q}$ -algebra. By a  $B$ -abelian variety up to  $R$ -isogeny we mean an abelian variety  $A$  up to  $R$ -isogeny plus a  $\mathbb{Q}$ -algebra homomorphism  $i: B \rightarrow \text{End}(A)$ . These form an  $R$ -linear category; we write  $\text{Hom}_B(A_1, A_2)$  for the  $R$ -module of  $B$ -homomorphisms from  $A_1$  to  $A_2$ . The dual  $\widehat{A}$  to a  $B$ -abelian variety up to  $R$ -isogeny is naturally a  $B$ -abelian variety up to  $R$ -isogeny, the homomorphism  $B \rightarrow \text{End}(\widehat{A})$  being given by the composition  $B \xrightarrow{*} B \xrightarrow{i} \text{End}(A) \rightarrow \text{End}(\widehat{A})$ . An  $R$ -symmetrization of a  $B$ -abelian variety  $A$  up to  $R$ -isogeny is an  $R$ -symmetrization of the underlying abelian variety up to  $R$ -isogeny that is at the same time a  $B$ -homomorphism (that is, an element of  $\text{Hom}_B(A, \widehat{A})$ ). Any  $R$ -symmetrization  $\lambda$  of the underlying abelian variety  $A$  determines a Rosati involution  $f \mapsto \iota_\lambda(f) := \lambda^{-1}\widehat{f}\lambda$  on  $\text{End}(A)$ , and it is immediate that  $\lambda$  is an  $R$ -symmetrization of the  $B$ -abelian variety  $A$  if and only if  $i$  is a  $*$ -homomorphism for  $*$  on  $B$  and  $\iota_\lambda$  on  $\text{End}(A)$ .

**Lemma 9.1.** *Let  $A$  be an abelian variety up to  $\mathbb{R}$ -isogeny and let  $W$  be the real vector space of symmetric elements ( $f = \widehat{f}$ ) in  $\text{Hom}_B(A, \widehat{A})$ . Then the set of  $\mathbb{R}$ -polarizations of the  $B$ -abelian variety  $A$  is a nonempty open convex cone in  $W$ . Let  $E$  be the  $\mathbb{R}$ -algebra  $\text{End}_B(A)$ . Then  $E^\times$  acts on the right of  $W$  by the rule  $\lambda \mapsto \widehat{f}\lambda f$  ( $\lambda \in W$ ,  $f \in E^\times$ ), and this action is transitive.*

First we show that the set of  $\mathbb{R}$ -polarizations of the  $B$ -abelian variety  $A$  is

nonempty. Let  $\lambda$  be an  $\mathbb{R}$ -polarization of the underlying abelian variety  $A$ , and let  $\iota_\lambda$  be the corresponding Rosati involution on the  $\mathbb{R}$ -algebra  $C := \text{End}(A)$ . By Lemma 2.10 there exists  $c \in C^\times$  such that  $\text{Int}(c) \circ i$  is a  $*$ -homomorphism for  $*$  on  $B$  and  $\iota_\lambda$  on  $C$ . It follows that  $i$  is a  $*$ -homomorphism for  $*$  on  $B$  and the Rosati involution for the  $\mathbb{R}$ -polarization  $c^*(\lambda) = \widehat{c}\lambda c$  of  $A$ . Therefore  $c^*(\lambda)$  is an  $\mathbb{R}$ -polarization of the  $B$ -abelian variety  $A$ .

Now fix an  $\mathbb{R}$ -polarization  $\lambda$  of the  $B$ -abelian variety  $A$ . Write  $*$  for the Rosati involution of  $C = \text{End}(A)$  determined by  $\lambda$ , and note that  $*$  preserves the subalgebra  $E = \text{End}_B(A)$  of  $C$ . Therefore  $*$  induces a positive involution on  $E$ . The map  $x \mapsto \lambda x$  identifies  $E_{\text{sym}}$  (respectively,  $C_{\text{sym}}$ ) with  $W$  (respectively, the real vector space  $V$  of symmetric elements of  $\text{Hom}(A, \widehat{A})$ ). This identifies the set of  $\mathbb{R}$ -polarizations of the abelian variety  $A$  with  $C_+$  and the set of  $\mathbb{R}$ -polarizations of the  $B$ -abelian variety  $A$  with  $E \cap C_+$ . Since  $E \cap C_+ = E_+$  by Lemma 2.9, the rest of Lemma 9.1 follows from Lemma 2.8.

**Lemma 9.2.** *Let  $A$  be an abelian variety up to  $\mathbb{Q}$ -isogeny. Then there exists a  $\mathbb{Q}$ -polarization of the  $B$ -abelian variety  $A$ .*

Let  $W$  be the  $\mathbb{Q}$ -vector space of symmetric elements in  $\text{Hom}_B(A, \widehat{A})$ . The set of  $\mathbb{R}$ -polarizations of the  $B$ -abelian variety  $A$  is a nonempty open subset of  $W_{\mathbb{R}}$  by Lemma 9.1. Since  $W$  is dense in  $W_{\mathbb{R}}$ , there exists an element of  $W$  that is an  $\mathbb{R}$ -polarization; it is the desired  $\mathbb{Q}$ -polarization of the  $B$ -abelian variety  $A$ .

## 10. VIRTUAL ABELIAN VARIETIES OVER FINITE FIELDS

Let  $\bar{k}$  be an algebraic closure of  $\mathbb{F}_p$ , let  $\sigma$  be the Frobenius automorphism  $x \mapsto x^p$  of  $\bar{k}$ , and for any positive integer  $r$  denote by  $k_r$  the fixed field of  $\sigma^r$  on  $\bar{k}$ , so that  $k_r$  is a field with  $p^r$  elements. By a virtual abelian variety  $A$  over  $k_r$  up to prime-to- $p$  isogeny we will mean a pair  $(\bar{A}, u)$  consisting of an abelian variety  $\bar{A}$  over  $\bar{k}$  up to prime-to- $p$  isogeny and a prime-to- $p$  isogeny  $u : \sigma^r(\bar{A}) \rightarrow \bar{A}$ . We define the dimension  $\dim(A)$  of  $A$  to be  $\dim(\bar{A})$ . Of course a homomorphism from  $A_1$  to  $A_2$  is a homomorphism  $f : \bar{A}_1 \rightarrow \bar{A}_2$  such that  $fu_1 = u_2\sigma^r(f)$ . We define the Frobenius element  $\pi_A \in \text{End}(\bar{A})$  by  $\pi_A := u \circ \Phi_r$ , where  $\Phi_r$  is the Frobenius morphism  $\Phi_r : \bar{A} \rightarrow \sigma^r(\bar{A})$ . The condition  $fu_1 = u_2\sigma^r(f)$  is equivalent to the condition  $f\pi_1 = \pi_2f$ ; in particular  $\text{End}(A)$  is the centralizer of  $\pi_A$  in  $\text{End}(\bar{A})$ , which implies that  $\pi_A$  belongs to the center of  $\text{End}(A)$ .

Any abelian variety  $A$  over  $k_r$  gives us a pair  $(\bar{A}, u)$ , where  $\bar{A} = A_{\bar{k}}$  and  $u$  is the isomorphism  $\sigma^r(\bar{A}) \rightarrow \bar{A}$  determined by the  $k_r$ -structure on  $\bar{A}$ . In this way the category of abelian varieties over  $k_r$  up to prime-to- $p$  isogeny is equivalent to a full subcategory of the category of virtual abelian varieties over  $k_r$  up to prime-to- $p$  isogeny. The notions of Frobenius endomorphism in the two categories coincide.

In this section we will be concerned with the category  $\mathcal{V}_r$  of virtual abelian varieties over  $k_r$  up to isogeny: it has the same objects as the category of virtual abelian varieties over  $k_r$  up to prime-to- $p$  isogeny, but a homomorphism from

$A_1$  to  $A_2$  is now an element  $f \in \text{Hom}(\bar{A}_1, \bar{A}_2)_{\mathbb{Q}}$  such that  $f\pi_1 = \pi_2 f$ .

Let  $s$  be a positive integer. There is a functor (base change) from  $\mathcal{V}$  to  $\mathcal{V}_{rs}$  sending  $A = (\bar{A}, u)$  to  $(\bar{A}, u\sigma^r(u)\cdots\sigma^{r(s-1)}(u))$ . The Frobenius element for the base change of  $A$  is the  $s$ th power of  $\pi_A$ . There is also a functor (Weil's restriction of scalars) from  $\mathcal{V}_{rs}$  to  $\mathcal{V}$  sending  $A = (\bar{A}, u)$  to  $(\bar{B}, v)$ , where  $\bar{B} = \bar{A} \times \sigma^r(\bar{A}) \times \cdots \times \sigma^{r(s-1)}(\bar{A})$  and  $v(a_0, \dots, a_{s-1}) = (u(a_{s-1}), a_0, \dots, a_{s-2})$ . In the category of abelian varieties over  $\bar{k}$  up to isogeny  $\bar{B}$  is  $\bar{A}^s$  (use the isogenies  $\Phi_{kr} : \bar{A} \rightarrow \sigma^{kr}(\bar{A})$ ) and the Frobenius element for  $(\bar{B}, v)$  is the element of  $\text{End}(\bar{B})_{\mathbb{Q}} = \mathbf{M}_s(\text{End}(\bar{A})_{\mathbb{Q}})$  given by the  $(s \times s)$ -matrix all of whose entries are 0 except for the upper right-hand entry, which is  $\pi_A$ , and the entries just under the main diagonal, all  $s - 1$  of which are 1.

Let  $A = (\bar{A}, u)$  be a virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny. For any prime  $l$  different from  $p$  we denote by  $H_1(\bar{A}, \mathbb{Q}_l)$  the Tate  $\mathbb{Q}_l$ -module of  $\bar{A}$ , and we denote by  $H_1(\bar{A}, \mathbb{A}_f^p)$  the Tate  $\mathbb{A}_f^p$ -module of  $\bar{A}$ . Of course the endomorphism  $\pi_A$  of  $\bar{A}$  acts on these modules.

The analogous  $p$ -adic construction requires a little more work. Let  $L$  denote the fraction field of the Witt ring  $W(\bar{k})$ . As usual we write  $\sigma$  for the automorphism of  $L$  induced by the automorphism  $\sigma$  of  $\bar{k}$ . For any positive integer  $r$  we denote by  $L_r$  the fixed field of  $\sigma^r$  on  $L$ , or, in other words, the fraction field of the Witt ring  $W(k_r)$ . We write  $\bar{\Lambda}$  for the  $W(\bar{k})$ -module dual to  $H_{\text{cris}}^1(\bar{A}/W(\bar{k}))$  and  $\bar{H}$  for its tensor product over  $W(\bar{k})$  with  $L$ . The usual  $\sigma$ -linear operator on  $H_{\text{cris}}^1(\bar{A}/W(\bar{k}))$  induces a  $\sigma$ -linear operator  $\Phi$  on  $\bar{H}$  such that  $\Phi(\bar{\Lambda}) \supset \bar{\Lambda}$ , and  $\Phi(\bar{\Lambda})/\bar{\Lambda}$  is isomorphic as  $W(\bar{k})$ -module to  $\bar{k}^{\dim(\bar{A})}$ . The prime-to- $p$  isogeny  $u$  induces a linear isomorphism  $u : \sigma^r(\bar{\Lambda}) \rightarrow \bar{\Lambda}$ , where  $\sigma^r(\bar{\Lambda})$  denotes the  $W(\bar{k})$ -module obtained from  $\bar{\Lambda}$  by extension of scalars for the homomorphism  $\sigma^r : W(\bar{k}) \rightarrow W(\bar{k})$ ; equivalently, we may view  $u$  as a  $\sigma^r$ -linear bijection from  $\bar{\Lambda}$  to itself. Put  $\Lambda = \{x \in \bar{\Lambda} | ux = x\}$  and  $H = \{x \in \bar{H} | ux = x\}$ . Then  $\Lambda$  is a  $W(k_r)$ -lattice in the  $L_r$ -vector space  $H$ , and the canonical map  $H \otimes_{L_r} L \rightarrow \bar{H}$  is an isomorphism (use that  $u(\bar{\Lambda}) = \bar{\Lambda}$  and then use the fact that any element of  $\text{GL}_n(W(\bar{k}))$  is  $\sigma^r$ -conjugate to the identity). Since  $\Phi$  commutes with  $u$ , it preserves the subspace  $H$  of  $\bar{H}$  and hence induces a  $\sigma$ -linear bijection  $H \rightarrow H$ . Moreover  $\Phi(\Lambda)$  contains  $\Lambda$ , and  $\Phi(\Lambda)/\Lambda$  is isomorphic as  $W(k_r)$ -module to  $k_r^{\dim(\bar{A})}$ . The triple  $(H, \Lambda, \Phi)$  is functorial in  $A$ ; in particular  $\pi_A$  induces endomorphisms of  $H$  and  $\Lambda$ . The equality  $\Phi^r = \pi_A^{-1}u$  on  $\bar{H}$  implies that  $\Phi^r = \pi_A^{-1}$  on  $H$  and that  $\Phi^{-r} = \pi_A$  on  $\Lambda$ .

By a polarization of an abelian variety  $\bar{A}$  over  $\bar{k}$  we mean a  $\mathbb{Q}$ -polarization in the sense of §9. As in §9, for any isogeny  $f : \bar{A}_1 \rightarrow \bar{A}_2$  and any polarization  $\lambda$  of  $\bar{A}_2$  we get a polarization  $f^*(\lambda)$  of  $\bar{A}_1$  by putting  $f^*(\lambda) = \widehat{f}\lambda f$ . Let  $c$  be a rational number and write  $c$  as  $c = p^r c_0$ . By a  $c$ -polarization of  $A$  we will mean a polarization  $\lambda$  of  $\bar{A}$  such that  $\pi_A^*(\lambda) = c\lambda$ . Note that  $c$  must be positive in order for  $\lambda$  to exist. It is immediate that the condition  $\pi_A^*(\lambda) = c\lambda$  is equivalent to  $\iota_\lambda(\pi_A)\pi_A = c$ , where  $\iota_\lambda$  denotes the Rosati involution of  $\text{End}(\bar{A})_{\mathbb{Q}}$ .

determined by  $\lambda$  (recall that  $\iota_\lambda(\pi_A) = \lambda^{-1} \hat{\pi}_A \lambda$ ), and it is not hard to see that it is also equivalent to the condition  $u^*(\lambda) = c_0 \sigma^r(\lambda)$ . In particular a  $p^r$ -polarization of an abelian variety  $A$  over  $k_r$  is a polarization  $\lambda: A \rightarrow \bar{A}$  defined over  $k_r$ ; thus our definition of polarization for virtual abelian varieties is a natural extension of the usual definition. We say that  $A$  is  $c$ -polarizable if a  $c$ -polarization of  $A$  exists.

Let  $\lambda$  be a  $c$ -polarization of  $A$ . Let  $l$  be a prime different from  $p$ . Then  $\lambda$  induces a  $\mathbb{Q}_l(1)$ -valued nondegenerate alternating form  $(\cdot, \cdot)$  on  $H_1(\bar{A}, \mathbb{Q}_l)$ . The condition  $\pi_A^*(\lambda) = c\lambda$  is equivalent to the condition that  $(\pi_A v, \pi_A w) = c(v, w)$  for all  $v, w \in H_1(\bar{A}, \mathbb{Q}_l)$ .

Again the  $p$ -adic situation requires a little more work. The  $c$ -polarization induces an  $L$ -valued nondegenerate alternating form  $(\cdot, \cdot)_1$  on  $\bar{H}$  (notation as before). The condition  $\pi_A^*(\lambda) = c\lambda$  is equivalent to the condition that  $(uv, uw)_1 = c_0 \sigma^r(v, w)_1$  for all  $v, w \in \bar{H}$ . It follows from this last condition that  $c_0$  is a  $p$ -adic unit (use that  $u(\bar{\Lambda}) = \bar{\Lambda}$ ). Therefore we may choose  $d \in \mathcal{O}_L^\times$  such that  $d^{-1} \sigma^r(d) = c_0$ . Let  $(\cdot, \cdot)_2$  be the alternating form on  $\bar{H}$  obtained by multiplying  $d$  times  $(\cdot, \cdot)_1$ ; it is immediate that  $\sigma^r(v, w)_2 = (uv, uw)_2$  for all  $v, w \in \bar{H}$ , which implies that  $(\cdot, \cdot)_2$  takes values in  $L_r$  on the  $L_r$ -subspace  $H$  of  $\bar{H}$ . We write  $(\cdot, \cdot)$  for the restriction of  $(\cdot, \cdot)_2$  to  $H$ . It is a nondegenerate alternating form on  $H$ , well defined up to multiplication by a unit in  $L_r$ , having the property that  $(\Phi v, \Phi w) = p^{-1} d \sigma(d)^{-1} \sigma(v, w)$  for all  $v, w \in H$  (just use that  $(\Phi v, \Phi w)_1 = p^{-1} \sigma(v, w)_1$ ). Note that  $d \sigma(d)^{-1} \in L_r^\times$  and that its norm down to  $\mathbb{Q}_p^\times$  is  $c_0^{-1}$ . Therefore the norm of  $p^{-1} d \sigma(d)^{-1}$  is  $p^{-r} c_0^{-1} = c^{-1}$ , and the property above can be rewritten as  $(\Phi v, \Phi w) = c' \sigma(v, w)$ , where  $c'$  is an element of  $L_r^\times$  whose norm down to  $\mathbb{Q}_p^\times$  is  $c^{-1}$ .

**Lemma 10.1.** *Let  $c$  be a positive rational number and let  $\pi \in \mathbb{Q}^\times$ . Then the following two conditions are equivalent.*

- (1) *There exists a positive involution on  $\mathbb{Q}[\pi]$  carrying  $\pi$  into  $c\pi^{-1}$ .*
- (2) *For every embedding of  $\mathbb{Q}[\pi]$  in  $\mathbb{C}$  the image of  $\pi$  has absolute value  $c^{1/2}$ .*

Tensor  $\mathbb{Q}[\pi]$  with  $\mathbb{R}$  and decompose it as a product of copies of  $\mathbb{R}$  and  $\mathbb{C}$ . For both  $\mathbb{R}$  and  $\mathbb{C}$  the only positive involution is  $x \mapsto \bar{x}$ . Therefore there is exactly one positive involution  $\iota$  on  $\mathbb{Q}[\pi] \otimes_{\mathbb{Q}} \mathbb{R}$ , namely, the one that induces  $x \mapsto \bar{x}$  on every copy of  $\mathbb{R}$  and  $\mathbb{C}$ . The first condition holds if and only if  $\iota(\pi) = c\pi^{-1}$  (since  $\iota(\pi) = c\pi^{-1}$  implies that  $\iota(\mathbb{Q}[\pi]) = \mathbb{Q}[\pi]$ ), which holds if and only if  $\bar{\pi} = c\pi^{-1}$  for every embedding of  $\mathbb{Q}[\pi]$  in  $\mathbb{C}$ , or, in other words, if and only if the second condition holds.

**Lemma 10.2.** *Let  $A$  be a  $c$ -polarizable virtual abelian variety over  $k_r$ , up to isogeny (for some positive rational number  $c$ ). Then  $\pi := \pi_A$  is a semisimple element of  $\text{End}(\bar{A})$ . Moreover the  $\mathbb{Q}$ -algebra  $\text{End}(A)$  is semisimple.*

Choose a  $c$ -polarization  $\lambda$  of  $A$  and let  $\iota_\lambda$  denote the corresponding Rosati involution of  $\text{End}(\bar{A})$ . Then  $\iota_\lambda(\pi)\pi = c$ . Thus  $c^{1/2}\pi$  is an element of the

compact group  $\{x \in \text{End}(\bar{A})_{\mathbb{R}} \mid i_{\lambda}(x)x = 1\}$ , which implies that  $\pi$  is semisimple as an element of the algebraic group  $\text{End}(\bar{A})^{\times}$  and hence that  $\pi$  is semisimple as an element of the algebra  $\text{End}(\bar{A})$ . The second statement of the lemma follows from the first, since  $\text{End}(A)$  is the centralizer of  $\pi$  in the semisimple algebra  $\text{End}(\bar{A})$ .

**Lemma 10.3.** *Let  $c$  be a positive rational number and let  $A$  be a virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny. Assume that  $\pi := \pi_A$  is a semisimple element of  $\text{End}(\bar{A})_{\mathbb{Q}}$ , and let  $\mathbb{Q}[\pi]$  denote the semisimple commutative  $\mathbb{Q}$ -subalgebra it generates. Then the following three conditions are equivalent.*

- (1) *The virtual abelian variety  $A$  is  $c$ -polarizable.*
- (2) *There exists a positive involution on  $\mathbb{Q}[\pi]$  that carries  $\pi$  into  $c\pi^{-1}$ .*
- (3) *For every  $\mathbb{Q}$ -algebra homomorphism from  $\mathbb{Q}[\pi]$  to  $\mathbb{C}$  the image of  $\pi$  has absolute value  $c^{1/2}$ .*

The equivalence of (2) and (3) is proved exactly the same way as Lemma 10.1. It is obvious that (1) implies (2): if  $\lambda$  is a  $c$ -polarization of  $\bar{A}$  then the Rosati involution for  $\lambda$  carries  $\pi$  into  $c\pi^{-1}$ . It remains to prove that (2) implies (1). Applying Lemma 9.2 to the  $\mathbb{Q}[\pi]$ -abelian variety  $\bar{A}$ , we conclude that there exists a polarization  $\lambda$  of  $\bar{A}$  such that the Rosati involution for  $\lambda$  carries  $\pi$  into  $c\pi^{-1}$ ; this last condition is equivalent to  $\lambda$  being a  $c$ -polarization of  $A$ .

From now on  $c$  will denote a positive rational number of the form  $p'c_0$ , where  $c_0$  is a  $p$ -adic unit (we have seen that  $c_0$  must be a  $p$ -adic unit if any  $c$ -polarizations exist). We say that an algebraic number  $\alpha \in \mathbb{Q}$  is a  $c$ -number if the image of  $\alpha$  under any embedding  $\mathbb{Q} \rightarrow \mathbb{Q}_p$  lies in the valuation ring of  $\mathbb{Q}_p$  and the image of  $\alpha$  under any embedding  $\mathbb{Q} \rightarrow \mathbb{C}$  has absolute value  $c^{1/2}$ .

**Lemma 10.4.** *Let  $A$  be a  $c$ -polarizable virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny, and let  $\mathbb{Q}[\pi]$  denote the semisimple commutative  $\mathbb{Q}$ -subalgebra of  $\text{End}(\bar{A})_{\mathbb{Q}}$  generated by  $\pi := \pi_A$ . Then the image of  $\pi$  under any  $\mathbb{Q}$ -algebra homomorphism  $\mathbb{Q}[\pi] \rightarrow \mathbb{Q}$  is a  $c$ -number.*

It follows from Lemma 10.3 that the image of  $\pi$  under any homomorphism  $\mathbb{Q}[\pi] \rightarrow \mathbb{C}$  has absolute value  $c^{1/2}$ . Since  $\bar{H}$  is a faithful representation of  $\mathbb{Q}[\pi] \otimes_{\mathbb{Q}} L$  on an  $L$ -vector space, the image of  $\pi$  under any homomorphism  $\mathbb{Q}[\pi] \rightarrow \bar{L}$  is an eigenvalue of  $\pi$  on  $\bar{H}$ , and these eigenvalues belong to the valuation ring of  $\bar{L}$  because  $\pi$  preserves the lattice  $\bar{\Lambda}$  in  $\bar{H}$ .

**Corollary 10.5.** *Let  $A$  be a virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny. There is at most one value of  $c$  for which  $A$  is  $c$ -polarizable.*

This is obvious, since  $c$  can be recovered by embedding  $\mathbb{Q}[\pi]$  in  $\mathbb{C}$  and taking the square of the absolute value of  $\pi$ .

**Lemma 10.6.** *Let  $A$  be a virtual abelian variety over  $k_r$  up to isogeny. Suppose that  $\pi := \pi_A$  is a semisimple element of  $\text{End}(\bar{A})$  (for example, suppose that  $A$  is  $c$ -polarizable). Then the  $\mathbb{Q}$ -subalgebra  $\mathbb{Q}[\pi]$  generated by  $\pi$  in  $\text{End}(A)$  is the center of  $\text{End}(A)$ .*

Let  $s$  be a positive integer large enough that  $\bar{A}$  and all its endomorphisms can be defined over  $k_{rs}$ . Choose such a  $k_{rs}$ -form  $A_0$  of  $\bar{A}$  and let  $\pi_0 \in \text{End}(A_0) = \text{End}(\bar{A})$  denote its Frobenius element. Since  $\text{End}(A)$  is the centralizer of the semisimple element  $\pi$  in  $\text{End}(\bar{A})$ , the center of  $\text{End}(A)$  is generated by  $\pi$  and the center of  $\text{End}(\bar{A})$ . From [T2] we know that any positive power of  $\pi_0$  generates the center of  $\text{End}(\bar{A})$ . Therefore, to prove the lemma it is enough to show that  $\pi_0^t \in \mathbb{Q}[\pi]$  for some positive integer  $t$ .

To prove that  $\pi_0^t \in \mathbb{Q}[\pi]$  it is enough to prove the following statement: if  $\rho, \tau$  are two  $\mathbb{Q}$ -algebra maps  $\mathbb{Q}[\pi, \pi_0] \rightarrow \bar{\mathbb{Q}}$  whose restrictions to  $\mathbb{Q}[\pi]$  are equal, then  $\rho(\pi_0^t) = \tau(\pi_0^t)$ . Let  $F$  be a finite extension of  $\mathbb{Q}$  in  $\bar{\mathbb{Q}}$  containing the images of  $\rho$  and  $\tau$ . Consider the elements  $\rho(\pi_0), \tau(\pi_0)$  of  $F$ . Since they are both Weil  $p^{rs}$ -numbers, they have the same absolute values at every place of  $F$  except possibly the places lying over  $p$ . It follows from the definition of a virtual abelian variety over  $k_r$  up to isogeny that  $\pi_0^{-1}\pi^s$  is a prime-to- $p$  isogeny; therefore  $\rho(\pi_0)$  has the same  $p$ -adic absolute values as  $\rho(\pi^s)$ , and  $\tau(\pi_0)$  has the same  $p$ -adic absolute values as  $\tau(\pi^s) = \rho(\pi^s)$ . Therefore  $\rho(\pi_0), \tau(\pi_0)$  have the same absolute values at every place of  $F$ , which means that there exists a positive integer  $t$  (depending on  $\rho, \tau$ ) such that  $\tau(\pi_0^t) = \rho(\pi_0^t)$ . Since there are only finitely many pairs  $(\rho, \tau)$ , there exists a positive integer  $t$  such that  $\tau(\pi_0^t) = \rho(\pi_0^t)$  for all  $\tau, \rho$  such that  $\tau(\pi) = \rho(\pi)$ . This concludes the proof.

**Lemma 10.7.** *Let  $A$  be a virtual abelian variety over  $k_r$  up to isogeny. Suppose that  $\pi := \pi_A$  is a semisimple element of  $\text{End}(\bar{A})$ . Then for every prime  $l$  different from  $p$  the canonical map  $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l \rightarrow \text{End}_{\pi}(H_1(\bar{A}, \mathbb{Q}_l))$  is an isomorphism, where  $\text{End}_{\pi}(H_1(\bar{A}, \mathbb{Q}_l))$  denotes the ring of endomorphisms of  $H_1(\bar{A}, \mathbb{Q}_l)$  that commute with  $\pi$ . The analogous statement with  $\text{Hom}(\cdot, \cdot)$  replacing  $\text{End}(\cdot)$  also holds.*

Write  $H_l$  as an abbreviation for  $H_1(\bar{A}, \mathbb{Q}_l)$ . By [T2] the canonical map  $\text{End}(\bar{A}) \otimes_{\mathbb{Q}} \mathbb{Q}_l \rightarrow \text{End}(H_l)$  is injective with image consisting of all elements in  $\text{End}(H_l)$  that commute with all elements in the center of  $\text{End}(\bar{A})$ . Therefore the image of  $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l$  consists of all elements in  $\text{End}(H_l)$  that commute with  $\pi$  and with all elements of the center of  $\text{End}(\bar{A})$ . Since  $\pi$  generates the center of  $\text{End}(A)$  by Lemma 10.6 and since the center of  $\text{End}(\bar{A})$  is contained in the center of  $\text{End}(A)$ , it follows that any element of  $\text{End}(H_l)$  that commutes with  $\pi$  automatically commutes with all elements of the center of  $\text{End}(\bar{A})$ . This gives the first statement of the lemma, and the statement about  $\text{Hom}(A_1, A_2)$  follows by applying what has already been done to  $\text{End}(A_1 \times A_2)$ , as in Lemma 3 of [T2].

**Lemma 10.8.** *Let  $A$  be a virtual abelian variety over  $k_r$  up to isogeny. Suppose that  $\pi := \pi_A$  is a semisimple element of  $\text{End}(\bar{A})$ . Let  $H$  be the  $L_r$ -vector space with  $\sigma$ -linear bijection  $\Phi$  that we have associated to  $A$ . Write  $\text{End}_{\Phi}(H)$  for the  $L_r$ -linear endomorphisms of  $H$  that commute with  $\Phi$ . Then the canonical map  $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p \rightarrow \text{End}_{\Phi}(H)$  is an isomorphism. The analogous statement with  $\text{Hom}(\cdot, \cdot)$  replacing  $\text{End}(\cdot)$  also holds.*

One knows from the theory of Dieudonné modules that the map is injective. Thus it is enough to prove that the dimensions of  $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p$  and  $\text{End}_{\Phi}(H)$  are equal. From Lemma 10.7 we know that the dimension of  $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p$  is equal to the dimension of the centralizer of  $\pi$  in  $\text{End}(H_1(\bar{A}, \mathbb{Q}_l))$ . The characteristic polynomial of the semisimple element  $\pi$  acting on  $H_1(\bar{A}, \mathbb{Q}_l)$  has rational coefficients and is equal to the characteristic polynomial of  $\pi$  acting on  $H$  (pass to  $\bar{H}$  to derive this from the usual statement). Therefore the dimension of  $\text{End}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p$  is equal to the dimension over  $L_r$  of the centralizer  $E$  in  $\text{End}(H)$  of  $\pi$ . But  $\text{End}_{\Phi}(H)$  is a  $\mathbb{Q}_p$ -form of the  $L_r$ -algebra  $E$  (the Frobenius element  $\sigma \in \text{Gal}(L_r/\mathbb{Q}_p)$  acts  $\sigma$ -linearly on  $E$  by  $f \mapsto \Phi f \Phi^{-1}$ ), which implies that the  $\mathbb{Q}_p$ -dimension of  $\text{End}_{\Phi}(H)$  is equal to the  $L_r$ -dimension of  $E$ . This proves the first statement of the lemma. The second follows from the first as in the proof of Lemma 10.7.

Denote by  $\mathcal{V}_{r,c}$  the full subcategory of  $\mathcal{V}_r$  whose objects are  $c$ -polarizable virtual abelian varieties over  $k_r$  up to isogeny.

**Lemma 10.9.** *The  $\mathbb{Q}$ -linear category  $\mathcal{V}_{r,c}$  is abelian and semisimple. All of its objects have finite length, and for any two objects  $A_1, A_2$  the  $\mathbb{Q}$ -vector space  $\text{Hom}(A_1, A_2)$  is finite dimensional.*

It is easy to see that  $\mathcal{V}_{r,c}$  is abelian and that the functor  $A \mapsto \bar{A}$  is a faithful exact functor from  $\mathcal{V}_{r,c}$  to the category of abelian varieties over  $\bar{k}$  up to isogeny. For example the kernel of a morphism  $A_1 \rightarrow A_2$  is obtained as follows. The kernel  $K$  of  $\bar{A}_1 \rightarrow \bar{A}_2$  (in the category of abelian varieties over  $\bar{k}$  up to isogeny) is stable by  $\pi_{A_1}$ , and hence  $\pi_{A_1}$  induces an endomorphism  $\pi_K$  of  $K$ .

Put  $u_K = \pi_K \Phi_r^{-1}$ . Then  $u_K$  is a prime-to- $p$  isogeny and the kernel of  $A_1 \rightarrow A_2$  is  $K := (\bar{K}, u_K)$  (note that any  $c$ -polarization of  $A_1$  induces one on  $K$ ). The rest is just as easy. It follows that all objects of  $\mathcal{V}_{r,c}$  have finite length and that all the vector spaces  $\text{Hom}(A_1, A_2)$  are finite dimensional, because these statements hold in the category of abelian varieties over  $\bar{k}$  up to isogeny. The semisimplicity of  $\mathcal{V}_{r,c}$  now follows from Lemmas 3.1 and 10.2.

In view of Lemma 10.9 we will understand  $\mathcal{V}_{r,c}$  completely if we describe its simple objects and their endomorphism rings. If  $A$  is a simple object, then  $E := \text{End}(A)$  is a finite-dimensional central division algebra over  $\mathbb{Q}[\pi] \subset E$ .

**Lemma 10.10.** *Let  $A_1, A_2$  be two simple objects in  $\mathcal{V}_{r,c}$  with Frobenius elements  $\pi_1, \pi_2$ . Suppose that there exists an isomorphism  $\mathbb{Q}[\pi_1] \rightarrow \mathbb{Q}[\pi_2]$  carrying  $\pi_1$  into  $\pi_2$ . Then  $A_1$  and  $A_2$  are isomorphic.*

Suppose that  $A_1$  and  $A_2$  were not isomorphic. Then the endomorphism algebra of  $A_1 \times A_2$  would be  $\text{End}(A_1) \times \text{End}(A_2)$ , which has center  $\mathbb{Q}[\pi_1] \times \mathbb{Q}[\pi_2]$ . The Frobenius element  $(\pi_1, \pi_2)$  for  $A_1 \times A_2$  would then generate the graph of the map  $\mathbb{Q}[\pi_1] \rightarrow \mathbb{Q}[\pi_2]$ , contradicting Lemma 10.6.

**Lemma 10.11.** *Let  $A$  be a simple object in  $\mathcal{V}_{r,c}$  with Frobenius element  $\pi$  and endomorphism algebra  $E$ . The Hasse invariant of the central division algebra*

$E$  over  $\mathbb{Q}[\pi]$  at a place  $v$  of  $\mathbb{Q}[\pi]$  is given by

$$\begin{cases} \frac{1}{2} & \text{if } v \text{ is real,} \\ [\mathbb{Q}[\pi]_v : \mathbb{Q}_p]v(\pi)/v(p^r) & \text{if } v \text{ divides } p, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover the following equality holds:

$$2 \dim(A) = [\mathbb{Q}[\pi] : \mathbb{Q}] (\dim_{\mathbb{Q}[\pi]} E)^{1/2}.$$

The statement about the local invariants of  $E$  at finite places  $v$  follows from Lemmas 10.7 and 10.8 (see §11 in the  $p$ -adic case). Suppose that  $v$  is a real place. Then the Rosati involution for any  $c$ -polarization of  $A$  must fix  $\pi$ , and therefore  $\pi^2 = c$ . If  $c$  is a square in  $\mathbb{Q}$ , then  $\mathbb{Q}[\pi] = \mathbb{Q}$ , and since  $c = p^r c_0$  where  $c_0$  is a  $p$ -adic unit, the local invariant of  $E$  at  $p$  is  $\frac{1}{2}$ . Since the local invariants for  $l \neq p$  are 0 and the sum of all local invariants is 0, the local invariant at the real place of  $\mathbb{Q}$  must be  $\frac{1}{2}$ . If  $c$  is not a square in  $\mathbb{Q}$ , we consider the base change  $A'$  of  $A$  to the quadratic extension  $k_{2r}$  of  $k_r$ . Its Frobenius is the square of  $\pi$ , hence is equal to  $c$ . Let  $E'$  be the endomorphism algebra of  $A'$ ; by the case just treated  $E'$  is a central simple algebra over  $\mathbb{Q}$  and the class of  $E'$  in the Brauer group of  $\mathbb{R}$  has invariant  $\frac{1}{2}$ . Since  $E$  is the centralizer of  $\mathbb{Q}[\pi] \otimes_{\mathbb{Q}} \mathbb{R} \approx \mathbb{R} \times \mathbb{R}$  in  $E'$ , the invariant of  $E$  at both real places of  $\mathbb{Q}[\pi]$  is  $\frac{1}{2}$ .

Let  $l$  be a prime different from  $p$ , and let  $H_l$  be  $H_1(\bar{A}, \mathbb{Q}_l)$ . The left side of the equality  $2 \dim A = [\mathbb{Q}[\pi] : \mathbb{Q}] (\dim_{\mathbb{Q}[\pi]} E)^{1/2}$  is the  $\mathbb{Q}_l$ -dimension of  $H_l$ , and the right side is the  $\mathbb{Q}_l$ -dimension of any maximal semisimple commutative subalgebra of  $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$ ; since  $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$  is the centralizer of a semisimple endomorphism of  $H_l$ , these two dimensions are equal. This finishes the proof of the lemma.

Let  $A$  be a simple object in  $\mathcal{V}_{r,c}$  with Frobenius element  $\pi$ . The image of  $\pi$  under an embedding  $\mathbb{Q}[\pi] \rightarrow \bar{\mathbb{Q}}$  is a  $c$ -number  $\pi \in \bar{\mathbb{Q}}$  whose  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -orbit is independent of the choice of embedding. Lemma 10.10 says that the isomorphism class of  $A$  is determined by the  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -orbit of  $\pi$ , and Lemma 10.11 gives a recipe for determining  $\dim(A)$  and the isomorphism class of  $\text{End}(A)$  from  $\pi$ . To complete the picture, all that remains is to prove the following lemma.

**Lemma 10.12.** *Every  $c$ -number  $\pi \in \bar{\mathbb{Q}}$  arises from some simple object in  $\mathcal{V}_{r,c}$ .*

By Lemma 10.1 there exists a positive involution  $*$  on  $\mathbb{Q}[\pi]$  such that  $\pi\pi^* = c$ . If  $*$  is nontrivial, we put  $F = \mathbb{Q}[\pi]$ . If  $*$  is trivial, then  $\mathbb{Q}[\pi]$  is totally real, and we take for  $F$  any totally complex quadratic extension of  $\mathbb{Q}[\pi]$ ; we then extend  $*$  to  $F$  by taking it to be the nontrivial automorphism of  $F$  over  $\mathbb{Q}[\pi]$ . Let  $T$  be the  $\mathbb{Q}$ -torus  $\{x \in F^\times | xx^* \in \mathbb{Q}^\times\}$ . Of course  $\pi \in T(\mathbb{Q})$ . For any finite place  $v$  of  $\mathbb{Q}$  we denote by  $K_v$  the maximal compact subgroup of  $T(\mathbb{Q}_v)$  and put  $X_v = T(\mathbb{Q}_v)/K_v$ . The canonical map  $T(\mathbb{Q}) \rightarrow \bigoplus_v X_v$  (the direct sum being taken over all finite places  $v$  of  $\mathbb{Q}$ ) has finite cokernel (this is true for any  $\mathbb{Q}$ -torus) and has finite kernel (this is true because  $T$  is an extension of a

split  $\mathbb{Q}$ -torus by a  $\mathbb{Q}$ -torus that is anisotropic over  $\mathbb{R}$ ). Therefore there exists a positive integer  $s$  and elements  $\pi_0, t \in T(\mathbb{Q})$  such that

- (1)  $\pi^s = \pi_0 t$ ,
- (2)  $\pi_0 \in K_l$  for all  $l \neq p$ ,
- (3)  $t \in K_p$ .

The element  $\pi_0 \in F$  is a Weil  $p^{rs}$ -number: it is clearly a unit at all finite places of  $F$  not dividing  $p$ ; it has nonnegative valuation at every place of  $F$  over  $p$  since this is true for  $\pi$ , and  $\pi^s, \pi_0$  differ (multiplicatively) by the element  $t$ , which is a unit at every place of  $F$  over  $p$ ; finally, since the positive rational number  $\pi_0 \pi_0^*$  is a unit away from  $p$ , it is a power of  $p$ , which because of (1) and (3) must be  $p^{rs}$ , and the equality  $\pi_0 \pi_0^* = p^{rs}$  implies that the image of  $\pi$  under any embedding of  $F$  in  $\mathbb{C}$  has absolute value  $p^{rs/2}$ .

By Honda-Tate theory [H, T3] there exist a simple abelian variety  $A_0$  over  $k_{rs}$  and an embedding  $\mathbb{Q}[\pi_0] \rightarrow \text{End}(A_0)$  such that the image of  $\pi_0$  in  $\text{End}(A_0)$  is the Frobenius element for  $A_0$ . Let  $m = [F : \mathbb{Q}[\pi_0]]$ . Then  $\mathbb{Q}[\pi_0] \rightarrow \text{End}(A_0^m) = M_m(\text{End}(A_0))$  can be extended to a homomorphism  $F \rightarrow \text{End}(A_0^m)$ . Using this homomorphism to regard  $\pi^s \pi_0^{-1}$  as a prime-to- $p$  isogeny from  $A_0^m$  to itself, we see that there exists a structure of virtual abelian variety  $A'$  over  $k_{rs}$  on  $(A_0^m)_k$  for which  $\pi^s$  is the Frobenius element. Applying the restriction of scalars functor (from  $k_{rs}$  to  $k_r$ ), we get a virtual abelian variety  $B$  over  $k_r$  for which there exists a homomorphism  $\mathbb{Q}[\pi_B] \rightarrow \mathbb{Q}$  taking  $\pi_B$  to  $\pi$ . Lemma 10.9 continues to hold (with the same proof) for the category of virtual abelian varieties over  $k_r$  up to isogeny for which the Frobenius element is semisimple. Some simple factor  $B'$  of  $B$  in this category has  $\pi$  as Frobenius. Since  $\pi$  is a  $c$ -number, Lemma 10.3 implies that  $B'$  is  $c$ -polarizable, and the proof is finished.

Let  $B$  be a simple algebra of dimension  $d^2$  over a number field  $F$ . Our last task in this section is to describe the simple objects in the category  $\mathcal{V}_{r,c,B}$  of  $B$ -objects in the category of  $c$ -polarizable virtual abelian varieties over  $k_r$  up to isogeny.

Let  $\pi$  be a  $c$ -number in  $\bar{F}$ . Picking an isomorphism  $\bar{F} \simeq \bar{\mathbb{Q}}$ , we get  $\pi \in \bar{\mathbb{Q}}$ , a simple object  $Y_\pi$  in  $\mathcal{V}_{r,c}$  corresponding to  $\pi$ , and a surjective homomorphism  $F \otimes_{\mathbb{Q}} \mathbb{Q}[\pi] \rightarrow F[\pi]$ ; according to the discussion in §3 we then get a simple object  $X_\pi$  in  $\mathcal{V}_{r,c,B}$  whose underlying virtual abelian variety is isotypic of type  $Y_\pi$ .

**Lemma 10.13.** *The construction  $\pi \mapsto X_\pi$  sets up a bijection between  $c$ -numbers in  $\bar{F}$  up to conjugacy over  $F$  and isomorphism classes of simple objects in  $\mathcal{V}_{r,c,B}$ . The endomorphism algebra  $\text{End}(X_\pi)$  is a central division algebra  $C$  over  $F[\pi]$  whose Hasse invariant at a place  $v$  of  $F[\pi]$  is given by*

$$\text{inv}_v(C) = \begin{cases} \frac{1}{2} - \text{inv}_v(B \otimes_F F[\pi]) & \text{if } v \text{ is real,} \\ [F[\pi]_v : \mathbb{Q}_p]v(\pi)/v(p^r) - \text{inv}_v(B \otimes_F F[\pi]) & \text{if } v \text{ divides } p, \\ -\text{inv}_v(B \otimes_F F[\pi]) & \text{otherwise.} \end{cases}$$

Moreover the dimension of the abelian variety  $\bar{A}$  over  $\bar{k}$  underlying  $X_\pi$  is given

by

$$2 \dim(A) = d[F[\pi] : \mathbb{Q}] (\dim_{F[\pi]} C)^{1/2}.$$

This lemma follows immediately from the last three lemmas together with Lemma 3.3.

## 11. SEMISIMPLE ISOCRYSTALS OVER $L_r$

As in §10,  $L_r$  denotes the fraction field of the Witt ring  $W(k_r)$ . An isocrystal over  $L_r$  is a finite-dimensional  $L_r$ -vector space  $V$  together with a  $\sigma$ -linear bijection  $\Phi$  from  $V$  to itself. For any isocrystal  $V$  we have the linear automorphism  $\pi_V := \Phi'$  of  $V$ , which belongs to the center of the  $\mathbb{Q}_p$ -algebra  $\text{End}_\Phi(V) := \{f \in \text{End}(V) | \Phi f = f\Phi\}$ . We say that the isocrystal  $V$  is semisimple if  $\pi_V$  is a semisimple endomorphism of the vector space  $V$ . Since  $\text{End}_\Phi(V)$  is a  $\mathbb{Q}_p$ -form of the centralizer of  $\pi_V$  in  $\text{End}(V)$  (an  $L_r$ -algebra),  $\text{End}_\Phi(V)$  is a semisimple ring if the isocrystal  $V$  is semisimple. The category of all semisimple isocrystals over  $L_r$  is obviously a  $\mathbb{Q}_p$ -linear abelian category all of whose objects have finite length. Lemma 3.1 implies that it is a semisimple category. We are going to determine the simple objects in this category as well as their endomorphism rings.

**Lemma 11.1.** *Suppose that  $V$  is a semisimple isocrystal. Then the center of  $\text{End}_\Phi(V)$  is generated by  $\pi_V$ .*

It is enough to check this statement after tensoring with  $L_r$ ; then it becomes obvious since  $\text{End}_\Phi(V) \otimes_{\mathbb{Q}_p} L_r$  is the centralizer of the semisimple element  $\pi_V$  in  $\text{End}(V)$ .

**Lemma 11.2.** *Suppose that  $V_1, V_2$  are simple objects in the category of semisimple isocrystals. Then  $V_1, V_2$  are isomorphic if and only if there exists a  $\mathbb{Q}_p$ -algebra isomorphism  $\mathbb{Q}_p[\pi_1] \rightarrow \mathbb{Q}_p[\pi_2]$  carrying  $\pi_1$  into  $\pi_2$ , where  $\mathbb{Q}_p[\pi_i]$  denotes the  $\mathbb{Q}_p$ -subalgebra of  $\text{End}_\Phi(V_i)$  generated by  $\pi_i$ .*

Use the method of proof of Lemma 10.10.

**Lemma 11.3.** *Let  $V$  be a simple object in the category of semisimple isocrystals, and write  $\pi$  for  $\pi_V$ . Then the Hasse invariant of the central division algebra  $\text{End}_\Phi(V)$  over  $\mathbb{Q}_p[\pi]$  is  $-[\mathbb{Q}_p[\pi] : \mathbb{Q}_p]v(\pi)/v(p')$ , where  $v$  denotes the valuation on  $\mathbb{Q}_p[\pi]$ . Moreover the following equality holds:*

$$\dim_{L_r}(V) = [\mathbb{Q}_p[\pi] : \mathbb{Q}_p] (\dim_{\mathbb{Q}_p[\pi]} \text{End}_\Phi(V))^{1/2}.$$

We use what is known about isocrystals over  $L$ , the fraction field of the Witt ring of  $\bar{k}$ . The isocrystal  $V_L$  over  $L$  obtained from  $V$  is isotypic of slope  $v(\pi)/v(p')$ . Therefore  $\text{End}_\Phi(V_L)$  is a matrix algebra over the central division algebra over  $\mathbb{Q}_p$  with invariant  $-v(\pi)/v(p')$ . Since  $\text{End}_\Phi(V)$  is the commutant of  $\mathbb{Q}_p[\pi]$  in  $\text{End}_\Phi(V_L)$ , the class of  $\text{End}_\Phi(V)$  in the Brauer group of  $\mathbb{Q}_p[\pi]$  is the image of the class of  $\text{End}_\Phi(V_L)$  in the Brauer group of  $\mathbb{Q}_p$ . The map  $\text{Br}(\mathbb{Q}_p) \rightarrow \text{Br}(\mathbb{Q}_p[\pi])$  has the effect of multiplying the invariant by  $[\mathbb{Q}_p[\pi] : \mathbb{Q}_p]$ .

This proves the first statement of the lemma. The second statement is proved the same way as the analogous statement in Lemma 10.11, by considering the  $\mathbb{Q}_p$ -dimension of a maximal commutative semisimple subalgebra of  $\text{End}_{\Phi}(V)$ .

Let  $V$  be a simple object in the category of semisimple isocrystals over  $L_r$ . The image of  $\pi := \pi_V$  under an embedding  $\mathbb{Q}_p[\pi] \rightarrow \mathbb{Q}_p$  is an element of  $\mathbb{Q}_p^\times$  whose  $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ -orbit is independent of the choice of embedding.

**Lemma 11.4.** *Every element  $\pi \in \mathbb{Q}_p^\times$  arises from some simple isocrystal  $V$ .*

Let  $F$  be a finite extension of  $\mathbb{Q}_p$  in  $\bar{\mathbb{Q}}_p$  containing  $\pi$  and large enough that  $L_r$  embeds in  $F$ . Then  $F \otimes_{\mathbb{Q}_p} L_r$  is a product of copies of  $F$ , and there exists  $\delta \in F \otimes_{\mathbb{Q}_p} L_r$  such that  $N_{(F \otimes_{\mathbb{Q}_p} L_r)/F}(\delta) = \pi$ . Put  $m = [F : \mathbb{Q}_p]$  and embed  $F$  in  $\mathbf{M}_m(\mathbb{Q}_p)$ ; this induces an embedding of  $F \otimes_{\mathbb{Q}_p} L_r$  in  $\mathbf{M}_m(L_r)$ . Let  $\Phi$  be the  $\sigma$ -linear bijection on  $(L_r)^m$  whose matrix is the image of  $\delta$  in  $\mathbf{M}_m(L_r)$ . Then  $\Phi'$  is the endomorphism of  $(L_r)^m$  whose matrix is the image of  $\pi$ . Therefore the simple factors of the isotypic semisimple isocrystal  $((L_r)^m, \Phi)$  give rise to  $\pi$ .

We now have a good understanding of the simple objects in the  $\mathbb{Q}_p$ -linear category  $\mathcal{C}$  of semisimple isocrystals over  $L_r$ . Our next task is to describe the simple objects in the category  $\mathcal{C}_B$  of  $B$ -objects in  $\mathcal{C}$ , where  $B$  is a finite-dimensional simple algebra over  $\mathbb{Q}_p$ . Write  $F$  for the center of  $B$ , a  $p$ -adic field, and define a positive integer  $d$  by  $d^2 = \dim_F(B)$ . Let  $\pi \in \bar{F}^\times$ . Picking an isomorphism  $\bar{F} \simeq \bar{\mathbb{Q}}_p$ , we get  $\pi \in \mathbb{Q}_p$ , a simple object  $Y_\pi$  in  $\mathcal{C}$  corresponding to  $\pi$ , and a surjective homomorphism  $F \otimes_{\mathbb{Q}_p} \mathbb{Q}_p[\pi] \rightarrow F[\pi]$ ; according to the discussion in §3 we then get a simple object  $X_\pi$  in  $\mathcal{C}_B$  whose underlying  $\mathcal{C}$ -object is isotypic of type  $Y_\pi$ .

**Lemma 11.5.** *The construction  $\pi \mapsto X_\pi$  sets up a bijection between elements of  $\bar{F}^\times$  up to conjugacy over  $F$  and isomorphism classes of simple objects in  $\mathcal{C}_B$ . The endomorphism algebra  $\text{End}(X_\pi)$  is a central division algebra  $C$  over  $F[\pi]$  whose Hasse invariant is given by*

$$\text{inv}(C) = -[F[\pi] : \mathbb{Q}_p]v(\pi)/v(p') - [F[\pi] : F]\text{inv}(B),$$

where  $v$  denotes the valuation on  $F[\pi]$ . Moreover the dimension of the  $L_r$ -vector space underlying  $X_\pi$  is  $d[F[\pi] : \mathbb{Q}_p](\dim_{F[\pi]} C)^{1/2}$ .

The lemma follows immediately from Lemmas 11.3 and 3.3. We will use Lemma 11.5 to analyze the objects in  $\mathcal{C}_B$  having a given  $L_r$ -dimension. Let  $(V, \Phi, i)$  be an object in  $\mathcal{C}_B$ ; thus  $(V, \Phi)$  is an isocrystal over  $L_r$  and  $i$  is a  $\mathbb{Q}_p$ -algebra homomorphism  $B \rightarrow \text{End}_{\Phi}(V)$ . The automorphism  $\pi_V = \Phi'$  is  $F \otimes_{\mathbb{Q}_p} L_r$ -linear. Since  $\Phi$  commutes with  $\pi_V$  and  $F$ , it provides a  $\sigma$ -linear isomorphism from the pair  $(V, \pi_V)$  to itself. The first consequence of this is that  $V$  is a free  $F \otimes_{\mathbb{Q}_p} L_r$ -module; therefore  $\dim_{L_r}(V)$  is divisible by  $[F : \mathbb{Q}_p]$  and it makes sense to consider the characteristic polynomial of the  $F \otimes_{\mathbb{Q}_p} L_r$ -linear map  $\pi_V$ . This characteristic polynomial is monic of degree

$\dim_{L_r}(V)/[F : \mathbb{Q}_p]$  and has coefficients in  $F \otimes_{\mathbb{Q}_p} L_r$ . The second consequence of the fact mentioned above is that the coefficients of the characteristic polynomial are fixed by the Frobenius element  $\sigma \in \text{Gal}(L_r/\mathbb{Q}_p)$  and hence lie in  $F \subset F \otimes_{\mathbb{Q}_p} L_r$ . Now let  $f \in F[T]$  be a monic polynomial of degree  $m$  and for  $\pi \in F^\times$  denote by  $m(\pi)$  the multiplicity of  $\pi$  as root of  $f$ .

**Lemma 11.6.** *The isomorphism class of an object in  $\mathcal{C}_B$  is determined by its characteristic polynomial. The polynomial  $f$  arises from an  $m[F : \mathbb{Q}_p]$ -dimensional object of  $\mathcal{C}_B$  if and only if the following statement holds for all  $\pi \in F^\times$ : the number  $m(\pi)$  is divisible by  $d$  and the quotient  $m(\pi)/d$  kills the class of  $\text{End}(X_\pi)$  in the Brauer group of  $F[\pi]$ .*

Writing an object  $V$  in  $\mathcal{C}_B$  as a sum of simple objects, we see that the characteristic polynomial is the product of the characteristic polynomials of those simple objects. The only roots of the characteristic polynomial  $f_\pi$  of  $X_\pi$  are the conjugates over  $F$  of  $\pi$ , and it follows from Lemma 11.5 that the multiplicity of each conjugate of  $\pi$  as a root of  $f_\pi$  is equal to  $d(\dim_{F[\pi]} C)^{1/2}$ , where  $C = \text{End}(X_\pi)$ . It is now clear that we can reconstruct the multiplicities of the irreducible constituents of  $V$  from the characteristic polynomial of  $V$ , which gives the first statement of the lemma. It is also clear that  $f$  arises from some  $V$  if and only if the following statement holds for all  $\pi \in F^\times$ : the number  $m(\pi)$  is divisible by  $d(\dim_{F[\pi]} C)^{1/2}$ . The second statement of the lemma follows from the fact that  $(\dim_{F[\pi]} C)^{1/2}$  is the order of  $C$  in the Brauer group of  $F[\pi]$ .

## 12. EQUALITY OF TWO FUNCTORIAL ISOMORPHISMS FROM $X_*(T)_\Gamma$ TO $B(T)$

Let  $K$  be a finite Galois extension of  $\mathbb{Q}_p$  contained in some algebraic closure  $\bar{\mathbb{Q}}_p$  of  $\mathbb{Q}_p$ . Let  $K^{\text{un}}$  denote the maximal unramified extension of  $K$  in  $\bar{\mathbb{Q}}_p$ , and let  $L$  denote the completion of the maximal unramified extension of  $\mathbb{Q}_p$  in  $\bar{\mathbb{Q}}_p$ . Write  $\Gamma$  for the Galois group  $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$  and  $\sigma$  for the Frobenius automorphism of  $L$  over  $\mathbb{Q}_p$ . Consider the category  $\mathcal{T}$  of tori  $T$  over  $\mathbb{Q}_p$  that are split by  $K$ . The functor  $T \mapsto X_*(T)$  is an equivalence of categories between  $\mathcal{T}$  and the category of  $\text{Gal}(K/\mathbb{Q}_p)$ -modules that are free of finite rank as abelian groups. The functor  $T \mapsto X_*(T)$  is represented by the torus  $R_{K/\mathbb{Q}_p} \mathbb{G}_m$  and the following cocharacter  $\mu_{\text{univ}} \in X_*(R_{K/\mathbb{Q}_p} \mathbb{G}_m)$ : the  $\text{Gal}(K/\mathbb{Q}_p)$ -module  $X_*(R_{K/\mathbb{Q}_p} \mathbb{G}_m)$  is the group algebra  $\mathbb{Z}[\text{Gal}(K/\mathbb{Q}_p)]$ , regarded as a left  $\text{Gal}(K/\mathbb{Q}_p)$ -module, and  $\mu_{\text{univ}}$  corresponds to the unit element  $1 \in \mathbb{Z}[\text{Gal}(K/\mathbb{Q}_p)]$ .

As in [K3] for any  $T \in \mathcal{T}$  we write  $B(T)$  for the group  $T(L)/\{t\sigma(t)^{-1} | t \in T(L)\}$ . In §2 of [K3] a functorial isomorphism  $f: X_*(T)_\Gamma \rightarrow B(T)$  is constructed, where  $X_*(T)_\Gamma$  denotes the coinvariants of  $\Gamma$  on  $X_*(T)$ . This isomorphism of functors  $X_*(\cdot)_\Gamma \rightarrow B(\cdot)$  can be characterized as follows: it is the unique homomorphism of functors  $X_*(\cdot)_\Gamma \rightarrow B(\cdot)$  that for  $\mathbb{G}_m$  sends the generator  $1 \in \mathbb{Z} = X_*(\mathbb{G}_m)_\Gamma$  to the element of  $B(\mathbb{G}_m)$  represented by  $p \in L^\times = \mathbb{G}_m(L)$ . Actually [K3] deals with the category of all  $\mathbb{Q}_p$ -tori, not just those split by  $K$ ,

but the methods of §2 of [K3] still apply and yield the characterization above.

Now we use Fontaine-Messing's theory of crystalline representations [FM] to give a second construction of this isomorphism of functors  $X_*(\cdot)_\Gamma \rightarrow B(\cdot)$ . We start with a torus  $T$  split by  $K$  and an element  $\mu \in X_*(T)$ . Since  $X_*(T)$  is represented by  $(R_{K/\mathbb{Q}_p} \mathbb{G}_m, \mu_{\text{univ}})$ , there exists a unique morphism  $h: R_{K/\mathbb{Q}_p} \mathbb{G}_m \rightarrow T$  such that  $h \circ \mu_{\text{univ}} = \mu$ . On  $\mathbb{Q}_p$ -valued points  $h$  induces a homomorphism  $K^\times \rightarrow T(\mathbb{Q}_p)$  that we restrict to the units  $\mathcal{O}_K^\times$  in the valuation ring  $\mathcal{O}_K$  of  $K$ ; this yields a continuous homomorphism  $\mathcal{O}_K^\times \rightarrow T(\mathbb{Q}_p)$ , which by local classfield theory can also be thought of as a continuous homomorphism  $\tilde{h}: \text{Gal}(\bar{\mathbb{Q}}_p/K^{\text{un}}) \rightarrow T(\mathbb{Q}_p)$ .

Let  $V$  be any representation of  $T$  on a finite-dimensional vector space over  $\mathbb{Q}_p$ . Then the representation of  $\text{Gal}(\bar{\mathbb{Q}}_p/K^{\text{un}})$  on  $V$  obtained from  $\tilde{h}$  is crystalline in the sense of [FM]. Indeed it is enough to prove this statement in the universal case  $(R_{K/\mathbb{Q}} \mathbb{G}_m, \mu_{\text{univ}})$ , and since the category of crystalline representations is stable under direct sums, subobjects, tensor products, and duals, it is even enough to consider only the obvious representation of  $R_{K/\mathbb{Q}_p} \mathbb{G}_m$  on the  $\mathbb{Q}_p$ -vector space  $K$ . The corresponding representation of  $\text{Gal}(\bar{\mathbb{Q}}_p/K^{\text{un}})$  comes from any Lubin-Tate  $p$ -divisible group attached to  $K$ , and Fontaine [F] has shown that these representations are crystalline.

Let  $\mathcal{REP}(T)$  denote the neutral  $\mathbb{Q}_p$ -linear Tannakian category of finite-dimensional representations of the torus  $T$ , and let  $\mathcal{CR}(K)$  denote the neutral  $\mathbb{Q}_p$ -linear Tannakian category of finite-dimensional crystalline representations of  $\text{Gal}(\bar{\mathbb{Q}}_p/K^{\text{un}})$ . We have just described a tensor functor  $\mathcal{REP}(T) \rightarrow \mathcal{CR}(K)$ , compatible with the fiber functors on the two categories. Let  $\mathcal{CRYST}$  denote the  $\mathbb{Q}_p$ -linear Tannakian category of  $\Phi$ -isocrystals  $(V, \Phi)$  ( $V$  is a finite-dimensional vector space over  $L$  and  $\Phi$  is a  $\sigma$ -linear bijection  $\Phi: V \rightarrow V$ ), and consider the tensor functor  $\mathcal{CR}(K) \rightarrow \mathcal{CRYST}$  of [FM]. Composing it with  $\mathcal{REP}(T) \rightarrow \mathcal{CR}(K)$ , we get a tensor functor  $\mathcal{REP}(T) \rightarrow \mathcal{CRYST}$ .

Although  $\mathcal{CRYST}$  has no fiber functor over  $\mathbb{Q}_p$ , it does have one over  $L$ , namely, the functor  $(V, \Phi) \mapsto V$ . Composing this with our tensor functor  $\mathcal{REP}(T) \rightarrow \mathcal{CRYST}$  gives a nonstandard fiber functor over  $L$  on  $\mathcal{REP}(T)$ . The difference between this fiber functor and the standard one is measured by an  $L$ -torsor under  $T$  for the f.p.q.c topology on  $\text{Spec}(L)$ . By descent theory this torsor is represented by a scheme of finite type over  $L$  and hence has a point in some finite extension of  $L$ . Thus the difference between the two fiber functors is measured by an element of the Galois cohomology group  $H^1(L, T)$ , and this group vanishes by a theorem of Steinberg. We conclude that the two fiber functors are isomorphic, and we choose an isomorphism between them. Any two choices differ by an automorphism of the standard fiber functor over  $L$ , or in other words, by an element of  $T(L)$ .

The isomorphism we just chose allows us to think of the  $\Phi$ -isocrystal associated by our functor to an object  $V$  of  $\mathcal{REP}(T)$  as living on  $V_L := V \otimes_{\mathbb{Q}_p} L$ ; we write  $\Phi_V$  for the  $\sigma$ -linear bijection  $V_L \rightarrow V_L$  obtained in this way. On  $V_L$  we also have the obvious  $\sigma$ -linear map  $\sigma: V_L \rightarrow V_L$  given by  $\sigma := \text{id}_V \otimes \sigma$ , and

we define an element  $b_V \in \text{Aut}_L(V_L)$  by the equation  $\Phi_V = b_V\sigma$ . The family of elements  $b_V$  (for varying  $V$ ) forms an automorphism of the standard fiber functor of  $\mathcal{REP}(T)$  over  $L$ , hence there exists a unique element  $b \in T(L)$  inducing the family  $b_V$ . The element  $b \in T(L)$  depends on our choice of isomorphism between the two fiber functors, but the image of  $b$  in  $B(T)$  is independent of this choice. Thus, starting from  $\mu \in X_*(T)$ , we have constructed an element  $b \in B(T)$ . It is easy to see that this construction is functorial in  $T$ , so that we have defined a map of set-valued functors  $g: X_*(\cdot) \rightarrow B(\cdot)$  on  $\mathcal{T}$ . In the beginning of this section we defined a map of functors  $f: X_*(\cdot)_\Gamma \rightarrow B(\cdot)$ . Of course there is an obvious map of functors  $X_*(\cdot) \rightarrow X_*(\cdot)_\Gamma$ , call it  $q$ .

**Lemma 12.1.** *The map of functors  $g: X_*(\cdot) \rightarrow B(\cdot)$  is the negative of the composition of  $q: X_*(\cdot) \rightarrow X_*(\cdot)_\Gamma$  and  $f: X_*(\cdot)_\Gamma \rightarrow B(\cdot)$ .*

Since  $X_*(\cdot)$  is represented by  $(R_{K/\mathbb{Q}_p} \mathbb{G}_m, \mu_{\text{univ}})$ , it is enough to check that  $fq$  and  $g$  agree on  $\mu_{\text{univ}} \in X_*(R_{K/\mathbb{Q}_p} \mathbb{G}_m)$ . Consider the norm map  $R_{K/\mathbb{Q}_p} \mathbb{G}_m \rightarrow \mathbb{G}_m$ . It carries  $\mu_{\text{univ}}$  to the element  $1 \in \mathbb{Z} = X_*(\mathbb{G}_m)$ , and it induces an isomorphism  $B(R_{K/\mathbb{Q}_p} \mathbb{G}_m) \rightarrow B(\mathbb{G}_m)$ . Therefore it is enough to check that  $fq$  and  $g$  agree on  $1 \in \mathbb{Z} = X_*(\mathbb{G}_m)$ . To calculate the element  $b \in B(\mathbb{G}_m)$  obtained by applying  $g$  to  $1 \in \mathbb{Z} = X_*(\mathbb{G}_m)$  it is enough to consider the standard one-dimensional representation  $V$  of  $\mathbb{G}_m$  on  $\mathbb{Q}_p$ . Using Deligne's normalization of the isomorphism of local classfield theory, we get the Tate object  $\mathbb{Q}_p(1)$  as the  $\text{Gal}(\bar{\mathbb{Q}}_p/K^{\text{un}})$ -module associated to  $V$ . Applying the functor of Fontaine-Messing, we get the Tate object in  $\mathcal{CHYI}$ , and since  $\Phi$  is given by  $p^{-1}\sigma$  for the Tate object, we conclude that  $b$  is represented by  $p^{-1} \in \mathbb{G}_m(L)$ . Since  $fq$  carries  $1 \in \mathbb{Z} = X_*(\mathbb{G}_m)$  into the element of  $B(\mathbb{G}_m)$  represented by  $p \in \mathbb{G}_m(L)$ , the proof of Lemma 12.1 is now complete. Note that for this proof we did not need to know that the maps  $g: X_*(T) \rightarrow B(T)$  are group homomorphisms, but of course the lemma shows that this is indeed the case.

### 13. POLARIZED ABELIAN VARIETIES WITH CM

Let  $F$  be a CM-algebra, by which we mean a finite product of number fields, each of which is a totally complex quadratic extension of a totally real field. Let  $*$  be the unique positive involution on  $F$ ; on each factor of  $F \otimes_{\mathbb{Q}} \mathbb{R} \approx \mathbb{C} \times \dots \times \mathbb{C}$  it induces complex conjugation. We write  $T$  for the  $\mathbb{Q}$ -torus  $\{x \in F^\times \mid xx^* \in \mathbb{Q}^\times\}$ . The symbols  $K, \mathbb{Q}_p, K^{\text{un}}, L, \Gamma, \sigma$  will have the same meaning as in §12, but we will assume in addition that  $K$  is large enough that there are  $[F : \mathbb{Q}]$  distinct  $\mathbb{Q}$ -algebra maps  $F \rightarrow K$ , so that in particular  $T_{\mathbb{Q}_p}$  is split by  $K$ . Now suppose that  $A$  is an abelian variety over  $K$  with good reduction and with CM by  $F$ . We actually consider  $A$  as an abelian variety up to isogeny, so that having CM by  $F$  means that we are given an injection  $F \rightarrow \text{End}(A)$  and that  $2\dim(A) = [F : \mathbb{Q}]$ . The tangent space  $\text{Lie}(A)$  is a vector space of dimension  $[F : \mathbb{Q}]/2$  over  $K$  on which  $F$  acts. The group  $X_*(R_{(F \otimes_{\mathbb{Q}} K)/\mathbb{Q}_p} \mathbb{G}_m)$  is free with basis  $S := \text{Hom}_{\mathbb{Q}-\text{alg}}(F, K)$ , and exactly half of the elements in  $S$  appear in the representation of  $F$  on  $\text{Lie}(A)$ , each with multiplicity one. This subset  $S_A$

of  $S$  is called the CM-type of  $A$ . The involution  $*$  on  $F$  induces a map  $*$  on  $S$ , and  $S_A$  has the following property:  $(S_A)$  and  $S_A$  are disjoint and their union is  $S$ . Thus the cocharacter  $\mu := \sum_{s \in S_A} s$  of  $R_{(F \otimes_{\mathbb{Q}} \mathbb{Q}_p)/\mathbb{Q}_p} \mathbb{G}_m$  belongs to the subgroup  $X_*(T_{\mathbb{Q}_p})$ .

Suppose further that we are given a  $\mathbb{Q}$ -symmetrization  $\lambda : A \rightarrow \widehat{A}$  of the  $F$ -abelian variety  $A$  up to  $\mathbb{Q}$ -isogeny. Recall (see §9) that this means that  $\lambda$  is a symmetric isogeny  $\lambda : A \rightarrow \widehat{A}$  such that  $F \rightarrow \text{End}(A)$  is a  $*$ -homomorphism for  $*$  on  $F$  and the Rosati involution for  $\lambda$  on  $\text{End}(A)$ .

In this section we will use the following terminology: a symplectic space with CM by  $F$  over a field  $E$  of characteristic 0 is a representation of  $F$  on an  $E$ -vector space  $V$  together with a nondegenerate alternating form  $(\cdot, \cdot)$  on  $V$  such that  $(xv, w) = (v, x^*w)$  for all  $x \in F$  and all  $v, w \in V$ , satisfying the further requirement that  $V$  be free of rank 1 as  $F \otimes_{\mathbb{Q}} E$ -module. By an isomorphism  $f : V_1 \rightarrow V_2$  between two such objects we mean an  $E$ -linear isomorphism  $f$  commuting with the action of  $F$  and carrying the alternating form on  $V_2$  into a scalar multiple of the one on  $V_1$  (here scalar means an element of  $E^\times$ ).

We also use  $A$  to denote the Neron model of  $A$ , and  $A_k$  to denote its geometric fiber over the residue field  $\bar{k}$  of  $K^{\text{un}}$ . The first homology group  $H := H_1(A_{\mathbb{Q}_p}, \mathbb{Q}_p)$  is a symplectic space with CM by  $F$  over  $\mathbb{Q}_p$ . Write  $D$  for the  $\Phi$ -isocrystal dual to  $H_{\text{cris}}^1(A_{\bar{k}}/W(\bar{k})) \otimes_{W(\bar{k})} L$ ; then  $D$  is a symplectic space with CM by  $F$  over  $L$ . The isomorphism classes of symplectic spaces with CM by  $F$  over  $L$  are classified by  $H^1(L, T)$ , and this group is trivial by a theorem of Steinberg [St]. Choose an isomorphism of symplectic spaces with CM by  $F$  from  $H_L := H \otimes_{\mathbb{Q}_p} L$  to  $D$ , and use this to transport the  $\sigma$ -linear operator  $\Phi$  on  $D$  to a  $\sigma$ -linear bijection  $\Phi : H_L \rightarrow H_L$ . Write  $\Phi = b\sigma$ , where  $\sigma := \text{id}_H \otimes \sigma$ . Then  $b$  is an automorphism of the symplectic space  $H_L$  with CM by  $F$  and hence defines an element  $b \in T(L)$ . Changing the choice of isomorphism  $H_L \simeq D$  does not change the image of  $b$  in  $B(T_{\mathbb{Q}_p})$ .

**Lemma 13.1.** *The image of  $b$  in  $B(T_{\mathbb{Q}_p})$  is equal to the negative of the image of  $\mu \in X_*(T_{\mathbb{Q}_p})$  under the canonical isomorphism  $X_*(T_{\mathbb{Q}_p})_\Gamma \simeq B(T_{\mathbb{Q}_p})$  of [K3].*

The group  $\text{Gal}(\mathbb{Q}_p/K)$  operates on  $H$  by automorphisms of symplectic spaces with CM by  $F$ , and thus we get a homomorphism  $\text{Gal}(\mathbb{Q}_p/K) \rightarrow T(\mathbb{Q}_p)$ . Shimura and Taniyama [ST] proved that the restriction of this homomorphism to  $\text{Gal}(\mathbb{Q}_p/K^{\text{un}})$  is associated to  $\mu \in X_*(T_{\mathbb{Q}_p})$  by the procedure of §12 (recall once again that we are using Deligne's normalization of the isomorphism of local classfield theory). Applying the functor of Fontaine-Messing to  $H$ , we get a symplectic space  $D'$  with CM by  $F$  over  $L$ , together with a  $\sigma$ -linear bijection  $\Phi : D' \rightarrow D'$  commuting with  $F$  and satisfying  $(\Phi v, \Phi w) = p^{-1}\sigma(v, w)$  for all  $v, w \in D'$ . The comparison theorem of Fontaine-Messing and Faltings [Fa] implies that the isocrystal  $D'$  is canonically isomorphic to  $D$ . Moreover the isomorphism is compatible with the action of  $F$  (functoriality of the

comparison isomorphism) and with the alternating forms (compatibility of the comparison isomorphism with first Chern classes of line bundles). As in §12 we choose an isomorphism between two fiber functors on  $\mathcal{REP}(T)$  over  $L$ . In particular for the object  $H$  of  $\mathcal{REP}(T)$  we get an isomorphism  $H_L \simeq D' = D$  of symplectic spaces with CM by  $F$  over  $L$ . Lemma 13.1 now follows from Lemma 12.1.

Our next task is to use Lemma 13.1 to get information about polarized abelian varieties (up to isogeny) with CM by  $F$  over an algebraic closure  $\bar{k}$  of  $\mathbb{F}_p$ . The symbols  $F$ ,  $*$ ,  $T$  have the same meaning as before. We consider an abelian variety  $A$  up to isogeny of dimension  $[F : \mathbb{Q}]/2$  over  $\bar{k}$  together with an injective  $\mathbb{Q}$ -algebra map  $F \rightarrow \text{End}(A)$ . We suppose further that we are given a  $\mathbb{Q}$ -polarization  $\lambda: A \rightarrow \widehat{A}$  of the  $F$ -abelian variety  $A$  up to  $\mathbb{Q}$ -isogeny.

Let  $V$  be a symplectic space with CM by  $F$  over  $\mathbb{Q}$ . The torus  $T$  is the group of automorphisms of  $V$ . We write  $\widehat{T}$  for the complex torus dual to  $T$ . We choose an algebraic closure  $\bar{\mathbb{Q}}$  of  $\mathbb{Q}$  as well as algebraic closures  $\bar{\mathbb{Q}}_v$  of  $\mathbb{Q}_v$  for every place  $v$  of  $\mathbb{Q}$ . We also choose embeddings  $\bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}_v$  for every place  $v$  of  $\mathbb{Q}$ . We write  $\Gamma$  for  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  and  $\Gamma(v)$  for  $\text{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v)$ ; our embedding  $\bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}_v$  induces an injection  $\Gamma(v) \rightarrow \Gamma$ . The group  $\Gamma$  (and its subgroups  $\Gamma(v)$ ) act on  $\widehat{T}$ . Recall (see [K2, K3]) that there are canonical isomorphisms

- (1)  $H^1(\mathbb{Q}_v, T) \simeq X^*(\pi_0(\widehat{T}^{\Gamma(v)}))$  for all  $v$ ,
- (2)  $B(T_{\mathbb{Q}_p}) \simeq X^*(\widehat{T}^{\Gamma(p)})$ ,

where  $\pi_0(\widehat{T}^{\Gamma(v)})$  denotes the quotient of  $\widehat{T}^{\Gamma(v)}$  by its identity component.

For each prime  $l$  different from  $p$  we get a symplectic space  $H_l(A, \mathbb{Q}_l)$  with CM by  $F$  over  $\mathbb{Q}_l$ . It differs from  $V_{\mathbb{Q}_l}$  by an element of  $H^1(\mathbb{Q}_l, T) \simeq X^*(\pi_0(\widehat{T}^{\Gamma(l)}))$ ; we denote by  $\alpha(l)$  this character on  $\widehat{T}^{\Gamma(l)}$  (trivial on the identity component of  $\widehat{T}^{\Gamma(l)}$ ).

For the prime  $p$  we have the isocrystal  $D$  dual to  $H_{\text{cris}}^1(A/W(\bar{k})) \otimes_{W(\bar{k})} L$ . Moreover  $D$  is a symplectic space with CM by  $F$  over  $L$ , and the  $\sigma$ -linear bijection  $\Phi: D \rightarrow D$  commutes with the action of  $F$  and satisfies the equality  $(\Phi v, \Phi w) = p^{-1}\sigma(v, w)$  for all  $v, w \in D$ . Using once again that any two symplectic spaces with CM by  $F$  over  $L$  are isomorphic, we choose an isomorphism  $V_L \simeq D$  and use it to transport  $\Phi$  to  $V_L$ . As before we write  $\Phi = b\sigma$  for  $b \in T(L)$ ; then the image of  $b$  in  $B(T_{\mathbb{Q}_p}) \simeq X^*(\widehat{T}^{\Gamma(p)})$  is independent of the choice of isomorphism  $V_L \simeq D$ , and we denote by  $\alpha(p)$  this character on  $\widehat{T}^{\Gamma(p)}$ .

Finally consider the infinite place  $\infty$  of  $\mathbb{Q}$ . By Lemma 4.3 there is a unique  $\mathbb{R}$ -algebra  $*$ -homomorphism  $h: \mathbb{C} \rightarrow \text{End}_F(V_{\mathbb{R}}) = F \otimes_{\mathbb{Q}} \mathbb{R}$  such that the symmetric bilinear form  $(v, h(i)w)$  on  $V_{\mathbb{R}}$  is positive definite. The restriction of  $h$  to  $\mathbb{C}^\times$  is a homomorphism of algebraic groups  $h: \mathbb{C}^\times \rightarrow T_{\mathbb{R}}$ . As in (2) of Lemma 4.1 the homomorphism  $h$  gives us a homomorphism  $\mu_h: \mathbb{G}_m \rightarrow T_{\mathbb{C}}$ , or, in other words, an element  $\mu_h \in X_*(T_{\mathbb{C}}) = X^*(\widehat{T})$ . Restricting  $\mu_h$  to  $\widehat{T}^{\Gamma(\infty)}$  gives us a character  $\alpha(\infty)$  on  $\widehat{T}^{\Gamma(\infty)}$ . Note that  $\alpha(\infty)$  is independent of the choice of  $i = (-1)^{1/2}$  in  $\mathbb{C}$ .

We have now defined a character  $\alpha(v)$  on  $\widehat{T}^{\Gamma(v)}$  for every place  $v$  of  $\mathbb{Q}$ , and all but a finite number of them are trivial. Restrict each  $\alpha(v)$  to the subgroup  $\widehat{T}^\Gamma$  of  $\widehat{T}^{\Gamma(v)}$  and take the product over all places  $v$  of these characters on  $\widehat{T}^\Gamma$ ; this yields a character on  $\widehat{T}^\Gamma$  that we will denote by  $\alpha$ . Note that the restriction of  $\alpha(v)$  to  $\widehat{T}^\Gamma$  is independent of the choice of embedding  $\bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}_v$ , and hence that  $\alpha$  is independent of the choice of these embeddings.

**Lemma 13.2.** *The character  $\alpha$  on  $\widehat{T}^\Gamma$  is trivial.*

First note that  $\alpha$  is independent of the choice of symplectic space  $V$  with CM by  $F$  over  $\mathbb{Q}$ . Indeed, any other such space  $V'$  differs from  $V$  by an element  $t \in H^1(\mathbb{Q}, T)$ . Writing  $t_v$  for the image of  $t$  under

$$H^1(\mathbb{Q}, T) \rightarrow H^1(\mathbb{Q}_v, T) \simeq X^*(\pi_0(\widehat{T}^{\Gamma(v)})),$$

one checks that  $\alpha'(v)$  (the analog for  $V'$  of  $\alpha(v)$  for  $V$ ) is given by  $\alpha'(v) = \alpha(v) - t_v$ . It follows from Tate-Nakayama duality (in the form given in the introduction to [K4]) that the product of the restrictions of the characters  $t_v$  to  $\widehat{T}^\Gamma$  is trivial and hence that  $\alpha$  is the same for  $V'$  as it is for  $V$ .

Next note that  $\alpha$  is independent of the choice of polarization  $\lambda$  of the  $F$ -abelian variety  $A$ . Indeed, any other such polarization  $\lambda'$  is given by  $\lambda f$  where  $f \in F_{\text{sym}}^\times$  and the image of  $f$  in  $(F \otimes_{\mathbb{Q}} \mathbb{R})_{\text{sym}}$  lies in the cone  $(F \otimes_{\mathbb{Q}} \mathbb{R})_+$  (apply Lemma 9.1). The discussion in §1 shows that  $F_{\text{sym}}^\times$  can be identified with the  $\mathbb{Q}$ -rational points of the quotient of the  $\mathbb{Q}$ -torus  $F^\times$  by the subtorus  $T_1 = \{x \in F^\times \mid xx^* = 1\}$ . Therefore the coboundary map for the exact sequence

$$1 \rightarrow T_1 \rightarrow F^\times \rightarrow F^\times/T_1 \rightarrow 1$$

associates to  $f \in F_{\text{sym}}^\times$  an element  $t_1 \in H^1(\mathbb{Q}, T_1)$ , whose image under

$$H^1(\mathbb{Q}, T_1) \rightarrow H^1(\mathbb{Q}, T) \rightarrow H^1(\mathbb{Q}_v, T) \simeq X^*(\pi_0(\widehat{T}^{\Gamma(v)}))$$

we denote by  $t_v$ . Then one checks that  $\alpha'(v)$  (the analog for  $\lambda'$  of  $\alpha(v)$  for  $\lambda$ ) is given by  $\alpha'(v) = \alpha(v) + t_v$ . As before Tate-Nakayama duality implies that  $\alpha$  is independent of  $\lambda$ .

Now we are ready to derive Lemma 13.2 from Lemma 13.1. The image of  $F$  in  $\text{End}(A)$  is a maximal commutative semisimple subalgebra of that semisimple  $\mathbb{Q}$ -algebra, and therefore the CM-algebra  $F$  splits  $\text{End}(A)$ . Tate [T3] proved that  $A$  is isogenous to the geometric special fiber of an abelian scheme with CM by  $F$  over the ring of integers in a  $p$ -adic field  $K$  (he was working with CM-fields and simple abelian varieties, but his proof goes through unchanged in our slightly more general case). Thus, in proving Lemma 13.2 we may revert to the situation at the beginning of this section, so that  $A$  now denotes an abelian variety over  $K$  and  $A_{\bar{k}}$  is its geometric special fiber. At that time, however, we allowed  $\lambda$  to be any  $\mathbb{Q}$ -symmetrization  $\lambda: A \rightarrow \widehat{A}$  of the  $F$ -abelian variety  $A$  over  $K$ . Now we take  $\lambda$  to be any  $\mathbb{Q}$ -polarization of  $A$  (for existence appeal to Lemma 9.2). Note that the  $\mathbb{Q}$ -symmetrization  $\bar{\lambda}: A_{\bar{k}} \rightarrow \widehat{A}_{\bar{k}}$  of  $A_{\bar{k}}$  induced

by  $\lambda: A \rightarrow \widehat{A}$  is actually a  $\mathbb{Q}$ -polarization, as we saw in §5 while verifying the valuative criterion of properness.

Since  $\alpha$  is independent of the choice of polarization of  $A_{\bar{k}}$ , we are free to take  $\bar{\lambda}$ . We are also free to use any symplectic space  $V$  with CM by  $F$  over  $\mathbb{Q}$ . The most convenient choice is  $V = H_1(A_{\mathbb{C}}, \mathbb{Q})$ , where  $A_{\mathbb{C}}$  is obtained from  $A$  by extension of scalars for some isomorphism  $\mathbb{Q}_p \rightarrow \mathbb{C}$  compatible with our chosen embeddings  $\mathbb{Q} \rightarrow \mathbb{Q}_p$  and  $\mathbb{Q} \rightarrow \mathbb{C}$ .

We need to determine the characters  $\alpha(v) \in X^*(\widehat{T}^{\Gamma(v)})$  for these choices of  $\bar{\lambda}, V$ . For any prime  $l$  different from  $p$  the isomorphism

$$H_1(A_{\bar{k}}, \mathbb{Q}_l) \simeq H_1(A_{\mathbb{Q}_p}, \mathbb{Q}_l) = H_1(A_{\mathbb{C}}, \mathbb{Q}_l) = V_{\mathbb{Q}_l}$$

of symplectic spaces with CM by  $F$  shows that  $\alpha(l)$  is trivial. As before the action of  $F$  on  $\text{Lie}(A)$  determines a cocharacter  $\mu \in X_*(T_{\mathbb{Q}_p}) = X^*(\widehat{T})$ , and Lemma 13.1 implies (in view of the isomorphism  $H_1(A_{\mathbb{Q}_p}, \mathbb{Q}_p) \simeq V_{\mathbb{Q}_p}$ )

that  $\alpha(p)$  is the negative of the restriction of  $\mu$  to  $\widehat{T}^{\Gamma(p)}$ . To get  $\alpha(\infty)$  we need to use the unique  $*$ -homomorphism  $\mathbb{C} \rightarrow \text{End}_F(V_{\mathbb{R}})$  such that  $(v, h(i)w)$  is positive definite on  $V_{\mathbb{R}}$ . Since  $\lambda$  is a polarization, the canonical complex structure  $h: \mathbb{C} \rightarrow \text{End}(V_{\mathbb{R}})$  on  $V_{\mathbb{R}} = H_1(A_{\mathbb{C}}, \mathbb{R}) = \text{Lie}(A_{\mathbb{C}})$  is the required  $h$ . From this  $h$  we get  $\mu_h \in X_*(T_{\mathbb{R}}) = X^*(\widehat{T})$  and  $\alpha(\infty)$  is the restriction of  $\mu_h$  to  $\widehat{T}^{\Gamma(\infty)}$ . Since  $\mathbb{Q}_p \rightarrow \mathbb{C}$  was chosen to be compatible with  $\mathbb{Q} \rightarrow \mathbb{Q}_p$  and  $\mathbb{Q} \rightarrow \mathbb{C}$ , the elements  $\mu$  and  $\mu_h$  of  $X^*(\widehat{T})$  are equal. This proves Lemma 13.2.

#### 14. CONSTRUCTION OF $(\gamma_0; \gamma, \delta)$ FROM $(A, \lambda, i)$

Let  $p, B, *, F, F_0, \mathcal{O}_B, V, (\cdot, \cdot), C, G, G_1, h, E$  be as in §5. However, we now consider only Cases A and C; in fact Case D will be excluded for the rest of this paper. Let  $\bar{k}, \sigma, r, k_r, L, L_r$  have the same meaning as in §10. Let  $c$  be a positive rational number of the form  $p^r c_0$  where  $c_0$  is a  $p$ -adic unit. Let  $A = (\bar{A}, u)$  be a virtual abelian variety over  $k_r$  up to isogeny, let  $i: B \rightarrow \text{End}(A)$  be a ring homomorphism, and let  $\lambda: A \rightarrow \widehat{A}$  be a  $c$ -polarization of the virtual abelian variety  $A$  such that  $\lambda \in \text{Hom}_B(A, \widehat{A})$ . Thus  $(A, \lambda, i)$  is a  $c$ -polarized virtual  $B$ -abelian variety over  $k_r$  up to isogeny.

We are going to make three assumptions on  $(A, \lambda, i)$ . Under these assumptions we will associate to  $(A, \lambda, i)$  a triple  $(\gamma_0; \gamma, \delta)$  of the type considered in §2 of [K5].

The first assumption is that the skew-Hermitian  $B$ -module  $H_1(\bar{A}, \mathbb{A}_f^p)$  be isomorphic to  $V \otimes_{\mathbb{Q}} \mathbb{A}_f^p$ . Choose an isomorphism  $H_1(\bar{A}, \mathbb{A}_f^p) \simeq V \otimes_{\mathbb{Q}} \mathbb{A}_f^p$  of skew-Hermitian  $B$ -modules. The Frobenius element  $\pi_A$  for  $A$  is an automorphism of the skew-Hermitian  $B$ -module  $H_1(\bar{A}, \mathbb{A}_f^p)$  (recall that our isomorphisms and automorphisms need only preserve the alternating form up to a scalar), and by means of the isomorphism we just chose,  $\pi_A$  can be viewed as an element  $\pi_A \in G(\mathbb{A}_f^p)$ . We take for  $\gamma$  the inverse of  $\pi_A$ ; it is an element of  $G(\mathbb{A}_f^p)$  whose conjugacy class is independent of the choice of isomorphism between  $H_1(\bar{A}, \mathbb{A}_f^p)$  and  $V \otimes_{\mathbb{Q}} \mathbb{A}_f^p$ .

From  $(A, \lambda, i)$  we get (see §10) a skew-Hermitian  $B$ -module  $H$  over  $L_r$ , together with a  $\sigma$ -linear bijection  $\Phi: H \rightarrow H$  commuting with  $B$  and satisfying  $(\Phi v, \Phi w) = c' \sigma(v, w)$  for all  $v, w \in H$ , where  $c'$  is some element of  $L_r^\times$  whose norm down to  $\mathbb{Q}_p^\times$  is  $c^{-1}$ . The second assumption on  $(A, \lambda, i)$  is that the skew-Hermitian  $B$ -module  $H$  be isomorphic to  $V \otimes_{\mathbb{Q}} L_r$ . Choose an isomorphism  $H \simeq V \otimes_{\mathbb{Q}} L_r$  of skew-Hermitian  $B$ -modules and use it to carry  $\Phi$  over to a  $\sigma$ -linear bijection  $\Phi: V \otimes_{\mathbb{Q}} L_r \rightarrow V \otimes_{\mathbb{Q}} L_r$ . As usual we then write  $\Phi = \delta \sigma$  for a linear automorphism  $\delta$  of  $V \otimes_{\mathbb{Q}} L_r$ , where  $\sigma$  is the  $\sigma$ -linear bijection  $\text{id}_V \otimes \sigma$  from  $V \otimes_{\mathbb{Q}} L_r$  to itself. Then  $\delta \in G(L_r)$  and changing our choice of isomorphism replaces  $\delta$  by a  $\sigma$ -conjugate  $x \delta \sigma(x)^{-1}$  ( $x \in G(L_r)$ ); in particular, the  $\sigma$ -conjugacy class of  $\delta \in G(L_r)$  is well defined.

Consider the canonical map

$$B(G_{\mathbb{Q}_p}) \rightarrow X^*(Z(\widehat{G})^{\Gamma(p)})$$

of §6 of [K5]. Applying this map to the element of  $B(G_{\mathbb{Q}_p})$  represented by  $\delta$ , we get an element of  $X^*(Z(\widehat{G})^{\Gamma(p)})$ . The third assumption on  $(A, \lambda, i)$  is that this element of  $X^*(Z(\widehat{G})^{\Gamma(p)})$  be equal to the element  $\mu_1$  constructed from  $\mu_h$  in §2 of [K5].

We have constructed  $\gamma, \delta$ , and it remains to construct  $\gamma_0$ . Let  $M$  be the semisimple  $\mathbb{Q}$ -algebra  $\text{End}_B(A)$ . The Rosati involution for  $\lambda$  preserves  $\text{End}_B(A)$ , giving a positive involution  $*$  on  $M$ . Let  $I$  be the  $\mathbb{Q}$ -group of automorphisms of  $(A, \lambda, i)$ ; thus

$$I(R) = \{x \in M_R \mid x x^* \in R^\times\}$$

for any  $\mathbb{Q}$ -algebra  $R$ . We also have the subgroup  $I_1$  given by

$$I_1(R) = \{x \in M_R \mid x x^* = 1\};$$

since  $*$  is positive the group  $(I_1)_{\mathbb{R}}$  is anisotropic over  $\mathbb{R}$ .

It follows from Lemma 10.7 that for any prime  $l$  different from  $p$  the group  $I_{\mathbb{Q}_l}$  is isomorphic to the centralizer of  $\gamma_l$  in  $G_{\mathbb{Q}_l}$ , where  $\gamma_l$  denotes the  $\mathbb{Q}_l$ -component of  $\gamma \in G(\mathbb{A}_f^p)$ . Since  $\pi_A$  is central in  $M$ , the element  $\gamma_l$  is semisimple. Recall that we are in Case A or C. In a general linear group over an algebraically closed field the centralizer of any semisimple element is a product of general linear groups, and in a symplectic group over an algebraically closed field the centralizer of any semisimple element is a product of general linear groups and symplectic groups. Therefore in both cases the group  $I_1$  becomes a product of general linear groups and symplectic groups after extending scalars to  $\mathbb{Q}_l$ .

Let  $T$  be a maximal torus in  $I$ . Its centralizer in  $M$  is a maximal commutative semisimple subalgebra  $N$  of  $M$ ; moreover, the involution  $*$  preserves  $N$  and  $N$  is free of rank 2 over its subalgebra  $N_0 := \{x \in N \mid x^* = x\}$  (use that no factor of  $I_1$  is an orthogonal group in an odd number of variables; actually, as we have just seen,  $I_1$  has no orthogonal factors at all). The torus  $T$  can be recovered from  $N$  as follows:

$$T(R) = \{x \in N_R \mid x x^* \in R^\times\}.$$

Since  $I$  is isomorphic over  $\mathbb{Q}_l$  to the centralizer  $G_{\gamma_l}$  of  $\gamma_l$  in  $G_{\mathbb{Q}_l}$ , the torus  $T$  has the same dimension as the maximal tori in  $G$ . Therefore  $N$ , which is naturally an  $F$ -algebra, has the same dimension over  $F$  as the maximal commutative semisimple subalgebras of  $C = \text{End}_B(V)$ , namely,  $(\dim_F C)^{1/2}$ .

Since  $\dim_F(N) = (\dim_F C)^{1/2}$ , there exists an  $F$ -algebra embedding  $N \rightarrow C$  if and only if  $N \otimes_F C$  is a matrix algebra over  $N$ , and any two such embeddings are conjugate under  $C^\times$ . This statement is well known, but we will recall its proof in order to give motivation for the proof of Lemma 14.1. Giving  $N \rightarrow C$  is the same as giving a left  $C \otimes_F N$ -module structure on  $C$  that extends the natural left  $C$ -module structure on  $C$  (use that  $\text{End}_C(C) = C^{\text{opp}}$  and that giving  $N \rightarrow C$  is the same as giving  $N \rightarrow C^{\text{opp}}$ ). Moreover two homomorphisms  $N \rightarrow C$  are conjugate under  $C^\times$  if and only if the corresponding  $C \otimes_F N$ -modules are isomorphic. Factor  $N$  as a product of field extensions  $N_1, \dots, N_t$  of  $F$ . Then  $C \otimes_F N$  has  $t$  simple left modules, and  $N \rightarrow C$  is an embedding if and only if each of these simple modules occurs at least once in the corresponding  $C \otimes_F N$ -module. Since  $C$ -modules are determined up to isomorphism by their  $F$ -dimensions, our problem reduces to determining the isomorphism classes of  $C \otimes_F N$ -modules  $W$  containing each simple module at least once and having  $F$ -dimension equal to that of  $C$ . Since the  $N_i$ -dimension of the simple  $C \otimes_F N$ -module corresponding to  $N_i$  is greater than or equal to  $(\dim_F C)^{1/2} = [N : F]$ , with equality if and only if  $C \otimes_F N_i$  is a matrix algebra, no such module  $W$  exists unless each  $C \otimes_F N_i$  is a matrix algebra, in which case  $W$  is isomorphic to a direct sum of one copy of each of the  $t$  simple modules for  $C \otimes_F N$ . A central simple algebra over  $N_i$  is a matrix algebra if and only if this is so locally, and the discussion above shows that  $N$  can be embedded (over  $F$ ) in  $C$  if and only if this is so locally for each place of  $F$ . Let us check that these local embeddings exist in our situation.

For any prime  $l$  different from  $p$  we have chosen an isomorphism  $H_1(\bar{A}, \mathbb{Q}_l) \simeq V \otimes_{\mathbb{Q}} \mathbb{Q}_l$  of skew-Hermitian  $B$ -modules. It follows from Lemma 10.7 that  $M_l$  embeds (as  $F_l$ -algebra) in  $\text{End}_B(V_l) = C_l$ , where we are using a subscript  $l$  to denote extension of scalars from  $\mathbb{Q}$  to  $\mathbb{Q}_l$ . This takes care of places of  $F$  lying over  $l$ , since  $N$  is an  $F$ -subalgebra of  $M$ . For places of  $F$  lying over  $p$  there is nothing to do since we have assumed that  $B$  splits at such places and this implies the same for  $C$  and  $C \otimes_F N$ . For infinite places of  $F$  we need only remark that every infinite place of  $N$  is complex (use that  $*$  is a positive involution on  $N$  and that  $N$  is free of rank 2 over  $N_0$ ).

We have now shown that there exists an  $F$ -algebra embedding  $i: N \rightarrow C$ , unique up to conjugacy under  $C^\times$ .

**Lemma 14.1.** *There exists an  $F$ -algebra embedding  $i: N \rightarrow C$  that is a  $*$ -homomorphism.*

Start by choosing an  $F$ -algebra embedding  $i: N \rightarrow C$ . We need to show that some  $C^\times$ -conjugate of  $i$  is a  $*$ -homomorphism. As before we use  $i$  to regard  $C$  as a left  $C \otimes_F N$ -module. Then  $i: N \rightarrow C$  is itself a  $*$ -homomorphism if and only if the standard  $F$ -valued  $C \otimes_F C^{\text{opp}}$ -Hermitian form  $(x, y)_1 := \text{tr}_{C/F}(xy^*)$

on  $C$  is  $C \otimes_F N$ -Hermitian as well. It follows that  $i$  is conjugate under  $C^\times$  to a  $*$ -homomorphism if and only if there is a  $C \otimes_F N$ -Hermitian form  $(\cdot, \cdot)$  on  $C$  that is equivalent as a  $C$ -Hermitian form to  $(\cdot, \cdot)_1$ .

For any prime  $l$  different from  $p$  the embedding  $i: N_l \rightarrow C_l$  is conjugate under  $C_l^\times$  to a  $*$ -homomorphism, namely, the embedding  $N_l \hookrightarrow M_l \hookrightarrow C_l$  discussed earlier. Consider the  $F_0$ -vector space  $W$  of all  $C \otimes_F N$ -Hermitian forms on  $C$ . Inside this vector space we have the Zariski open subset of non-degenerate  $C \otimes_F N$ -Hermitian forms. The discussion for  $l \neq p$  shows that this Zariski open subset is nonempty. Since the  $F_0$ -rational points of  $W$  (regarded as variety over  $F_0$ ) are Zariski dense in  $W$ , it follows that there exists a nondegenerate  $C \otimes_F N$ -Hermitian form  $(\cdot, \cdot)'$  on  $C$ .

The difference between  $(\cdot, \cdot)'$  and  $(\cdot, \cdot)_1$  as  $C$ -Hermitian forms is measured by an element  $\alpha \in H^1(F_0, A)$ , where  $A$  is the  $F_0$ -group of automorphisms of the  $C$ -Hermitian module  $(C, (\cdot, \cdot)')$  (here, for a change, we mean automorphisms preserving  $(\cdot, \cdot)'$ , not just preserving it up to a scalar). Since  $\text{End}_{C \otimes_F N}(C) = N$ , we see that the group of automorphisms of the  $C \otimes_F N$ -Hermitian module  $(C, (\cdot, \cdot)')$  is the  $F_0$ -torus  $T_0 = \{x \in N | xx^* = 1\}$ . The embedding  $i: N \rightarrow C$  is conjugate to a  $*$ -homomorphism if and only if there is another  $C \otimes_F N$ -Hermitian form  $(\cdot, \cdot)$  on  $C$  (differing from  $(\cdot, \cdot)'$  by an element of  $H^1(F_0, T_0)$ ) that is equivalent to  $(\cdot, \cdot)_1$  as a  $C$ -Hermitian form, and this happens if and only if the element  $\alpha$  is in the image of

$$H^1(F_0, T_0) \rightarrow H^1(F_0, A).$$

The group  $A$  is a reductive group over  $F_0$ , and since we are in Case A or C, it is connected as well. The element  $\alpha \in H^1(F_0, A)$  lies in the image of  $H^1(F_0, T)$  if and only if the maximal torus  $T_0$  of  $A$  transfers to the inner form  $A_\alpha$  of  $A$  obtained by using  $\alpha$  to twist  $A$  (see §9 of [K2] for a review of the notion of transferring tori to inner forms). It follows from what we have already done that  $T_0$  transfers to  $A_\alpha$  locally for all places of  $F_0$  away from  $p$  and  $\infty$ . The group  $A_\alpha$  is the  $F_0$ -group  $\{x \in C | xx^* = 1\}$ , and the hypotheses made in §5 guarantee that  $A_\alpha$  is an unramified group at places of  $F_0$  over  $p$  and in particular that  $A_\alpha$  is quasi-split at such places. It is well known that any maximal torus transfers to the quasi-split form, and we conclude that  $T_0$  transfers to  $A_\alpha$  at all  $p$ -adic places of  $F_0$ . The infinite places of  $F_0$  are real and at each such place  $T_0$  is anisotropic (again use that  $*$  is a positive involution on  $N$ ), and it is well known that anisotropic tori in groups over local fields transfer to all inner forms. Therefore  $T_0$  transfers to  $A_\alpha$  locally at every place of  $F_0$ .

The obstruction (due to Langlands [L5] and constructed another way in §9 of [K2]) to transferring  $T_0$  to  $A_\alpha$  lies in  $\ker^2(F_0, U)$  (locally trivial elements in  $H^2(F_0, U)$ ), where  $U$  denotes the  $F_0$ -torus obtained by taking the intersection of  $T_0$  with the derived group of  $A$  (this derived group is simply connected in our case). By Tate-Nakayama duality for  $U$  the group  $\ker^2(F_0, U)$  is dual to

$\ker^1(F_0, X^*(U))$ , which may in turn be identified with

$$\ker[\pi_0(\widehat{U}^\Gamma) \rightarrow \prod_v \pi_0(\widehat{U}^{\Gamma(v)})],$$

with notation as in [K2] (in particular  $\Gamma = \text{Gal}(\bar{F}/F_0)$  for the moment). Therefore  $\ker^2(F_0, U)$  vanishes if there is any place  $v$  of  $F_0$  such that  $X^*(U)^\Gamma = X^*(U)^{\Gamma(v)}$  (so that the identity components of  $\widehat{U}^\Gamma$  and  $\widehat{U}^{\Gamma(v)}$  coincide). This happens in our case since  $T_0$  (and hence  $U$ ) is anisotropic at every infinite place of  $F_0$ . We conclude that  $T_0$  transfers to  $A_\alpha$ , and the proof of the lemma is complete.

Recall that we are trying to associate a triple  $(\gamma_0; \gamma, \delta)$  to  $(A, \lambda, i)$  and that we have already constructed  $\gamma, \delta$ . Lemma 14.1 allows us to construct  $\gamma_0$ . Choose a  $*$ -homomorphism  $i: N \rightarrow C$  (as in the lemma). The Frobenius element  $\pi_A$  of  $A$  belongs to the center of  $M = \text{End}_B(A)$  and therefore belongs to the maximal commutative semisimple subalgebra  $N$  of  $M$ . Since  $A$  is  $c$ -polarizable, we have  $\pi_A \pi_A^* = c$  and therefore  $\pi_A$  gives an element  $\pi_A \in T(\mathbb{Q})$ . We first define an element  $\gamma_0 \in T(\mathbb{Q})$  by taking the inverse of  $\pi_A$ . Then, using the  $*$ -homomorphism  $N \rightarrow C$  to embed  $T$  in  $G$  over  $\mathbb{Q}$ , we regard  $\gamma_0$  as an element of  $G(\mathbb{Q})$ . Of course  $\gamma_0 \in G(\mathbb{Q})$  depends on the choice of embedding  $i$ , but since any two such embedding are conjugate under  $G(\bar{\mathbb{Q}})$ , the stable conjugacy class of  $\gamma_0$  is well defined.

We finally have the desired triple  $(\gamma_0; \gamma, \delta)$ , but we still must show that it satisfies all the conditions imposed in §2 of [K5]. It is clear that  $\gamma_0$  is semisimple and that it is elliptic in  $G(\mathbb{R})$ . It is also clear that  $\gamma_0$  is conjugate under  $C_l^\times$  to the  $l$ -adic component  $\gamma_l$  of  $\gamma$  for all  $l$  different from  $p$ . Moreover, both  $\gamma_l$  and  $\gamma_0$  have image  $c^{-1}$  under the usual homomorphism  $G \rightarrow \mathbb{G}_m$ , and it follows from Lemma 7.1 that  $\gamma_l$  and  $\gamma_0$  are conjugate in  $G(\bar{\mathbb{Q}})$ .

Once again let  $H$  denote the  $L_r$ -vector space with  $\sigma$ -linear bijection  $\Phi$  that we get from  $A$ . We have chosen an isomorphism  $H \simeq V \otimes_{\mathbb{Q}} L_r$  of skew-Hermitian  $B$ -modules; use it to regard  $\pi_A^{-1}$  as an element  $\gamma_p \in G(L_r)$ . Then the equality  $\Phi' = \pi_A^{-1}$  shows that  $N\delta = \gamma_p$ . On the other hand it is again clear that  $\gamma_p$  is conjugate to  $\gamma_0$  under  $(C \otimes_{\mathbb{Q}} L_r)^\times$  and that both  $\gamma_p$  and  $\gamma_0$  have image  $c^{-1}$  under  $G \rightarrow \mathbb{G}_m$ , and once again Lemma 7.1 shows that  $N\delta$  is conjugate to  $\gamma_0$  in  $G(\bar{L}_r)$ . Since we have imposed the second condition of §2 of [K5] on  $\delta$  as one of our three hypotheses on  $(A, \lambda, i)$ , we are now finished verifying that  $(\gamma_0; \gamma, \delta)$  satisfies all the conditions of §2 of [K5].

There is one last task in this section. We have the  $\mathbb{Q}$ -group  $I$  (automorphisms of the triple  $(A, \lambda, i)$ ) and another  $\mathbb{Q}$ -group  $I_0 := G_{\gamma_0}$ , the centralizer of  $\gamma_0$  in  $G$ . By Lemma 10.7 (respectively, Lemma 10.8) the group  $I_{\mathbb{Q}_l}$  (respectively,  $I_{\mathbb{Q}_p}$ ) is isomorphic to  $G_{\gamma_l}$  (respectively,  $G_{\delta\sigma}$ , the twisted centralizer of  $\delta$ ), where  $\gamma_l$  denotes the  $l$ -adic component of  $\gamma$  for a prime  $l \neq p$ . Since  $\gamma_0$  and  $\gamma_l$  (respectively,  $N\delta$ ) are stably conjugate, there are inner twistings  $\psi_v: I_0 \rightarrow I$  over  $\mathbb{Q}_v$ , canonical up to inner automorphisms of  $I_0$  over  $\mathbb{Q}_v$ , for every finite place  $v$  of  $\mathbb{Q}$ .

Let  $M_0$  denote the centralizer of  $\gamma_0$  in the algebra  $C$ . Then the involution  $*$  on  $C$  preserves  $M_0$ . The functor  $\Psi$  taking a  $\mathbb{Q}$ -algebra  $R$  to the set  $\Psi(R)$  of  $*$ -isomorphisms of  $F$ -algebras from  $M_0$  to  $M = \text{End}_B(A)$  over  $R$  carrying  $\gamma_0$  into  $\pi_A^{-1}$  is representable by a scheme of finite type over  $\mathbb{Q}$  (in fact a locally closed subscheme of the affine space  $\text{Hom}(M_0, M)$ ). When  $R$  is an algebraically closed field, every  $F$ -algebra automorphism of  $(M_0, *)$  over  $R$  carrying  $\gamma_0$  into itself comes from an inner automorphism of  $I_0$  over  $R$ ; therefore an element of  $\Psi(R)$  induces an inner twisting  $I_0 \rightarrow I$ . For every finite place  $v$  of  $\mathbb{Q}$  the set  $\Psi(\mathbb{Q}_v)$  is nonempty and the inner twisting  $\psi_v$  comes from some element of  $\Psi(\mathbb{Q}_v)$ . In particular the scheme  $\Psi$  is nonempty and hence has a  $\mathbb{Q}$ -valued point  $\psi \in \Psi(\mathbb{Q})$ , inducing an inner twisting  $\psi: I_0 \rightarrow I$  over  $\mathbb{Q}$  that differs from  $\psi_v$  by an inner automorphism of  $I_0$  over  $\mathbb{Q}_v$ . Since  $I_{\mathbb{R}}$  is anisotropic modulo  $\mathbb{G}_m$  (use that  $*$  is positive), it follows that the inner twisting  $\psi_{\infty}: I_0 \rightarrow I$  over  $\mathbb{C}$  obtained from  $\psi$  is equivalent to the inner twisting  $\psi_{\infty}: I_0 \rightarrow I(\infty)$  constructed in §3 of [K5] (use that there is a unique element of  $H^1(\mathbb{R}, I_2)$  corresponding to the compact form of  $I_0$ , where  $I_2$  denotes the adjoint group of  $I_0$ ). It follows that the group  $I$  of this paper can serve as the group  $I$  used in §3 of [K5].

### 15. VANISHING OF $\alpha(\gamma_0; \gamma, \delta)$

We keep the notation of §14 and continue to exclude Case D. Starting from a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$  up to isogeny satisfying the three assumptions of §14, we constructed a triple  $(\gamma_0; \gamma, \delta)$  satisfying the conditions of §2 of [K5]. In that section of that paper there is a construction of an element  $\alpha(\gamma_0; \gamma, \delta) \in \mathcal{K}(I_0/\mathbb{Q})^D$ , where  $I_0$  denotes the centralizer of  $\gamma_0$  in  $G$ . The group  $I_0$  is connected and reductive since  $\gamma_0$  is semisimple and the derived group of  $G$  is simply connected. Recall that  $\mathcal{K}(I_0/\mathbb{Q})$  is the subgroup of  $\pi_0((Z(\widehat{I}_0)/Z(\widehat{G}))^{\Gamma})$  consisting of elements whose image in  $H^1(\mathbb{Q}, Z(\widehat{G}))$  lies in  $\ker^1(\mathbb{Q}, Z(\widehat{G}))$ , the subgroup of locally trivial elements in  $H^1(\mathbb{Q}, Z(\widehat{G}))$  ( $\Gamma$  denotes  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ). In this section we will prove the following result.

**Lemma 15.1.** *Let  $(A, \lambda, i)$  be a  $c$ -polarized virtual  $B$ -abelian variety over  $k_r$  satisfying the three conditions of §14, and let  $(\gamma_0; \gamma, \delta)$  be the triple associated to  $(A, \lambda, i)$ . Then the element  $\alpha(\gamma_0; \gamma, \delta)$  of  $\mathcal{K}(I_0/\mathbb{Q})^D$  is trivial.*

In §18 when we determine the image of the map  $(A, \lambda, i) \mapsto (\gamma_0; \gamma, \delta)$ , we will need a slight generalization of Lemma 15.1, which we will now formulate. Again we start with a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$  up to isogeny, but we do not assume that  $(A, \lambda, i)$  satisfies the three conditions of §14. Instead we make the following weaker assumption. We assume that there exists a semisimple element  $\gamma_0 \in G(\mathbb{Q})$ , elliptic in  $G(\mathbb{R})$ , with  $\gamma_0 \gamma_0^* = c^{-1}$ , and such that for every prime  $l$  different from  $p$  the  $B \otimes_{\mathbb{Q}} \mathbb{Q}[T]$ -modules  $V_l := V \otimes_{\mathbb{Q}} \mathbb{Q}_l$  and  $H_l := H_1(\bar{A}, \mathbb{Q}_l)$  are isomorphic, where  $T$  acts on  $V_l$  by  $\gamma_0^{-1}$  and on  $H_l$  by  $\pi_A$ .

Put  $I := \text{Aut}(A, \lambda, i)$  and  $I_0 := G_{\gamma_0}$ . We claim that  $I$  is an inner twist of  $I_0$  (canonically, up to inner automorphisms of  $I_0$  over  $\mathbb{Q}$ ). Put  $M = \text{End}_B(A)$

and let  $M_0$  be the centralizer of  $\gamma_0$  in  $C = \text{End}_B(V)$ . We have involutions on  $M$  and  $M_0$ . Let  $\Psi$  be the functor considered at the end of §14. Pick any prime  $l$  different from  $p$ . Then  $\Psi(\mathbb{Q}_l)$  is nonempty, since our hypothesis that  $V_l$  be isomorphic to  $H_l$  as  $B \otimes_{\mathbb{Q}} \mathbb{Q}[T]$ -module implies that  $V_l$  and  $H_l$  are isomorphic over  $\mathbb{Q}_l$  as skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules (where  $\mathbb{Q}[\pi_A]$  denotes the subalgebra of  $\text{End}(A)$  generated by  $\pi_A$ , and where  $\pi_A$  acts on  $V_l$  by  $\gamma_0^{-1}$ ), and  $(M_0)_{\mathbb{Q}_l}$  (respectively,  $M_{\mathbb{Q}_l}$ ) is the \*-algebra  $\text{End}_{B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]}(V_l)$  (respectively,  $\text{End}_{B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]}(H_l)$ ). Therefore  $\Psi(\mathbb{Q})$  is nonempty. Pick  $\psi \in \Psi(\mathbb{Q})$ . Then the restriction of  $\psi$  to  $I_0 \subset M_0^\times$  is the desired inner twisting  $\psi: I_0 \rightarrow I$ .

The inner twistings  $\psi \in \Psi(\mathbb{Q})$  allow us to identify the  $\Gamma$ -modules  $Z(\widehat{I}_0)$  and  $Z(\widehat{I})$ . We are going to generalize the construction of  $\alpha(\gamma_0; \gamma, \delta)$  by constructing an element  $\alpha(\gamma_0; A, \lambda, i) \in X^*(Z(\widehat{I}_0)^\Gamma)$ . As usual we first define, for each place  $v$  of  $\mathbb{Q}$ , an element  $\alpha_v \in X^*(Z(\widehat{I}_0)'^{(v)})$ , and then we define  $\alpha(\gamma_0; A, \lambda, i)$  to be the product over all places of  $\mathbb{Q}$  of the restrictions of  $\alpha_v$  to  $Z(\widehat{I}_0)^\Gamma \subset Z(\widehat{I}_0)'^{(v)}$ .

First consider a prime  $l$  different from  $p$ . The difference between the skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules  $H_l$  and  $V_l$  is measured by an element of  $H^1(\mathbb{Q}_l, I_0)$  (since  $(I_0)_{\mathbb{Q}_l} = \text{Aut}(V_l)$ ); we define  $\alpha_l$  to be the image of this element of  $H^1(\mathbb{Q}_l, I_0)$  under the map

$$H^1(\mathbb{Q}_l, I_0) \rightarrow \pi_0(Z(\widehat{I}_0)'^{\Gamma(l)})^D \subset X^*(Z(\widehat{I}_0)^\Gamma).$$

Next consider the prime  $p$ . As usual  $A$  gives rise to an isocrystal  $(H, \Phi)$  over  $L_r$ . Our hypothesis that for  $l \neq p$  the  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules  $V_l$  and  $H_l$  be isomorphic implies that the  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules  $V_L$  and  $H_L$  are isomorphic (with  $\pi_A$  acting on  $V_L$  by  $\gamma_0^{-1}$ , as usual). Since  $H^1(L, (I_0)_L)$  is trivial by Steinberg's vanishing theorem,  $V_L$  and  $H_L$  are isomorphic as skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules; choose such an isomorphism  $V_L \simeq H_L$  and use it to transport  $\Phi$  over to a  $\sigma$ -linear bijection from  $V_L$  to itself, which we then write as  $b\sigma$  for  $b \in G(L)$ . Since  $b\sigma$  centralizes  $\pi_A = \gamma_0^{-1} \in G(\mathbb{Q}_p)$ , it follows that  $b$  centralizes  $\gamma_0$ , or in other words, that  $b \in I_0(L)$ . Changing the choice of isomorphism  $V_L \simeq H_L$  replaces  $b$  by a  $\sigma$ -conjugate in  $I_0(L)$ , so that  $b$  is well defined as an element of  $B((I_0)_{\mathbb{Q}_p})$ . We define  $\alpha_p$  to be the image of this element of  $B((I_0)_{\mathbb{Q}_p})$  under the map

$$B((I_0)_{\mathbb{Q}_p}) \rightarrow X^*(Z(\widehat{I}_0)'^{\Gamma(p)}).$$

Finally consider the place  $\infty$  of  $\mathbb{Q}$ . We have the \*-homomorphism  $h: \mathbb{C} \rightarrow C_{\mathbb{R}}$  of §5. Choose an elliptic maximal torus  $T$  of  $G$  containing  $\gamma_0$  (and hence contained in  $I_0$ ). Some conjugate  $h'$  of  $h$  under  $G_1(\mathbb{R})$  factors through  $T$ , and as usual  $h'$  gives us  $\mu_{h'} \in X_*(T) = X^*(\widehat{T})$ , which we restrict to  $Z(\widehat{I}_0)'^{(\infty)} \subset \widehat{T}'^{(\infty)} \subset \widehat{T}$  to get  $\alpha_\infty \in X^*(Z(\widehat{I}_0)'^{(\infty)})$  (see §2 of [K5] for a proof that  $\alpha_\infty$  is independent of the choices made in its construction).

**Lemma 15.2.** *The element  $\alpha(\gamma_0; A, \lambda, i)$  is trivial.*

Before proving Lemma 15.2 let us check that Lemma 15.2 implies Lemma 15.1. The first point to verify is that the natural map

$$Z(\widehat{I}_0)^\Gamma \rightarrow \mathfrak{K}(I_0/\mathbb{Q})$$

is surjective in the situation at hand. In view of the long exact cohomology sequence for the exact sequence

$$1 \rightarrow Z(\widehat{G}) \rightarrow Z(\widehat{I}_0) \rightarrow Z(\widehat{I}_0)/Z(\widehat{G}) \rightarrow 1$$

what we need to check is that

$$\ker^1(\mathbb{Q}, Z(\widehat{G})) \rightarrow \ker^1(\mathbb{Q}, Z(\widehat{I}_0))$$

is injective. Let  $T$  be a maximal torus of  $I_0$ . Then  $Z(\widehat{I}_0) \hookrightarrow \widehat{T}$  and it is enough to check that

$$\ker^1(\mathbb{Q}, Z(\widehat{G})) \rightarrow \ker^1(\mathbb{Q}, \widehat{T})$$

is injective, or, equivalently, that

$$\ker^1(\mathbb{Q}, \widehat{T})^D \rightarrow \ker^1(\mathbb{Q}, Z(\widehat{G}))^D$$

is surjective. Recall that the derived group  $G_{\text{der}}$  of  $G$  is simply connected (we are in Case A or C) and hence that  $Z(\widehat{G})$  is the complex torus dual to  $D := G/G_{\text{der}}$ . By Tate-Nakayama duality (see (3.4.5.1) of [K2]) it is equivalent to check that

$$\ker^1(\mathbb{Q}, T) \rightarrow \ker^1(\mathbb{Q}, D)$$

is surjective. But from Lemma 4.3.1 of [K2] we know that  $\ker^1(\mathbb{Q}, D) = \ker^1(\mathbb{Q}, G)$ , and from the discussion in §7 we know that the canonical map  $\ker^1(\mathbb{Q}, Z) \rightarrow \ker^1(\mathbb{Q}, G)$  is surjective (even bijective) in both Case A and Case C ( $Z$  denotes the center of  $G$ ); it follows that

$$\ker^1(\mathbb{Q}, T) \rightarrow \ker^1(\mathbb{Q}, D)$$

is indeed surjective.

Now suppose that  $(A, \lambda, i), (\gamma_0; \gamma, \delta)$ , and  $\alpha(\gamma_0; \gamma, \delta)$  are as in Lemma 15.1. We use the surjection

$$Z(\widehat{I}_0)^\Gamma \rightarrow \mathfrak{K}(I_0/\mathbb{Q})$$

to view  $\alpha(\gamma_0; \gamma, \delta)$  as an element of  $X^*(Z(\widehat{I}_0)^\Gamma)$ . We also have the element  $\alpha(\gamma_0; A, \lambda, i) \in X^*(Z(\widehat{I}_0)^\Gamma)$ , which Lemma 15.2 states is trivial. Since a glance at the definition of the local factors of  $\alpha(\gamma_0; \gamma, \delta)$  and  $\alpha(\gamma_0; A, \lambda, i)$  shows that they are the same, we see that  $\alpha(\gamma_0; \gamma, \delta)$  is trivial, as desired.

It remains to prove Lemma 15.2. We have seen that  $I$  is an inner twist of  $I_0$ . Choose a maximal torus  $T$  of  $I$  that is elliptic at the infinite place of  $\mathbb{Q}$  as well as all the finite places of  $\mathbb{Q}$  at which  $I_0$  is not quasi-split. Then  $T$  transfers to  $I_0$  locally everywhere. Moreover, since  $T$  is elliptic at  $\infty$ , the argument in §14 shows that  $T$  transfers to  $I_0$  globally.

Let  $N$  be the centralizer of  $T$  in  $M := \text{End}_B(A)$ . Recall the following facts from §14. The algebra  $N$  is a maximal commutative semisimple subalgebra of  $M$ . The involution  $*$  preserves  $N$  (hence is positive on  $N$ ), and  $N$  is free of rank 2 over  $N_0 := \{x \in N | x^* = x\}$ ; together these facts imply that  $N$  is a CM-algebra. The torus  $T$  is equal to  $\{x \in N | xx^* \in \mathbb{G}_m\}$ .

Since  $T$  transfers to  $I_0$ , the element of  $H^1(\mathbb{Q}, I_{\text{ad}})$  corresponding to the inner twist  $I_0$  comes from a 1-cocycle  $(t_\sigma)$  of  $\Gamma$  in  $T_{\text{ad}}(\mathbb{Q})$ , where  $T_{\text{ad}}$  denotes the image of  $T$  in the adjoint group  $I_{\text{ad}}$  of  $I$ . The  $*$ -algebra  $(M_0, *)$  is obtained from  $(M, *)$  by twisting by the 1-cocycle  $(t_\sigma)$ . This twisting does not affect the subalgebra  $N$  of  $M$ , or, in other words, the subalgebra  $N$  transfers to  $M_0$ , in the sense that we have a  $*$ -algebra embedding of  $N$  as a maximal commutative semisimple subalgebra of  $M_0$ , canonical up to “stable conjugacy” (conjugation by an element  $x \in I_0(\mathbb{Q})$  such that the composed map

$$N \hookrightarrow M_0 \xrightarrow{\text{Int}(x)} M_0$$

is defined over  $\mathbb{Q}$ ).

The map  $N \rightarrow M_0$  gives us an embedding  $T \rightarrow I_0$ . Since  $T \rightarrow I_0$  is the restriction to  $T$  of the inverse of some  $\psi \in \Psi$  (with  $\Psi$  as before), it follows that  $T \rightarrow I_0$  maps  $\pi_A^{-1}$  to  $\gamma_0$ .

We will now complete the proof of Lemma 15.2 in two steps. The first step will be to construct a character  $\alpha'$  on  $\widehat{T}^\Gamma$  whose restriction to  $Z(\widehat{I}_0)^\Gamma$  is equal to  $\alpha(\gamma_0; A, \lambda, i)$ ; the second step will be to use Lemma 13.2 to prove that  $\alpha'$  is trivial.

The construction of  $\alpha'$  exactly parallels the construction of the character  $\alpha$  in §13. Using  $N \rightarrow M_0 \hookrightarrow \text{End}_B(V)$ , we regard  $V$  as a skew-Hermitian  $B \otimes_F N$ -module (for the involution  $b \otimes n \mapsto b^* \otimes n^*$  on  $B \otimes_F N$ ). Note that  $N$  is a maximal semisimple commutative subalgebra of  $\text{End}_B(V)$  (since  $M_0$  is the centralizer of a semisimple element in  $\text{End}_B(V)$ ) and hence that  $\text{End}_{B \otimes_F N}(V) = N$ ; it follows that  $T$  is the group of automorphisms of the skew-Hermitian  $B \otimes_F N$ -module  $V$ .

Using  $N \hookrightarrow M = \text{End}_B(A)$ , we regard  $A$  as a  $c$ -polarized virtual  $B \otimes_F N$ -abelian variety over  $k$ . Since  $N$  is a maximal commutative subalgebra of  $M$ , and since  $M$  is the centralizer of the semisimple element  $\pi_A$  of  $\text{End}_B(\bar{A})$ , it follows that  $N$  is also a maximal commutative semisimple subalgebra of  $\text{End}_B(\bar{A})$  and hence that  $\text{End}_{B \otimes_F N}(\bar{A}) = N$ . Therefore the group  $T$  is also the group of automorphisms of the  $c$ -polarized  $B \otimes_F N$ -abelian variety  $\bar{A}$  up to isogeny.

As usual the character  $\alpha' \in X^*(\widehat{T}^\Gamma)$  will be defined as the product over all places of  $\mathbb{Q}$  of the restrictions of characters  $\alpha'_v \in X^*(\widehat{T}^{\Gamma(v)})$ . For each prime  $l$  different from  $p$  we have two skew-Hermitian  $B \otimes_F N$ -modules over  $\mathbb{Q}_l$ , namely,  $H_l$  and  $V_l$ . Since  $\text{End}_{B \otimes_F N \otimes_{\mathbb{Q}} \mathbb{Q}_l}(H_l) = N \otimes_{\mathbb{Q}} \mathbb{Q}_l = \text{End}_{B \otimes_F N \otimes_{\mathbb{Q}} \mathbb{Q}_l}(V_l)$ , the  $B \otimes_F N$ -modules  $H_l, V_l$  over  $\mathbb{Q}_l$  are isomorphic and hence their difference as skew-Hermitian  $B \otimes_F N$ -modules is measured by an element of  $H^1(\mathbb{Q}_l, T)$ .

We define  $\alpha'_l$  to be the image of this element under the map

$$H^1(\mathbb{Q}_l, T) \rightarrow \pi_0(\widehat{T}^{\Gamma(l)})^D \subset X^*(\widehat{T}^{\Gamma(l)}).$$

For the prime  $p$  we have the isocrystal  $D$  over  $L$  dual to  $H_{\text{cris}}^1(A/W(\bar{k})) \otimes_{W(\bar{k})} L$ . Moreover,  $D$  is a skew-Hermitian  $B \otimes_F N$ -module over  $L$ , and the  $\sigma$ -linear bijection  $\Phi$  on  $D$  commutes with the action of  $B \otimes_F N$  and satisfies the equality  $(\Phi v, \Phi w) = p^{-1}\sigma(v, w)$  for all  $v, w \in D$ . Since  $H_l, V_l$  are isomorphic as  $B \otimes_F N$ -modules over  $\mathbb{Q}_l$  (for  $l$  different from  $p$ ), it follows that  $D$  and  $V_L$  are isomorphic as  $B \otimes_F N$ -modules over  $L$ , and by Steinberg's vanishing theorem they are even isomorphic as skew-Hermitian  $B \otimes_F N$ -modules over  $L$ . Choose such an isomorphism  $V_L \simeq D$  and use it to transport  $\Phi$  to  $V_L$ . As usual we write  $\Phi = b\sigma$  for  $b \in T(L)$ ; then the image of  $b$  in  $B(T_{\mathbb{Q}_p})$  is well defined. We define  $\alpha'_p$  to be the image of this element of  $B(T_{\mathbb{Q}_p})$  under

$$B(T_{\mathbb{Q}_p}) \rightarrow X^*(\widehat{T}^{\Gamma(p)}).$$

Finally consider the infinite place  $\infty$  of  $\mathbb{Q}$ . The involution on  $B \otimes_F N$  is positive since  $B \otimes_F N$  is a direct factor of  $B \otimes_{F_0} N$  and  $b \otimes n \mapsto b^* \otimes n^*$  is positive on  $B \otimes_{F_0} N$  (use Lemma 2.3). Choose a  $G_1(\mathbb{R})$ -conjugate  $h'$  of  $h : \mathbb{C} \rightarrow C_{\mathbb{R}}$  such that  $h' : \mathbb{C}^\times \rightarrow G_{\mathbb{R}}$  factors through  $T_{\mathbb{R}}$  (note that  $T_{\mathbb{R}}$  is elliptic in  $G_{\mathbb{R}}$ ). As usual  $h'$  gives us  $\mu_{h'} \in X_*(T) = X^*(\widehat{T})$ , which we restrict to  $\widehat{T}^{\Gamma(\infty)}$  to get  $\alpha'_{\infty} \in X^*(\widehat{T}^{\Gamma(\infty)})$ . Applying Lemma 4.3 to  $B \otimes_F N$  and  $V$ , we see that  $h'$  is unique and hence that  $\alpha'_{\infty}$  is well defined.

To complete the first step we must show that the restriction of  $\alpha'$  to  $Z(\widehat{I}_0)^\Gamma$  is equal to  $\alpha(\gamma_0; A, \lambda, i)$ . For this it is enough to check that for every place  $v$  of  $\mathbb{Q}$  the character  $\alpha_v$  on  $Z(\widehat{I}_0)^{\Gamma(v)}$  is the restriction of the character  $\alpha'_v$  on  $\widehat{T}^{\Gamma(v)}$ . This local statement is an easy consequence of the definitions of  $\alpha_v, \alpha'_v$ ; for  $l \neq p$  use that

$$\begin{array}{ccc} H^1(\mathbb{Q}_l, T) & \longrightarrow & H^1(\mathbb{Q}_l, I_0) \\ \downarrow & & \downarrow \\ X^*(\widehat{T}^{\Gamma(l)}) & \longrightarrow & X^*(Z(\widehat{I}_0)^{\Gamma(l)}) \end{array}$$

commutes (Theorem 1.2 of [K4]) and for  $p$  use the analogous statement about  $B(T)$  and  $B(I_0)$  (Lemma 6.2 of [K5]).

We are now done with the first step. Recall that the second step is to prove that  $\alpha'$  is trivial. If  $B = F$  then  $B \otimes_F N = N$ , and we have only to appeal to Lemma 13.2. If  $B \neq F$ , we can still reduce to the situation of Lemma 13.2 by using a version of Morita equivalence. Factor the  $F$ -algebra  $N$  as a product  $N = N_1 \times \cdots \times N_t$  of field extensions of  $F$ . Since  $N$  is a maximal commutative semisimple subalgebra of  $\text{End}_B(V)$ , each field  $N_i$  splits  $\text{End}_B(V)$  (we recalled the proof of this in §14). Of course  $\text{End}_B(V)$  is a matrix algebra over  $B^{\text{opp}}$ , and thus it follows that the central simple  $F$ -algebra  $B$  splits over

each  $N_i$ . Therefore we may choose an isomorphism  $B \otimes_F N \simeq \mathbf{M}_d(N)$ , where  $d = (\dim_F B)^{1/2}$ . Transporting the involution  $*$  on  $B \otimes_F N$  over to  $\mathbf{M}_d(N)$ , we get an involution of that matrix algebra that induces  $*$  on its center  $N$ . We also have the standard involution  $x \mapsto x'$  on  $\mathbf{M}_d(N)$  (take the transpose of the  $(d \times d)$ -matrix  $x$  and then apply  $*$  to each of its entries). Since any  $N$ -algebra automorphism of  $\mathbf{M}_d(N)$  is inner, there exists  $a \in \mathbf{GL}_d(N)$  such that  $x^* = ax'a^{-1}$  for all  $x \in \mathbf{M}_d(N)$ . Since  $*$  is an involution,  $a^* = ba$  for some  $B \in N^\times$  such that  $bb^* = 1$ . Since  $N$  is free of rank 2 over  $N_0 = \{x \in N \mid x = x^*\}$ , Hilbert's Theorem 90 holds for  $N/N_0$ , and we may modify  $a$  by an element of  $N^\times$  so that the new  $a$  satisfies  $a^* = a$ . It is well known that the Hermitian matrix  $a$  can be diagonalized by an element of  $\mathbf{GL}_d(N)$ ; thus, by changing our choice of isomorphism  $B \otimes_F N \simeq \mathbf{M}_d(N)$ , we may assume that the involution  $*$  on  $B \otimes_F N$  goes over to an involution  $*$  on  $\mathbf{M}_d(N)$  of the form  $x \mapsto ax'a^{-1}$ , where  $a$  is an invertible diagonal Hermitian matrix.

For  $i = 1, \dots, d$  write  $e_i$  for the element of  $\mathbf{M}_d(N)$  whose entries are all 0 with the exception of the  $i$ th diagonal entry, which is 1. Then  $e_1, \dots, e_d$  are orthogonal idempotents in  $\mathbf{M}_d(N)$  with  $e_1 + \dots + e_d = 1$ . Moreover, since the matrix  $a$  is diagonal, we have  $e_i^* = e_i$  for  $i = 1, \dots, d$ .

For any abelian category  $\mathcal{A}$  the functor  $X \mapsto X^d$  is an equivalence of categories from the category of  $N$ -objects in  $\mathcal{A}$  to the category of  $\mathbf{M}_d(N)$ -objects in  $\mathcal{A}$ , and the  $i$ th factor of  $X$  in  $X^d$  is the image of the idempotent endomorphism of  $X^d$  given by  $e_i \in \mathbf{M}_d(N)$ . Applying this to the category of abelian varieties over  $\bar{k}$  up to isogeny, we write the abelian variety  $\bar{A}$  as  $\bar{A} = A_0^d$  for an abelian  $N$ -variety  $A_0$  over  $\bar{k}$  up to isogeny. Applying it to the category of  $\mathbb{Q}$ -vector spaces, we write the  $B \otimes_F N$ -module  $V$  as  $V_0^d$  for an  $N$ -module  $V_0$ .

Since the idempotents  $e_1, \dots, e_d$  satisfy  $e_i^* = e_i$ , the skew-Hermitian form  $(\cdot, \cdot)$  on  $V$  is the direct sum of skew-Hermitian (for  $N$ ) forms  $(\cdot, \cdot)_1, \dots, (\cdot, \cdot)_d$  on the  $d$  factors  $V_0$  of  $V$ . Moreover  $(\cdot, \cdot)_i$  and  $(\cdot, \cdot)_1$  are related by  $(x, y)_i = (a_1 a_i^{-1} x, y)_1$ , where  $a_i$  denotes the  $i$ th diagonal entry of  $a$ . Similarly the polarization  $\lambda: A \rightarrow \widehat{A}$  is the direct product of polarizations  $\lambda_1, \dots, \lambda_d$  on the  $d$  factors  $A_0$  of  $\bar{A}$ , and  $\lambda_i$  is related to  $\lambda_1$  by  $\lambda_i = \lambda_1 \circ (a_1 a_i^{-1})$  ( $a_1 a_i^{-1}$  gives an endomorphism of  $A_0$ ); of course each polarization  $\lambda_1, \dots, \lambda_d$  is compatible with the  $N$ -action on  $A_0$ .

As we have already seen, the algebras  $\text{End}_{B \otimes_F N}(\bar{A})$  and  $\text{End}_{B \otimes_F N}(V)$  are both equal to  $N$ . Therefore  $\text{End}_N(A_0)$  and  $\text{End}_N(V_0)$  are both equal to  $N$ , which means that  $A_0$  has CM by  $N$  and that  $V_0$  is free of rank 1 over  $N$ , so that each  $(V_0, (\cdot, \cdot)_i)$  is a symplectic space with CM by  $N$  over  $\mathbb{Q}$  in the sense of §13. Fix a value of  $i$ , say  $i = 1$ . Then  $(A_0, \lambda_1)$  and  $(V_0, (\cdot, \cdot)_1)$  are as in §13, so that the constructions of §13 yield characters  $\alpha(v)$  on  $\widehat{T}^{\Gamma(v)}$  for each place  $v$  of  $\mathbb{Q}$ . The constructions of this section yield characters  $\alpha'_v$  on  $\widehat{T}^{\Gamma(v)}$ . It follows easily from the definitions that  $\alpha(v) = \alpha'_v$  for all  $v$ . Therefore

Lemma 13.2 implies that  $\alpha'$  is trivial, which completes the proof of Lemma 15.2.

## 16. COUNTING FIXED POINTS OF $\Phi_p^j \circ f$ WITHIN A SINGLE ISOGENY CLASS

In this section we use the notation of §5, so that in particular  $S_{K^p}$  is the moduli scheme over  $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$  obtained from  $B, V, (\cdot, \cdot), K^p, h$ . Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_E$  lying over  $p$ , let  $k$  be the residue field of  $\mathcal{O}_E$  at  $\mathfrak{p}$ , and let  $\bar{k}$  be an algebraic closure of  $k$ . In this section we will be interested exclusively in the  $k$ -scheme obtained from  $S_{K^p}$  by extension of scalars to  $k$ , and we may as well just use  $S_{K^p}$  to denote this  $k$ -scheme. We denote by  $\Phi_{\mathfrak{p}}$  the Frobenius endomorphism of the  $k$ -scheme  $S_{K^p}$ . Fix a positive integer  $j$ ; then we can consider the  $j$ th power  $\Phi_{\mathfrak{p}}^j$  of  $\Phi_{\mathfrak{p}}$ . Fix an element  $g$  of  $G(\mathbb{A}_f^p)$  and, as in §6, use it to get a Hecke correspondence

$$S_{K^p} \xleftarrow{a} S_{K_g^p} \xrightarrow{b} S_{K_p}$$

from  $S_{K^p}$  to itself (as before,  $K_g^p := K^p \cap gK^pg^{-1}$ ); we denote by  $f$  this Hecke correspondence. In this section we are going to begin to study the fixed points of the composition  $\Phi_{\mathfrak{p}}^j \circ f$  of the morphism  $\Phi_{\mathfrak{p}}^j$  and the correspondence  $f$ ; the composition is the correspondence

$$S \xleftarrow{a} S' \xrightarrow{c} S,$$

where  $c = \Phi_{\mathfrak{p}}^j \circ b$  and we have written  $S$  (respectively,  $S'$ ) for  $S_{K^p}$  (respectively,  $S_{K_g^p}$ ) in order to simplify the notation.

By a fixed point we mean an element of  $S'(\bar{k})$  whose images in  $S(\bar{k})$  under  $a$  and  $c$  coincide. Thus a fixed point is a  $\bar{k}$ -point  $(\bar{A}, \lambda, i, \bar{\eta})$  of the moduli problem for  $K_g^p$  having the property that  $(\bar{A}, \lambda, i, \bar{\eta}\bar{g})$  be isomorphic to  $\sigma'(\bar{A}, \lambda, i, \bar{\eta})$  (as objects of the moduli problem for  $K^p$ ), where  $\sigma$  denotes the Frobenius automorphism  $x \mapsto x^p$  of  $\bar{k}$  and  $r$  is the positive integer  $j[k : \mathbb{F}_p]$ . Here  $\sigma'(\bar{A}, \lambda, i, \bar{\eta})$  denotes the object  $(\sigma'(\bar{A}), \sigma'(\lambda), \sigma'(i), \sigma'(\bar{\eta}))$  over  $\bar{k}$  obtained from  $(\bar{A}, \lambda, i, \bar{\eta})$  by extension of scalars for  $\sigma' : \bar{k} \rightarrow \bar{k}$ . In other words a  $\bar{k}$ -point  $(\bar{A}, \lambda, i, \bar{\eta})$  of  $S'$  is a fixed point if and only if there is a prime-to- $p$  isogeny  $u : \sigma'(\bar{A}) \rightarrow \bar{A}$ , commuting with the action of  $\mathcal{O}_B$ , carrying  $\sigma'(\bar{\eta})$  into  $\bar{\eta}\bar{g}$  (as level structures of type  $K^p$ ), and carrying  $\sigma'(\lambda)$  into a scalar multiple of  $\lambda$  (a scalar in  $\mathbb{Z}_{(p)}^\times$ ). Since we have assumed that  $K^p$  is small enough that our objects have no automorphisms, the isogeny  $u$  is unique. The pair  $A := (\bar{A}, u)$  is a virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny, in the sense of §10. Moreover, the image of the homomorphism  $i : \mathcal{O}_B \rightarrow \text{End}(\bar{A})$  is contained in the subring  $\text{End}(A)$  of  $\text{End}(\bar{A})$ , and there is a scalar  $c_0 \in \mathbb{Z}_{(p)}^\times$  such that  $u^* \lambda = c_0 \sigma'(\lambda)$ , which means that  $\lambda$  is a  $c$ -polarization of  $A$  (in the sense of §10) with  $c := p^r c_0$ . The condition that

$u$  carry  $\sigma'(\bar{\eta})$  into  $\overline{\eta g}$  is equivalent to the condition that  $\eta g = \pi_A \eta$  (modulo  $K^p$ ).

Thus we can associate to any fixed point  $(\bar{A}, \lambda, i, \bar{\eta})$  a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$  up to prime-to- $p$  isogeny. Our next goal is to show that  $(A, \lambda, i)$  satisfies the three conditions of §14. The first condition is an immediate consequence of the existence of a level structure on  $\bar{A}$ . In particular the  $B$ -module  $H_1(\bar{A}, \mathbb{Q}_l)$  is isomorphic to  $V_l$  for any  $l$  different from  $p$ . Since the character of the  $B$ -module  $H$  over  $L_r$  is equal to the character of the  $B$ -module  $H_1(\bar{A}, \mathbb{Q}_l)$ , we conclude that  $H$  is isomorphic as  $B$ -module to  $V \otimes_{\mathbb{Q}} L_r$ . Moreover, since the lattice  $\Lambda \subset H$  of §10 is preserved by  $\mathcal{O}_B$  and is self-dual under the alternating form on  $H$ , Lemma 7.2 implies (see Remark 7.5) that the skew-Hermitian  $B$ -module  $H$  over  $L_r$  is isomorphic to  $V \otimes_{\mathbb{Q}} L_r$ ; this verifies the second condition of §14.

The third condition is harder to verify. It comes from the determinant condition on  $(\bar{A}, i)$ . As in §14 we choose an isomorphism  $H \simeq V \otimes_{\mathbb{Q}} L_r$  of skew-Hermitian spaces over  $L_r$  and use it to get  $\delta \in G(L_r)$ . In order to verify the third condition we need to understand the relative position of the lattices  $\Lambda$  and  $\Phi(\Lambda)$  (now regarded as  $\mathcal{O}_B$ -lattices in  $V \otimes_{\mathbb{Q}} L_r$ ). The lattice  $\Lambda$  is self-dual and  $\Phi(\Lambda)$  is self-dual up to a scalar in  $L_r^\times$ . Recall that in §5 we chose a self-dual  $\mathcal{O}_B$ -lattice  $\Lambda_0$  in  $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ . We also write  $\Lambda_0$  for the  $\mathcal{O}_B$ -lattice in  $V \otimes_{\mathbb{Q}} L_r$  obtained from  $\Lambda_0$  by extension of scalars from  $\mathbb{Z}_p$  to the valuation ring of  $L_r$ . The stabilizer  $K$  (respectively,  $K_r$ ) of  $\Lambda_0$  in  $G(\mathbb{Q}_p)$  (respectively,  $G(L_r)$ ) is a hyperspecial maximal compact subgroup of  $G(\mathbb{Q}_p)$  (respectively,  $G(L_r)$ ) (this uses the hypotheses of §5). By Corollary 7.3 (see Remark 7.5) there exists  $x \in G(L_r)$  such that  $\Lambda = x\Lambda_0$ . Then  $\Phi(\Lambda) = \delta\sigma(x)\Lambda_0$ , and the relative position of  $\Phi(\Lambda)$  and  $\Lambda$  is measured by the double coset  $K_r x^{-1} \delta\sigma(x) K_r$  of  $K_r$  in  $G(L_r)$ .

On the other hand the procedure of §3 in [K5] gives us a canonical double coset of  $K_r$  in  $G(L_r)$ , constructed as follows. The homomorphism  $h : \mathbb{C}^\times \rightarrow G_{\mathbb{R}}$  of §§4 and 5 gives us a homomorphism  $\mu_h : \mathbb{G}_m \rightarrow G_{\mathbb{C}}$  (see Lemma 4.1). The  $G(\mathbb{C})$ -conjugacy class of  $\mu_h$  gives us a  $G(\mathbb{Q}_p)$ -conjugacy class of homomorphisms  $\mu : \mathbb{G}_m \rightarrow G_{\mathbb{Q}_p}$ , fixed by  $\text{Gal}(\mathbb{Q}_p/E_p)$  and hence by its subgroup  $\text{Gal}(\mathbb{Q}_p/L_r)$  ( $L_r$  is the unramified extension of  $E_p$  corresponding to the extension  $k_r/k$  of residue fields). Choose a maximal  $\mathcal{O}_{L_r}$ -split torus  $S$  in  $G$  over  $\mathcal{O}_{L_r}$ . Then  $S$  is also a maximal  $L_r$ -split torus in  $G$  over  $L_r$ , and by Lemma (1.1.3) of [K1] we can choose  $\mu$  so that it factors through  $S$ . Put  $a = \mu(p^{-1})$ , an element of  $S(L_r)$ ; then the double coset  $K_r a K_r$  is the canonical one mentioned above.

We need a more concrete description of  $K_r a K_r$ . As in §7 we write  $H$  for the algebraic group  $C^\times$  and  $i : G \rightarrow H$  for the canonical inclusion. By Lemma 7.4 it is enough to describe the double coset  $K_H i(a) K_H$  in  $H(L_r)$ , where  $K_H$  denotes the stabilizer of  $\Lambda_0$  in  $H(L_r)$ . When we introduced the determinant condition in §5 we used  $h$  to decompose the  $B_{\mathbb{C}}$ -module  $V_{\mathbb{C}}$  as  $V_1 \oplus V_2$ ; clearly  $\mu_h : \mathbb{G}_m \rightarrow G$  makes  $t \in \mathbb{G}_m$  act on  $V_1$  by  $t$  and on  $V_2$  by 1. Since the

isomorphism class of  $V_1$  is defined over  $E$ , and since  $B$  splits over every  $p$ -adic place of  $F$ , the representation  $V_1$  of  $B$  can be realized over  $E_p$  and hence over  $L_r$ . Since the  $p$ -adic completion of  $\mathcal{O}_B$  is a maximal order, we can decompose the  $\mathcal{O}_B \otimes_{\mathbb{Z}_{(p)}} \mathcal{O}_{L_r}$ -module  $\Lambda_0$  as  $\Lambda_1 \oplus \Lambda_2$  in such a way that  $\Lambda_1$  satisfies the determinant condition of §5 (in other words,

$$\det(X_1\alpha_1 + \cdots + X_t\alpha_t; \Lambda_1) = f(X_1, \dots, X_t),$$

with notation as in §5). Then the composition of  $\mu : \mathbb{G}_m \rightarrow G_{L_r}$  with the inclusion  $G \subset H$  is conjugate to the homomorphism  $\mathbb{G}_m \rightarrow H_{L_r}$  that makes  $t \in \mathbb{G}_m$  act by  $t$  on  $\Lambda_1 \otimes L_r$  and by 1 on  $\Lambda_2 \otimes L_r$ . Let  $h \in H(L_r)$ . Then the discussion above shows that  $h \in K_H i(a)K_H$  if and only if  $p^{-1}\Lambda_0 \supset h\Lambda_0 \supset \Lambda_0$  and the representation of  $\mathcal{O}_B$  on the  $k_r$ -module  $h\Lambda_0/\Lambda_0$  satisfies the determinant condition (of course we must use the usual description of double cosets for maximal compact subgroups of general linear groups over  $p$ -adic fields).

Recall that we are assuming that  $(\bar{A}, i)$  satisfies the determinant condition. Since  $\sigma(\text{Lie}(\bar{A}))$  is canonically isomorphic to  $\Phi(\Lambda)/\Lambda$ , we conclude that the double cosets  $K_r x^{-1} \delta\sigma(x)K_r$  and  $K_r a K_r$  are related by  $K_r x^{-1} \delta\sigma(x)K_r = K_r \sigma(a)K_r$ . We will use this relation again later in this section. We use it now to finish the verification that  $\delta$  satisfies the third condition of §14. Let  $D$  denote the unramified  $\mathbb{Q}_p$ -torus  $G/G_{\text{der}}$  ( $G_{\text{der}}$  is the derived group of  $G$ ); then  $Z(\hat{G}) = \hat{D}$  and what we must show is that the image of  $\delta$  in  $D(L_r) \subset D(L)$  is  $\sigma$ -conjugate in  $D(L)$  to  $\mu_1(p)^{-1}$ , where  $\mu_1$  is the composition of  $\mu$  and  $G \rightarrow D$ . Since  $\sigma(a)$  is  $\sigma$ -conjugate to  $a$  and every element of  $D(\mathcal{O}_L)$  is  $\sigma$ -conjugate to the identity (see [K3]), the relation  $x^{-1} \delta\sigma(x) \in K_r \sigma(a)K_r$  shows that the image of  $\delta$  in  $D(L)$  is  $\sigma$ -conjugate to  $\mu_1(p)^{-1}$ , as we wanted to show.

Now fix a  $c$ -polarized virtual  $B$ -abelian variety  $(A_0, \lambda_0, i_0)$  over  $k_r$  up to isogeny, satisfying the three conditions of §14. Our goal in this section is to count the number of fixed points  $(\bar{A}, \lambda, i, \eta)$  of our correspondence for which the associated  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  is isogenous to  $(A_0, \lambda_0, i_0)$ , in the sense that there exists a  $\mathbb{Q}$ -isogeny  $\varphi : A \rightarrow A_0$  compatible with the  $B$ -actions and polarizations (up to  $\mathbb{Q}^\times$ ).

As in §14 we write  $M$  for  $\text{End}_B(A_0)$  and  $I$  for the  $\mathbb{Q}$ -group  $\{x \in M | xx^* \in \mathbb{G}_m\}$  (the group of isogenies from  $(A_0, \lambda_0, i_0)$  to itself). The set of fixed points for which  $(A, \lambda, i)$  is isogenous to  $(A_0, \lambda_0, i_0)$  is equal to the quotient  $I(\mathbb{Q}) \backslash Y$ , where  $Y$  is the set of such fixed points together with an isogeny  $\varphi : A \rightarrow A_0$  as above. The category of pairs  $(A, \varphi)$  (with  $A$  a virtual abelian variety over  $k_r$  up to prime-to- $p$  isogeny and  $\varphi$  an isogeny  $\varphi : A \rightarrow A_0$ ) is equivalent to the category of lattices  $\Lambda$  in the  $L_r$ -isocrystal  $H$  obtained from  $A$  such that

$$p^{-1}\Lambda \supset \Phi(\Lambda) \supset \Lambda.$$

The lattice  $\Lambda$  is self-dual up to a scalar if and only if there exists a scalar such that  $\varphi^*(\lambda_0)$  is a prime-to- $p$  isogeny from  $A$  to  $\hat{A}$ , and the lattice  $\Lambda$  is preserved by  $\mathcal{O}_B$  if and only if the  $B$ -action on  $A$  obtained from  $\varphi$  comes from an  $\mathcal{O}_B$ -action on the virtual abelian variety  $A$  up to prime-to- $p$  isogeny.

Moreover, assuming  $\Lambda$  satisfies all the conditions above, the  $B$ -abelian variety  $\bar{A}$  over  $\bar{k}$  satisfies the determinant condition if and only if the  $\mathcal{O}_B \otimes_{\mathbb{Z}_{(p)}} k_r$ -module  $\sigma^{-1}(\Phi(\Lambda)/\Lambda)$  satisfies the determinant condition.

As in §14 we fix isomorphisms  $H_1(\bar{A}_0, \mathbb{A}_f^p) \simeq V \otimes_{\mathbb{Q}} \mathbb{A}_f^p$  and  $H \simeq V \otimes_{\mathbb{Q}} L_r$  of skew-Hermitian  $B$ -modules and use them to get  $\gamma \in G(\mathbb{A}_f^p)$  and  $\delta \in G(L_r)$ . As before we have the self-dual  $\mathcal{O}_B$ -lattice  $\Lambda_0$  in  $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$  (and  $V \otimes_{\mathbb{Q}} L_r$ ) that we fixed in §5. The discussion earlier in this section together with the discussion above shows that giving  $(A, \phi)$  is the same as giving an element  $x \in G(L_r)/K_r$  such that  $x^{-1}\delta\sigma(x) \in K_r\sigma(a)K_r$ .

Since we have fixed the isomorphism  $H_1(\bar{A}_0, \mathbb{A}_f^p) \simeq V \otimes_{\mathbb{Q}} \mathbb{A}_f^p$ , giving a level structure of type  $K_g^p$  on  $\bar{A}_0$  is the same as giving an element  $y \in G(\mathbb{A}_f^p)/K_g^p$ , and it is also the same as giving a level structure  $\bar{\eta}$  on  $\bar{A}$  if we have a given  $\varphi : A \rightarrow A_0$ . The condition  $\eta g = \pi_A \eta$  (modulo  $K^p$ ) becomes the condition  $yg = \gamma^{-1}y$  (modulo  $K^p$ ), or, equivalently,  $y^{-1}\gamma y \in K^p g^{-1}$ . We conclude that there is a bijection from the set of fixed points  $(\bar{A}, \lambda, i, \bar{\eta})$  with  $(A, \lambda, i)$  isogenous to  $(A_0, \lambda_0, i_0)$  to the quotient set  $I(\mathbb{Q}) \setminus (Y^p \times Y_p)$ , where

$$\begin{aligned} Y^p &= \{y \in G(\mathbb{A}_f^p)/K_g^p \mid y^{-1}\gamma y \in K^p g^{-1}\}, \\ Y_p &= \{x \in G(L_r)/K_r \mid x^{-1}\delta\sigma(x) \in K_r\sigma(a)K_r\}. \end{aligned}$$

It follows that the cardinality of this set is the integral

$$\int_{I(\mathbb{Q}) \setminus (G(\mathbb{A}_f^p) \times G(L_r))} \tilde{f}^p(y^{-1}\gamma y) \tilde{\phi}_r(x^{-1}\delta\sigma(x)),$$

where  $\tilde{f}^p$  is the characteristic function of  $K^p g^{-1}$  and  $\tilde{\phi}_r$  is the characteristic function of the double coset  $K_r\sigma(a)K_r$ ; we use the Haar measure on  $I(\mathbb{Q})$  giving points measure 1, the Haar measure on  $G(\mathbb{A}_f^p)$  giving  $K_g^p$  measure 1, and the Haar measure on  $G(L_r)$  giving  $K_r$  measure 1. It follows from Lemma 10.7 that  $I(\mathbb{A}_f^p)$  is the centralizer of  $\gamma$  in  $G(\mathbb{A}_f^p)$ , and from Lemma 10.8 that  $I(\mathbb{Q}_p) = G_{\delta\sigma}(\mathbb{Q}_p)$ , the twisted centralizer of  $\delta$  in  $G(L_r)$ . Therefore the integral above is equal to

$$\text{vol}(I(\mathbb{Q}) \setminus I(\mathbb{A}_f)) O_\gamma(\tilde{f}^p) T O_\delta(\tilde{\phi}_r),$$

where

$$\begin{aligned} O_\gamma(\tilde{f}^p) &= \int_{I(\mathbb{A}_f^p) \setminus G(\mathbb{A}_f^p)} \tilde{f}^p(y^{-1}\gamma y), \\ T O_\delta(\tilde{\phi}_r) &= \int_{I(\mathbb{Q}_p) \setminus G(L_r)} \tilde{\phi}_r(x^{-1}\delta\sigma(x)). \end{aligned}$$

It is easy to check that  $O_\gamma(\tilde{f}^p) = O_\gamma(f^p)$ , where  $f^p$  is the characteristic function of  $K^p g^{-1} K^p$  and the orbital integral  $O_\gamma(f^p)$  is taken with respect to the Haar measure on  $G(\mathbb{A}_f^p)$  giving  $K^p$  measure 1 (but still using the other Haar measure to define  $O_\gamma(\tilde{f}^p)$ ). Moreover, replacing  $x$  by  $\sigma(x)$  in the integral defining  $T O_\delta(\tilde{\phi}_r)$  shows that  $T O_\delta(\tilde{\phi}_r) = T O_{\sigma^{-1}(\delta)}(\phi_r)$ ,

where  $\phi_r$  is the characteristic function of  $K_r a K_r$ . But since  $\sigma^{-1}(\delta)$  is  $\sigma$ -conjugate to  $\delta$  (in fact,  $\sigma^{-1}(\delta) = c\delta\sigma(c)^{-1}$  for  $c = \sigma^{-1}(\delta)$ ), we also have that  $TO_{\sigma^{-1}(\delta)}(\phi_r) = TO_\delta(\phi_r)$ . The conclusion is that the number of fixed points  $(\bar{A}, \lambda, i, \bar{\eta})$  for which  $(A, \lambda, i)$  is isogenous to  $(A_0, \lambda_0, i_0)$  is equal to

$$\text{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f)) O_\gamma(f^p) TO_\delta(\phi_r),$$

where  $f^p$  is the characteristic function of  $K^p g^{-1} K^p$ ,  $\phi_r$  is the characteristic function of  $K_r a K_r$ , and where the Haar measure on  $G(\mathbb{A}_f^p)$  (respectively,  $G(L_r)$ ) used to define the orbital integral (respectively, the twisted orbital integral) is the one giving measure 1 to  $K^p$  (respectively,  $K_r$ ).

Recall from §6 the smooth  $\lambda$ -adic sheaf  $\mathcal{F}_{K^p}$  on  $S_{K^p}$  obtained from a finite-dimensional representation  $\xi$  of  $G$ . As above we write  $S$  (respectively,  $S'$ ) for  $S_{K^p}$  (respectively,  $S_{K_g^p}$ ). Suppose that  $x' \in S'(\bar{k})$  is a fixed point of the correspondence

$$S \xleftarrow{a} S' \xrightarrow{c} S$$

considered above, and let  $x \in S(\bar{k})$  denote the common image of  $x'$  under  $a$  and  $c$ . Write  $\mathcal{F}$  (respectively,  $\mathcal{F}'$ ) for  $\mathcal{F}_{K^p}$  (respectively,  $\mathcal{F}_{K_g^p}$ ). Then we have maps

$$\mathcal{F}_x \xrightarrow{\Phi} \mathcal{F}_{b(x')} = (b^* \mathcal{F})_{x'} \simeq \mathcal{F}'_{x'} \xrightarrow{g} (a^* \mathcal{F})_{x'} = \mathcal{F}_x,$$

where we have written  $\Phi$  instead of  $\Phi_p$  and we have put  $g$  above the isomorphism sign as a reminder that the isomorphism between  $a^* \mathcal{F}$  and  $\mathcal{F}'$  depends on  $g$ . The composition of these maps (going from left to right) gives us an automorphism  $\beta$  of the stalk  $\mathcal{F}_x$ . For use in §19 we will now calculate the trace of this automorphism.

The system of sheaves  $\mathcal{F}_{K^p}$  arises from the right action of  $G(\mathbb{A}_f^p)$  on the system of spaces  $S_{K^p}$  and a continuous representation  $\rho$  of  $G(\mathbb{A}_f^p)$  on a finite-dimensional  $\lambda$ -adic vector space  $W$ . The action of  $\Phi$  on this system of spaces gives rise to the usual isomorphism  $\Phi: \Phi^*(\mathcal{F}_{K^p}) \rightarrow \mathcal{F}_{K^p}$ . An easy exercise in using the definition of the sheaves  $\mathcal{F}_{K^p}$  shows that if we pick a point  $\tilde{x}$  of  $\varprojlim S_{K^p}(\bar{k})$  lying over  $x'$ , so that  $\tilde{x}g$  is a point of  $\varprojlim S_{K^p}(\bar{k})$  lying over  $x$ , then the automorphism  $\beta: \mathcal{F}_x \rightarrow \mathcal{F}_x$  is equal to  $\rho(k^{-1}g^{-1})$ , where  $k \in K^p$  is defined by the equality  $\Phi(\tilde{x}) = \tilde{x}gk$  and we have used  $\tilde{x}gk$  to identify  $\mathcal{F}_x$  with  $W$ .

We need to relate  $k^{-1}g^{-1}$  to something more familiar. Suppose that the fixed point  $x'$  is given by  $(\bar{A}, \lambda, i, \bar{\eta})$ . Choosing  $\tilde{x}$  is the same as choosing  $\eta: V_{\mathbb{A}_f^p} \rightarrow H_1(\bar{A}, \mathbb{A}_f^p)$  in the class  $\bar{\eta}$ . As before we let  $u: \sigma^r(\bar{A}) \rightarrow \bar{A}$  denote the unique prime-to- $p$  isogeny commuting with the action of  $\mathcal{O}_B$ , carrying  $\sigma^r(\bar{\eta})$  into  $\bar{\eta}g$  (as level structures of type  $K^p$ ), and carrying  $\lambda$  into a scalar multiple  $c_0$  of  $\sigma^r(\lambda)$ , so that  $A = (\bar{A}, u)$  is a  $c$ -polarized virtual  $B$ -abelian variety over  $k_r$  for  $c = p^r c_0$ . Then  $\sigma^r(\bar{A}, \lambda, i, \eta)$  is isomorphic to  $(\bar{A}, \lambda, i, \pi_A \eta)$ , and therefore  $\sigma^r(\tilde{x}) = \tilde{x}gk$  where  $k \in K^p$  is defined so that  $\pi_A \eta = \eta gk$ . Since

$\eta^{-1}\pi_A^{-1}\eta$  can serve as the usual element  $\gamma \in G(\mathbb{A}_f^p)$  determined by  $A$ , we see that  $k^{-1}g^{-1} = \gamma$ .

We have now shown that the trace of the automorphism  $\beta$  induced by our correspondence at a fixed point  $x'$  is equal to  $\text{tr } \rho(\gamma)$ , where  $\gamma \in G(\mathbb{A}_f^p)$  is the element associated to the  $c$ -polarized virtual  $B$ -abelian variety  $A$  obtained from  $x'$  ( $\gamma$  is well defined up to conjugacy, so that the trace is well defined). In addition to  $\gamma$  we also have the element  $\gamma_0 \in G(\mathbb{Q})$  associated to  $A$ , well defined up to conjugacy in  $G(\mathbb{Q})$ . Our representation  $\rho$  of  $G(\mathbb{A}_f^p)$  is given by projecting  $G(\mathbb{A}_f^p)$  on  $G(\mathbb{Q}_l)$  ( $l$  is the rational prime below the prime  $\lambda$  of the number field  $L$ ) and using the representation  $\xi$  of  $G$  on a finite-dimensional  $L$ -vector space to get a finite-dimensional representation of  $G(L_\lambda)$  on a finite-dimensional  $L_\lambda$ -vector space. Therefore, since  $\gamma_0$  and the  $l$ -adic component of  $\gamma$  are conjugate in  $G(\mathbb{Q}_l)$ , the trace  $\text{tr } \rho(\gamma)$  is also equal to  $\text{tr } \xi(\gamma_0)$ .

### 17. $\mathbb{Q}$ -ISOGENY CLASSES WITHIN A $\bar{\mathbb{Q}}$ -ISOGENY CLASS

Let  $(A, \lambda, i)$  be a  $c$ -polarized virtual  $B$ -abelian variety over  $k_r$  up to isogeny. Let  $(A', i')$  be a virtual  $B$ -abelian variety over  $k_r$  up to isogeny, and let  $\lambda': A' \rightarrow \widehat{A}'$  be a symmetric isogeny commuting with  $B$ . We refer to  $(A', \lambda', i')$  as a symmetrized virtual  $B$ -abelian variety over  $k_r$  up to isogeny.

Suppose that  $(A', \lambda', i')$  is  $\mathbb{Q}$ -isogenous to  $(A, \lambda, i)$  in the sense that there exists a  $\mathbb{Q}$ -isogeny  $f: A \rightarrow A'$  commuting with  $B$  such that  $f^*(\lambda') = d\lambda$  for some  $d \in \mathbb{Q}^\times$ . As in §14 we write  $M$  for  $\text{End}_B(A)$  and  $I$  for the  $\mathbb{Q}$ -group of automorphisms of  $(A, \lambda, i)$ . Then  $\tau \mapsto f^{-1} \circ \tau(f)$  ( $\tau \in \Gamma$ ) is a 1-cocycle of  $\Gamma = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  in  $I(\mathbb{Q})$ .

**Lemma 17.1.** *This construction sets up a bijection from the set of  $\mathbb{Q}$ -isogeny classes of triples  $(A', \lambda', i')$  that are  $\bar{\mathbb{Q}}$ -isogenous to  $(A, \lambda, i)$  to the set  $H^1(\mathbb{Q}, I)$ . Moreover, there exists  $d \in \mathbb{Q}^\times$  such that  $d\lambda'$  is a polarization if and only if the corresponding element of  $H^1(\mathbb{Q}, I)$  has trivial image in  $H^1(\mathbb{R}, I)$ , in which case  $d\lambda'$  is necessarily a  $c$ -polarization.*

It is immediate that the map is well defined and injective. To show surjectivity we start with a 1-cocycle  $a_\tau$  of  $\Gamma$  in  $I(\mathbb{Q})$ . Since  $H^1(\mathbb{Q}, M^\times)$  is trivial (we regard  $M^\times$  as a  $\mathbb{Q}$ -group in the usual way), we see that there exists  $x \in (M \otimes_{\mathbb{Q}} \mathbb{Q})^\times$  such that  $a_\tau = x\tau(x)^{-1}$  for all  $\tau \in \Gamma$ . Put  $\lambda' := \widehat{x}\lambda x \in \text{Hom}_B(A, \widehat{A}) \otimes_{\mathbb{Q}} \mathbb{Q}$ . Then  $\lambda'$  is symmetric and is defined over  $\mathbb{Q}$  up to scalars in  $\mathbb{Q}^\times$ ; from the vanishing of  $H^1(\mathbb{Q}, \mathbb{G}_m)$  we conclude that there exists a scalar (in  $\mathbb{Q}^\times$ ) multiple  $\lambda''$  of  $\lambda'$  such that  $\lambda'' \in \text{Hom}_B(A, \widehat{A})$ . Then  $(A, \lambda'', i)$  is a symmetrized virtual  $B$ -abelian variety over  $k_r$  and by construction  $(A, \lambda'', i)$  is  $\mathbb{Q}$ -isogenous to  $(A, \lambda, i)$  with associated 1-cocycle  $a_\tau$  (use  $x^{-1}$  as the  $\mathbb{Q}$ -isogeny from  $(A, \lambda, i)$  to  $(A, \lambda'', i)$ ). This proves the first statement of the lemma.

For the second statement of the lemma we need to show that a symmetrization  $\lambda'' \in \text{Hom}_B(A, \widehat{A})$  is a scalar multiple of a polarization if and only if

$(A, \lambda'', i)$  is  $\mathbb{R}$ -isogenous to  $(A, \lambda, i)$ . Put  $\lambda'' = \lambda y$  for  $y \in (M \otimes_{\mathbb{Q}} \mathbb{R})_{\text{sym}}$  and let  $d \in \mathbb{Q}^{\times}$ . By Lemma 9.1  $d\lambda''$  is a polarization if and only if  $dy \in (\text{End}(\bar{A}) \otimes_{\mathbb{Q}} \mathbb{R})_+$ . By Lemma 2.9 this happens if and only if  $dy \in (M \otimes_{\mathbb{Q}} \mathbb{R})_+$ , which by Lemma 2.8 happens if and only if  $dy$  is of the form  $x^*x$  for some  $x \in (M \otimes_{\mathbb{Q}} \mathbb{R})^{\times}$ . But  $dy = x^*x$  is equivalent to  $x: A \rightarrow A$  being an  $\mathbb{R}$ -isogeny from  $(A, \lambda'', i)$  to  $(A, \lambda, i)$  such that  $x^*(\lambda) = d\lambda''$ .

It remains to see that if  $\lambda''$  is a polarization, then it is necessarily a  $c$ -polarization. This is clear since the Rosati involution for  $\lambda''$  differs from the Rosati involution for  $\lambda$  by an inner automorphism of  $M$  and  $\pi_A$  belongs to the center of  $M$ , so that  $\pi_A \pi_A^*$  is the same for  $\lambda''$  as it is for  $\lambda$ . This concludes the proof of Lemma 17.1.

Let  $(A', \lambda', i')$  be a symmetrized virtual  $B$ -abelian variety over  $k_r$  up to isogeny, and assume that it is  $\mathbb{Q}$ -isogenous to  $(A, \lambda, i)$ , so that  $(A', \lambda', i')$  corresponds to some element  $\alpha$  of  $H^1(\mathbb{Q}, I)$ . For  $l$  different from  $p$  write  $H_l$  (respectively,  $H'_l$ ) for the skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -module  $H_1(\bar{A}, \mathbb{Q}_l)$  (respectively,  $H_1(\bar{A}', \mathbb{Q}_l)$ ) over  $\mathbb{Q}_l$ . By Lemma 10.7  $I_{\mathbb{Q}_l}$  is the group of automorphisms of the skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -module  $H_l$ . It is clear that  $H_l$  and  $H'_l$  become isomorphic over  $\mathbb{Q}_l$  and that the difference between  $H'_l$  and  $H_l$  is measured by the element of  $H^1(\mathbb{Q}_l, I)$  obtained as the image of  $\alpha$  under

$$H^1(\mathbb{Q}, I) \rightarrow H^1(\mathbb{Q}_l, I).$$

Similarly, write  $(H, \Phi)$  (respectively,  $(H', \Phi')$ ) for the skew-Hermitian isocrystal over  $L_r$  obtained from  $(A, \lambda, i)$  (respectively,  $(A', \lambda', i')$ ). Then by Lemma 10.8  $I_{\mathbb{Q}_p}$  is the group of automorphisms of the skew-Hermitian isocrystal  $(H, \Phi)$ . It is clear that  $(H \otimes_{\mathbb{Q}_p} \mathbb{Q}_p, \Phi \otimes \text{id})$  and  $(H' \otimes_{\mathbb{Q}_p} \mathbb{Q}_p, \Phi' \otimes \text{id})$  are isomorphic as skew-Hermitian isocrystals over  $L_r \otimes_{\mathbb{Q}_p} \mathbb{Q}_p$  (we leave it to the reader to give a meaning—the obvious one—to this term), and that the difference between  $(H, \Phi)$  and  $(H', \Phi')$  is measured by the element of  $H^1(\mathbb{Q}_p, I)$  obtained as the image of  $\alpha$  under

$$H^1(\mathbb{Q}, I) \rightarrow H^1(\mathbb{Q}_p, I).$$

**Lemma 17.2.** *Let  $(A, \lambda, i)$ ,  $(A', \lambda', i')$  be two  $c$ -polarized virtual  $B$ -abelian varieties over  $k_r$  up to isogeny, and suppose that they both satisfy the three conditions of §14, so that we obtain triples  $(\gamma_0; \gamma, \delta)$ ,  $(\gamma'_0; \gamma', \delta')$  from  $(A, \lambda, i)$ ,  $(A', \lambda', i')$  respectively. Then the triples  $(\gamma_0; \gamma, \delta)$  and  $(\gamma'_0; \gamma', \delta')$  are equivalent (that is,  $\gamma_0, \gamma'_0$  are stably conjugate;  $\gamma, \gamma'$  are conjugate;  $\delta, \delta'$  are  $\sigma$ -conjugate) if and only if  $(A', \lambda', i')$  is  $\mathbb{Q}$ -isogenous to  $(A, \lambda, i)$  and the element  $\alpha \in H^1(\mathbb{Q}, I)$  measuring their difference lies in  $\ker^1(\mathbb{Q}, I)$ .*

Assume that  $(A', \lambda', i')$  is  $\mathbb{Q}$ -isogenous to  $(A, \lambda, i)$  and that  $\alpha$  lies in  $\ker^1(\mathbb{Q}, I)$ . The previous discussion shows that  $H_l, H'_l$  are isomorphic as skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules over  $\mathbb{Q}_l$ . Since  $H_l$  (respectively,  $H'_l$ )

is isomorphic to  $V_l$  with  $\pi_A$  acting by the  $l$ -adic component of  $\gamma$  (respectively,  $\gamma'$ ), we see that  $\gamma, \gamma'$  are conjugate in  $G(\mathbb{A}_f^p)$ . Similarly, the previous discussion shows that  $(H, \Phi)$  and  $(H', \Phi')$  are isomorphic as skew-Hermitian isocrystals, and therefore  $\delta, \delta'$  are  $\sigma$ -conjugate in  $G(L_r)$ .

Conversely, suppose that  $(\gamma_0; \gamma, \delta)$  and  $(\gamma'_0; \gamma', \delta')$  are equivalent. It is clear that the functor associating to any  $\mathbb{Q}$ -algebra  $R$  the set of  $R$ -isogenies from  $(A, \lambda, i)$  to  $(A', \lambda', i')$  is representable by a scheme of finite type over  $\mathbb{Q}$  (in fact, by a locally closed subscheme of the affine space  $\text{Hom}_B(A, A')$ ). Pick a prime  $l$  different from  $p$ . Since  $\gamma_l$  is conjugate to  $\gamma'_l$ , Lemma 10.7 implies that this scheme has a  $\mathbb{Q}_l$ -valued point and is therefore nonempty; it then follows that it has a  $\bar{\mathbb{Q}}$ -valued point, which means that  $(A', \lambda', i')$  is  $\bar{\mathbb{Q}}$ -isogenous to  $(A, \lambda, i)$ . Let  $\alpha \in H^1(\mathbb{Q}, I)$  be the element measuring the difference between  $(A, \lambda, i)$  and  $(A', \lambda', i')$ . Then the image of  $\alpha$  in  $H^1(\mathbb{R}, I)$  is trivial by Lemma 17.1. Moreover, by our previous discussion the image of  $\alpha$  in  $H^1(\mathbb{Q}_l, I)$  is trivial for all  $l \neq p$  (since  $\gamma, \gamma'$  are conjugate) and the image of  $\alpha$  in  $H^1(\mathbb{Q}_p, I)$  is trivial (since  $\delta, \delta'$  are  $\sigma$ -conjugate). Thus the element  $\alpha$  is locally trivial at all places of  $\mathbb{Q}$ .

### 18. IMAGE OF THE MAP $(A, \lambda, i) \mapsto (\gamma_0; \gamma, \delta)$

In this section we will find necessary and sufficient conditions on a triple  $(\gamma_0; \gamma, \delta)$  in order that it come from a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$  up to isogeny satisfying the three conditions of §14. In order to do this we need to use the characteristic  $F$ -polynomial of Frobenius for virtual  $F$ -abelian varieties (as usual,  $F$  is the center of  $B$ ).

Let  $A$  be a virtual  $F$ -abelian variety over  $k_r$  up to isogeny,  $c$ -polarizable as virtual abelian variety for some  $c$ , so that  $\pi_A$  is a semisimple element of  $\text{End}_F(A)$ . We will now define the characteristic polynomial  $f_A \in F[T]$  of  $A$ , a monic polynomial of degree  $2 \dim(A)/[F : \mathbb{Q}]$ . The  $F$ -subalgebra  $F[\pi_A]$  of  $\text{End}_F(A)$  generated by  $\pi_A$  is a product of field extensions of  $F$ , say  $F[\pi_A] = F_1 \times \dots \times F_s$ . Let  $l$  be a prime different from  $p$ , choose an algebraic closure  $\bar{\mathbb{Q}}_l$  of  $\mathbb{Q}_l$ , and temporarily take  $\mathbb{Q}$  to be the algebraic closure of  $\mathbb{Q}$  in  $\bar{\mathbb{Q}}_l$ . Denote by  $I$  the set of  $\mathbb{Q}$ -algebra homomorphisms  $i: F[\pi_A] \rightarrow \bar{\mathbb{Q}}_l$ . Then  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  acts on  $I$ , and the orbits of this action correspond bijectively to the  $s$  factors  $F_1, \dots, F_s$ . Let  $m(i)$  denote the multiplicity of the character  $i$  of  $F[\pi_A]$  in the representation of  $F[\pi_A]$  on the  $\mathbb{Q}_l$ -vector space  $H_l \otimes_{\mathbb{Q}_l} \bar{\mathbb{Q}}_l$ , where  $H_l := H_1(\bar{A}, \bar{\mathbb{Q}}_l)$ , as usual.

Since the character of this representation of  $F[\pi_A]$  has rational values, the multiplicity  $m(i)$  depends only on the orbit of  $i$  under  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ; for  $j = 1, \dots, s$  define  $m_l(j)$  to be the common multiplicity of the elements  $i$  in the  $j$ th orbit. Then for all  $\alpha \in F$

$$\text{tr}(\alpha; H_l) = \sum_{j=1}^s m_l(j) \text{tr}_{F_j/\mathbb{Q}}(\alpha).$$

Since the left-hand side of this equation is independent of  $l$ , so is the right-

hand side, which means that  $m_i(j)$  is independent of  $l$ , call it  $m(j)$ . Let  $V$  be the  $F[\pi_A]$ -module  $\bigoplus_{j=1}^s F_j^{m(j)}$ . Then we have shown that  $H_l$  is isomorphic to  $V \otimes_{\mathbb{Q}} \mathbb{Q}_l$  as  $F[\pi_A]$ -module over  $\mathbb{Q}_l$ . We define  $f_A$  to be the characteristic polynomial of the endomorphism  $\pi_A$  of the  $F$ -vector space  $V$ . Note that  $V$  has dimension  $2 \dim(A)$  over  $\mathbb{Q}$ , hence that  $2 \dim(A)$  is divisible by  $[F : \mathbb{Q}]$  and  $f_A$  is monic of degree  $2 \dim(A)/[F : \mathbb{Q}]$ .

We return to the notation of §14. In §10 we described completely the simple objects in the category  $\mathcal{V}_{r,c,B}$  of  $B$ -objects in the category of  $c$ -polarizable virtual abelian varieties  $A$  over  $k_r$  up to isogeny. We have just seen that  $2 \dim(A)$  must be divisible by  $[F : \mathbb{Q}]$  for any such  $A$ . Fix a positive integer  $m$  and consider the problem of determining the isomorphism classes of objects  $A$  in  $\mathcal{V}_{r,c,B}$  such that  $2 \dim(A) = [F : \mathbb{Q}]m$ . For such an object  $A$  the construction above gives us a monic polynomial  $f_A \in F[T]$  of degree  $m$ .

Now let  $f \in F[T]$  be monic of degree  $m$ . From our work in §10 we see that  $f$  comes from some  $A$  in  $\mathcal{V}_{r,c,B}$  if and only if every root  $\alpha$  of  $f$  in  $\bar{F}$  is a  $c$ -number and the multiplicity  $m(\alpha)$  of each root  $\alpha$  of  $f$  is divisible by its multiplicity in the characteristic polynomial  $f_\alpha$  of the simple virtual  $B$ -abelian variety  $A_\alpha$  corresponding to  $\alpha$ .

Define a positive integer  $d$  by the condition  $d^2 = \dim_F B$ . The roots of  $f_\alpha$  are the various conjugates of  $\alpha$  over  $F$ , and each has the same multiplicity, namely,  $2 \dim(A_\alpha)/[F[\alpha] : \mathbb{Q}]$ , which by Lemma 10.13 is equal to  $de$ , where  $e = (\dim_{F[\alpha]} \text{End}_B(A_\alpha))^{1/2}$ . It is well known that  $e$  is equal to the order of the class of  $\text{End}_B(A_\alpha)$  in the Brauer group of  $F[\alpha]$ , or, in other words, to the least positive integer  $e$  such that  $e \cdot \text{inv}_v(\text{End}_B(A_\alpha)) = 0$  for every place  $v$  of  $F[\alpha]$ . Applying Lemma 10.13, we see that  $f$  comes from some  $A$  in  $\mathcal{V}_{r,c,B}$  if and only if every root  $\alpha$  of  $f$  in  $\bar{F}$  is a  $c$ -number and the multiplicity  $m(\alpha)$  of each root  $\alpha$  of  $f$  has the property that it is divisible by  $d$  and for every place  $v$  of  $F[\alpha]$  the element

$$\begin{cases} \frac{1}{2} - \text{inv}_v(B \otimes_F F[\alpha]) & \text{if } v \text{ is real,} \\ [F[\alpha]_v : \mathbb{Q}_p]v(\alpha)/v(p^r) - \text{inv}_v(B \otimes_F F[\alpha]) & \text{if } v \text{ divides } p, \\ -\text{inv}_v(B \otimes_F F[\alpha]) & \text{otherwise} \end{cases}$$

of  $\mathbb{Q}/\mathbb{Z}$  is killed by  $m(\alpha)/d$ .

We will now use this discussion to determine the image of the map  $(A, \lambda, i) \mapsto (\gamma_0; \gamma, \delta)$ . Let  $c$  be a positive rational number of the form  $p^r c_0$ , where  $c_0$  is a  $p$ -adic unit. Suppose that  $(A, \lambda, i)$  is a  $c$ -polarized virtual  $B$ -abelian variety over  $k_r$  up to isogeny satisfying the three conditions of §14. In §14 we associated to  $(A, \lambda, i)$  a triple  $(\gamma_0; \gamma, \delta)$  satisfying the conditions of §2 of [K5]. Now let  $(\gamma_0; \gamma, \delta)$  be a triple satisfying the conditions of §2 in [K5].

**Lemma 18.1.** *There exists a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$ , satisfying the three conditions of §14, such that the triple associated to  $(A, \lambda, i)$  is  $(\gamma_0; \gamma, \delta)$ , if and only if the following three conditions hold:*

- (1)  $\gamma_0 \gamma_0^* = c^{-1}$ ,
- (2)  $\alpha(\gamma_0; \gamma, \delta)$  is trivial,

(3) there exists a lattice  $\Lambda$  in  $V_{L_r}$  such that  $(\delta\sigma)(\Lambda) \supset \Lambda$ .

First we show that if  $(\gamma_0; \gamma, \delta)$  comes from  $(A, \lambda, i)$ , then it satisfies (1), (2), and (3). In fact, (1) is obvious and Lemma 15.1 asserts that (2) holds. Since  $A$  comes from a virtual abelian variety up to prime-to- $p$  isogeny there is a lattice  $\Lambda$  in  $H$  such that  $\Phi(\Lambda) \supset \Lambda$  and the corresponding lattice in  $V_{L_r} \simeq H$  satisfies  $(\delta\sigma)(\Lambda) \supset \Lambda$ , which shows that (3) holds as well.

Now suppose that  $(\gamma_0; \gamma, \delta)$  satisfies (1), (2), and (3). Put  $\pi := \gamma_0^{-1}$ . Then  $c = \pi\pi^*$ . The endomorphism  $\pi$  of the  $B$ -module  $V$  is  $F$ -linear and hence has a characteristic polynomial  $f \in F[T]$ , monic of degree  $m$ , where  $m = \dim_F V$ . Our first goal is to show that there exists an object  $A$  of  $\mathcal{V}_{r,c,B}$  whose dimension satisfies  $2\dim(A) = [F : \mathbb{Q}]m$  and whose characteristic polynomial is  $f$ . As we saw earlier in this section, there are two conditions to check.

The first is that every root of  $f$  be a  $c$ -number. Since  $\pi$  is elliptic in  $G(\mathbb{R})$ , every root of  $f$  in  $\mathbb{C}$  has the same absolute value, and since  $\pi\pi^* = c$ , this absolute value must be  $c^{1/2}$ . The inverse of  $N\delta := \delta\sigma(\delta) \cdots \sigma^{r-1}(\delta) \in G(L_r)$  satisfies  $(N\delta)^{-1}(\Lambda) \subset \Lambda$ , where  $\Lambda$  is the lattice whose existence is asserted in (3). Since  $N\delta$  is conjugate to  $\gamma_0$  in  $G(\bar{L}_r)$ , it follows that every root of  $f$  in  $\mathbb{Q}_p$  belongs to the valuation ring of  $\mathbb{Q}_p$ . Therefore the roots of  $f$  are indeed  $c$ -numbers.

The second condition to check is the one on the multiplicities  $m(\alpha)$  of the roots  $\alpha$  of  $f$ . Let  $\alpha$  be a root of  $f$  in  $\bar{F}$  and let  $v$  be a place of  $F[\alpha]$ . Begin with the case that  $v$  lies over a prime  $l$  different from  $p$ . Then  $V \otimes_F F[\alpha]_v$  is a  $B \otimes_F F[\alpha]_v$ -module admitting the semisimple automorphism  $\pi$ . By Lemma 3.5 and Corollary 3.4  $m(\alpha)$  is divisible by  $d$  and  $m(\alpha)/d$  kills the element  $-\text{inv}_v(B \otimes_F F[\alpha])$  of  $\mathbb{Q}/\mathbb{Z}$ .

Next consider the case in which  $v$  divides  $p$ . Then  $V \otimes_F F[\alpha] \otimes_{\mathbb{Q}} L_r$  admits the  $\sigma$ -linear bijection  $\Phi := \delta\sigma$ , commuting with the action of  $B \otimes_F F[\alpha]$ . We have

$$F[\alpha] \otimes_{\mathbb{Q}} L_r = \prod_{v|p} F[\alpha]_v \otimes_{\mathbb{Q}_p} L_r$$

and a corresponding decomposition

$$V \otimes_F F[\alpha] \otimes_{\mathbb{Q}} L_r = \bigoplus_{v|p} V \otimes_F (F[\alpha]_v \otimes_{\mathbb{Q}_p} L_r),$$

as well as a direct sum decomposition  $\Phi = \bigoplus_{v|p} \Phi_v$ , where  $\Phi_v$  is a  $\sigma$ -linear bijection on  $V \otimes_F F[\alpha]_v \otimes_{\mathbb{Q}_p} L_r$ , commuting with the action of  $B \otimes_F F[\alpha]_v$ . Since  $\pi^{-1}$  is conjugate in  $G(\bar{L}_r)$  to  $N\delta$ , the number  $m(\alpha)$  is equal to the multiplicity of  $\alpha^{-1}$  as a root of the characteristic polynomial of the  $B \otimes_F F[\alpha]_v$ -object  $V \otimes_F (F[\alpha]_v \otimes_{\mathbb{Q}_p} L_r)$  in the category of semisimple isocrystals over  $L_r$ . It follows from Lemmas 11.5 and 11.6 that  $m(\alpha)$  is divisible by  $d$  and that  $m(\alpha)/d$  kills the element

$$[F[\alpha]_v : \mathbb{Q}_p]v(\alpha)/v(p') - \text{inv}_v(B \otimes_F F[\alpha])$$

of  $\mathbb{Q}/\mathbb{Z}$  (use that  $v(\alpha^{-1}) = -v(\alpha)$ ).

Finally consider the case in which  $v$  is real. We have the standing assumption that we are in Case A or C, and Case A is excluded since  $F$  is then totally complex. In Case C the field  $F$  is totally real and we are assuming that  $F[\alpha]_v$  is real, which happens if and only if  $\alpha = \pm c^{1/2}$ . As usual we denote by  $C$  the algebra  $\text{End}_B(V)$  and we write  $C_v$  for  $C \otimes_F F_v$ . In §7 we noted that in Case C the algebra  $C_v$  is isomorphic to  $M_{2n}(\mathbb{R})$  and that  $G_1(F_v)$  is isomorphic to  $\text{Sp}_{2n}(\mathbb{R})$ . Put  $\pi_1 = c^{-1/2}\pi_0$ . The multiplicity of  $c^{1/2}$  (respectively,  $-c^{1/2}$ ) as a root of  $f$  is equal to  $d$  times the multiplicity of 1 (respectively, -1) as an eigenvalue of  $\pi_1 \in \text{Sp}_{2n}(\mathbb{R})$ , and it is easy to see that the multiplicities of 1 and -1 as eigenvalues of any element of  $\text{Sp}_{2n}(\mathbb{C})$  are both even. Therefore, when  $v$  is real the number  $m(\alpha)/d$  is even and hence kills the element

$$\frac{1}{2} - \text{inv}(B \otimes_F F[\alpha]_v)$$

of  $\mathbb{Q}/\mathbb{Z}$ .

At this point we have completed the first step of the argument. We now know that there exists a  $B$ -object  $(A, i)$  in the category of  $c$ -polarizable virtual abelian varieties over  $k_r$  up to isogeny such that the characteristic polynomial of  $(A, i)$  is equal to the characteristic polynomial of  $\gamma_0^{-1}$ .

Choose a  $c$ -polarization  $\lambda$  of the  $B$ -abelian variety  $(A, i)$  (for existence use Lemma 9.2, applied to the  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -abelian variety  $\bar{A}$  over  $\bar{k}$  and the involution obtained as the tensor product of the involution  $*$  on  $B$  and the involution  $\pi_A \mapsto c\pi_A^{-1}$  on  $\mathbb{Q}[\pi_A]$ , the latter of which is positive by the proof of Lemma 10.1). We now have a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$  up to isogeny and a semisimple element  $\gamma_0 \in G(\mathbb{Q})$ , elliptic in  $G(\mathbb{R})$ , with  $\gamma_0\gamma_0^* = c^{-1}$ , such that for every prime  $l$  different from  $p$  the characteristic  $F$ -polynomials of  $\gamma_0^{-1}$  on  $V_l := V \otimes_{\mathbb{Q}} \mathbb{Q}_l$  and  $\pi_A$  on  $H_l$  are equal. It follows that the  $B \otimes_{\mathbb{Q}} \mathbb{Q}[T]$ -modules  $V_l$  and  $H_l$  are isomorphic, where  $T$  acts on  $V_l$  by  $\gamma_0^{-1}$  and on  $H_l$  by  $\pi_A$ . Therefore we are in the situation of §15 and have the element  $\alpha(\gamma_0; A, \lambda, i) \in X^*(Z(\widehat{I}_0)^\Gamma)$ , where  $I_0 = G_{\gamma_0}$ , as usual. Lemma 15.2 says that  $\alpha(\gamma_0; A, \lambda, i)$  is trivial. By hypothesis the element  $\alpha(\gamma_0; \gamma, \delta) \in X^*(Z(\widehat{I}_0)^\Gamma)$  is also trivial (recall that in §15 we showed that  $Z(\widehat{I}_0)^\Gamma$  maps onto  $\mathcal{K}(I_0/\mathbb{Q})$  in Cases A and C, so that we are free to work with  $Z(\widehat{I}_0)^\Gamma$  rather than  $\mathcal{K}(I_0/\mathbb{Q})$ ).

The element  $\alpha(\gamma_0; A, \lambda, i)$  (respectively,  $\alpha(\gamma_0; \gamma, \delta)$ ) was defined as the product of the restrictions of local elements  $\alpha_v(\gamma_0; A, \lambda, i)$  (respectively,  $\alpha_v(\gamma_0; \gamma, \delta)$ ) in  $X^*(Z(\widehat{I}_0)^{\Gamma(v)})$ . Put  $I = \text{Aut}(A, \lambda, i)$ , an inner form of  $I_0$ . For any place  $v$  of  $\mathbb{Q}$  put  $\beta_v = \alpha_v(\gamma_0; \gamma, \delta) - \alpha_v(\gamma_0; A, \lambda, i)$ . It follows immediately from the definitions that  $\beta_\infty$  is trivial. For  $l$  different from  $p$  the element  $\beta_l$  is the image under

$$H^1(\mathbb{Q}_l, I) \rightarrow \pi_0(Z(\widehat{I}_0)^{\Gamma(l)})^D$$

of the element of  $H^1(\mathbb{Q}_l, I)$  measuring the difference between the skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -modules  $H_l$  and  $V_l$  over  $\mathbb{Q}_l$ , with  $\pi_A$  acting on  $V_l$

by the  $l$ -adic component of  $\gamma^{-1} \in G(\mathbb{A}_f^p)$  (we used Lemma 10.7 to identify  $I_{\mathbb{Q}_l}$  with the group of automorphisms of the skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$ -module  $H_l$  over  $\mathbb{Q}_l$ ). Similarly the element  $\beta_p$  is the image under

$$H^1(\mathbb{Q}_p, I) \rightarrow \pi_0(Z(\widehat{I}_0)^{\Gamma(p)})^D$$

of the element of  $H^1(\mathbb{Q}_p, I)$  that measures the difference between the skew-Hermitian isocrystals  $(H, \Phi)$  and  $(V_{L_r}, \delta\sigma)$  over  $L_r$  (we used Lemma 10.8 to identify  $I_{\mathbb{Q}_p}$  with the group of automorphisms of the skew-Hermitian isocrystal  $(H, \Phi)$ ).

By Proposition 2.6 of [K4] there exists  $\beta \in H^1(\mathbb{Q}, I)$  whose image in  $H^1(\mathbb{Q}_v, I)$  is  $\beta_v$  for every place  $v$  of  $\mathbb{Q}$  (since the product over  $v$  of the restrictions of  $\beta_v$  to  $Z(\widehat{I}_0)^{\Gamma}$  is equal to the difference of  $\alpha(\gamma_0; \gamma, \delta)$  and  $\alpha(\gamma_0; A, \lambda, i)$  and is therefore trivial). According to Lemma 17.1 there is a  $c$ -polarized virtual  $B$ -abelian variety  $(A', \lambda', i')$  over  $k_r$ ,  $\mathbb{Q}$ -isogenous to  $(A, \lambda, i)$ , such that  $\beta$  measures the difference between  $(A, \lambda, i)$  and  $(A', \lambda', i')$ . It follows from the discussion above together with the discussion preceding Lemma 17.2 that  $H'_l$  is isomorphic to  $V_l$  as a skew-Hermitian  $B \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_{A'}]$ -module and  $(H', \Phi')$  is isomorphic to  $(V_{L_r}, \delta\sigma)$  as a skew-Hermitian isocrystal over  $L_r$ , where we are using a “prime” to indicate objects attached to  $(A', \lambda', i')$ . Clearly  $(A', \lambda', i')$  satisfies the three conditions of §14 (recall the condition imposed on  $\delta$  in §2 of [K5]) and  $(A', \lambda', i') \mapsto (\gamma_0; \gamma, \delta)$  (use Lemma 7.1 to check that  $\gamma_0$  is right). This completes the proof of Lemma 18.1.

## 19. TOTAL NUMBER OF FIXED POINTS

In this section we will combine the results of the previous sections, obtaining an expression for the number of fixed points of the correspondence  $\Phi_{\mathfrak{p}}^j \circ f$  of §16 and, more generally, for the sum

$$T(j, f) := \sum_{x' \in \text{Fix}} \text{tr}(\Phi_{\mathfrak{p}}^j \circ f; \mathcal{F}_{x'}),$$

where  $\text{Fix}$  denotes the set of fixed points of  $\Phi_{\mathfrak{p}}^j \circ f$ . We keep the notation of §§14–18.

In §16 we associated to each  $x' \in \text{Fix}$  a positive rational number  $c$  of the form  $c_0 p^{r'}$ , where  $c_0$  is a  $p$ -adic unit, and a  $c$ -polarized virtual  $B$ -abelian variety  $(A, \lambda, i)$  over  $k_r$  up to isogeny, satisfying the three conditions of §14. Therefore  $T(j, f)$  can be decomposed as

$$(19.1) \quad T(j, f) = \sum_c \sum_{(A, \lambda, i)} T(A, \lambda, i),$$

where  $c$  runs through rational numbers of the type mentioned above and  $(A, \lambda, i)$  runs through the isogeny classes of  $c$ -polarized virtual  $B$ -abelian varieties over  $k_r$  satisfying the three conditions of §14 and where

$$T(A, \lambda, i) = \sum_{x'} \text{tr}(\Phi_{\mathfrak{p}}^j \circ f; \mathcal{F}_{x'})$$

with  $x'$  running through those fixed points to which is associated  $(A, \lambda, i)$ .

In §14 we associated to each  $(A, \lambda, i)$  as above a triple  $(\gamma_0; \gamma, \delta)$  satisfying the conditions of §2 of [K5] and having the property that  $\alpha(\gamma_0; \gamma, \delta) = 1$  (Lemma 15.1). In §16 we calculated  $T(A, \lambda, i)$  in terms of  $(\gamma_0; \gamma, \delta)$ ,

$$(19.2) \quad T(A, \lambda, i) = \text{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f)) O_\gamma(f^p) T O_\delta(\phi_r) \text{tr} \xi(\gamma_0).$$

Recall from the discussion at the end of §14 that  $I$  is the inner form of  $I_0 = G_{\gamma_0}$  constructed from  $(\gamma_0; \gamma, \delta)$  in §3 of [K5]. Since the expression in (19.2) depends only on  $(\gamma_0; \gamma, \delta)$ , we can denote it by  $T(\gamma_0; \gamma, \delta)$ . Then

$$(19.3) \quad T(j, f) = \sum_{(\gamma_0; \gamma, \delta)} n(\gamma_0; \gamma, \delta) T(\gamma_0; \gamma, \delta),$$

where the sum is taken over the equivalence classes (see Lemma 17.2) of triples  $(\gamma_0; \gamma, \delta)$  satisfying the conditions of §2 of [K5] and having the property that  $\alpha(\gamma_0; \gamma, \delta) = 1$ , and where  $n(\gamma_0; \gamma, \delta)$  denotes the number of  $c$ -polarized (for some  $c$ ) virtual abelian varieties  $(A, \lambda, i)$  satisfying the three conditions of §14 such that  $(A, \lambda, i) \leftrightarrow (\gamma_0; \gamma, \delta)$ . If  $n(\gamma_0; \gamma, \delta)$  is nonzero, then by Lemma 17.2 it is equal to  $|\ker^1(\mathbb{Q}, I)|$ , which by (4.2.2) of [K2] is also equal to  $|\ker^1(\mathbb{Q}, I_0)|$ . Therefore, if  $n(\gamma_0; \gamma, \delta)$  is nonzero, we have

$$(19.4) \quad n(\gamma_0; \gamma, \delta) T(\gamma_0; \gamma, \delta) = |\ker^1(\mathbb{Q}, I_0)| T(\gamma_0; \gamma, \delta).$$

In fact (19.4) is valid even when  $n(\gamma_0; \gamma, \delta)$  is 0. What we must check is that  $n(\gamma_0; \gamma, \delta) = 0$  implies  $T(\gamma_0; \gamma, \delta) = 0$ . Suppose that  $T(\gamma_0; \gamma, \delta)$  is nonzero. Put  $c = (\gamma_0 \gamma_0^*)^{-1} \in \mathbb{Q}^\times$ . Since  $\gamma_0$  is elliptic in  $G(\mathbb{R})$ ,  $c$  is positive. Since  $T(\gamma_0; \gamma, \delta)$  is nonzero, so is  $T O_\delta(\phi_r)$  and from this it follows that the  $p$ -adic absolute value of  $\delta \delta^* \in L_r^\times$  is equal to that of  $p^{-1}$ , which implies that  $c = p' c_0$  for a  $p$ -adic unit  $c_0$ . It follows from Lemma 18.1 that  $n(\gamma_0; \gamma, \delta)$  is nonzero: it is obvious that conditions (1) and (2) of that lemma hold, and since  $T O_\delta(\phi_r)$  is nonzero, condition (3) holds as well.

Now consider the factor  $|\ker^1(\mathbb{Q}, I_0)|$  appearing in (19.4). In both Cases A and C the map

$$\ker^1(\mathbb{Q}, Z) \rightarrow \ker^1(\mathbb{Q}, G)$$

is surjective (see §7), where  $Z$  denotes the center of  $G$ . Therefore the map

$$\ker^1(\mathbb{Q}, I_0) \rightarrow \ker^1(\mathbb{Q}, G)$$

is surjective, and it follows easily from Lemmas 4.3.1 and 4.3.2 of [K2] that all the fibers of this map have the same cardinality. Therefore  $|\ker^1(\mathbb{Q}, I_0)|$  is the product of  $|\ker^1(\mathbb{Q}, G)|$  and

$$|\ker[\ker^1(\mathbb{Q}, I_0) \rightarrow \ker^1(\mathbb{Q}, G)]|.$$

As in §3 of [K5] we define  $c(\gamma_0; \gamma, \delta)$  to be the product of  $\text{vol}(I(\mathbb{Q}) \backslash I(\mathbb{A}_f))$  and

$$|\ker[\ker^1(\mathbb{Q}, I_0) \rightarrow \ker^1(\mathbb{Q}, G)]|.$$

Our final result is that  $T(j, f)$  is equal to

$$(19.5) \quad |\ker^1(\mathbb{Q}, G)| \sum_{(\gamma_0; \gamma, \delta)} c(\gamma_0; \gamma, \delta) O_\gamma(f^p) T O_\delta(\phi_r) \operatorname{tr} \xi(\gamma_0),$$

with  $(\gamma_0; \gamma, \delta)$  running through all equivalence classes of triples satisfying the conditions of §2 of [K5] and having the property that  $\alpha(\gamma_0; \gamma, \delta) = 1$ . The functions  $f^p$  and  $\phi_r$  are the ones defined in §16.

In §8 we saw that  $S_{K^p}$  is the disjoint union of  $|\ker^1(\mathbb{Q}, G)|$  copies of the canonical model for the Shimura variety associated to the data  $(G, h^{-1}, K^p)$ . Therefore the analog of  $T(j, f)$  for a single copy of the canonical model is

$$(19.6) \quad \sum_{(\gamma_0; \gamma, \delta)} c(\gamma_0; \gamma, \delta) O_\gamma(f^p) T O_\delta(\phi_r) \operatorname{tr} \xi(\gamma_0),$$

which is the formula (3.1) of [K5], except for the following point. In [K5] it is claimed that (19.6) is the value of  $T(j, f)$  for the Shimura variety associated to  $(G, h, K^p)$ ; however, we have just seen that it should be  $(G, h^{-1}, K^p)$  rather than  $(G, h, K^p)$ . Of course this mistake also affects the conclusion of [K5]: the right conjecture is that the virtual representation of  $\mathcal{H}_L$  and  $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  described in §10 of that paper be equal to the virtual representation

$$\bigoplus_{i=0}^{2 \dim S_K} (-1)^i IH^i(\bar{S}_K, \mathcal{F}) \otimes L_\lambda$$

for the canonical model  $S_K$  for  $(G, h^{-1}, K)$  (rather than  $(G, h, K)$ ).

## REFERENCES

- [B] A. Borel, et. al., *Seminar on algebraic groups and related finite groups*, Lecture Notes in Math., vol. 131, Springer, Heidelberg, 1970.
- [BS] A. Borel and J-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comment. Math. Helv. **39** (1964), 111–164.
- [D1] P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.
- [D2] ———, *Travaux de Griffiths*, Sémin. Bourbaki Mai 1970, Exposé 376, Lecture Notes in Math., vol. 180, Springer, Heidelberg, 1971.
- [D3] ———, *Travaux de Shimura*, Sémin. Bourbaki Février 1971, Exposé 389, Lecture Notes in Math., vol. 244, Springer, Heidelberg, 1971.
- [D4] ———, *Variétés de Shimura*, Automorphic Forms, Representations and  $L$ -functions, Proc. Sympos. Pure Math., vol. 33, Amer. Math. Soc., Providence, RI, 1979, pp. 247–290.
- [Fa] G. Faltings, *Crystalline cohomology and  $p$ -adic Galois representations*, Algebraic Analysis, Geometry, and Number Theory, The Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 25–80.
- [F] J.-M. Fontaine, *Sur certains types de représentations  $p$ -adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Ann. of Math. (2) **115** (1982), 529–577.
- [FM] J.-M. Fontaine and W. Messing,  *$p$ -adic periods and  $p$ -adic étale cohomology*, Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 179–207.
- [H] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

- [I1] Y. Ihara, *The congruence monodromy problems*, J. Math. Soc. Japan **20** (1968), 107–121.
- [I2] ——, *On congruence monodromy problems I, II*, Univ. of Tokyo, 1968, 1969.
- [K1] R. Kottwitz, *Shimura varieties and twisted orbital integrals*, Math. Ann. **269** (1984), 287–300.
- [K2] ——, *Stable trace formula: cuspidal tempered terms*, Duke Math. J. **51** (1984), 611–650.
- [K3] ——, *Isocrystals with additional structure*, Compositio Math. **56** (1985), 201–220.
- [K4] ——, *Stable trace formula: elliptic singular terms*, Math. Ann. **275** (1986), 365–399.
- [K5] ——, *Shimura varieties and  $\lambda$ -adic representations*, Automorphic Forms, Shimura Varieties and  $L$ -functions, part 1, Perspectives in Mathematics, vol. 10, Academic Press, San Diego, CA, 1990, pp. 161–209.
- [L1] R. P. Langlands, *Some contemporary problems with origins in the Jugendtraum*, Mathematical Developments Arising from Hilbert Problems, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, RI, 1976, pp. 401–418.
- [L2] ——, *Shimura varieties and the Selberg trace formula*, Canad. J. Math. **29** (1977), 1292–1299.
- [L3] ——, *On the zeta-functions of some simple Shimura varieties*, Canad. J. Math. **31** (1979), 1121–1216.
- [L4] ——, *Automorphic representations, Shimura varieties and motives*, Automorphic Forms, Representations and  $L$ -functions, Proc. Sympos. Pure Math., vol. 33, 1979, Amer. Math. Soc., Providence, RI, pp. 205–246.
- [L5] ——, *Les débuts d'une formule des traces stable*, Publ. Math. Univ. Paris VII, vol. 13, Paris, 1983.
- [LR] R. P. Langlands and M. Rapoport, *Shimuravarietäten und Gerben*, J. Reine Angew. Math. **378** (1987), 113–220.
- [Me] W. Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Math., vol. 264, Springer, Heidelberg, 1972.
- [Mi1] J. S. Milne, *Points on Shimura varieties mod  $p$* , Automorphic Forms, Representations and  $L$ -functions, Proc. Sympos. Pure Math., vol. 33, 1979, Amer. Math. Soc., Providence, RI, pp. 165–184.
- [Mi2] ——, *The conjecture of Langlands and Rapoport for Siegel modular varieties*, Bull. Amer. Math. Soc. **24** (1991), 335–341.
- [M1] D. Mumford, *Geometric invariant theory*, Springer, Heidelberg, 1965.
- [M2] ——, *Abelian varieties*, Oxford Univ. Press, London, 1974.
- [RZ1] H. Reimann and T. Zink, *Der Dieudonnémodul einer polarisierten abelschen Mannigfaltigkeit vom CM-Typ*, Ann. of Math. (2) **128** (1988), 461–482.
- [RZ2] ——, *The good reduction of Shimura varieties associated to quaternion algebras over a totally real number field*, preprint.
- [SeT] J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
- [S] G. Shimura, *Moduli of abelian varieties and number theory*, Algebraic Groups and Discontinuous Subgroups, Proc. Sympos. Pure Math., vol. 9, 1966 Amer. Math. Soc., Providence, RI, pp. 312–332.
- [ST] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, no. 6, 1961.
- [St] R. Steinberg, *Regular elements of semisimple algebraic groups*, Inst. Hautes Études Sci. Publ. Math. **25** (1965), 49–80.
- [T1] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Congress Math., Stockholm, 1962, pp. 288–295.
- [T2] ——, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

- [T3] ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Sémin. Bourbaki Nov. 1968, Exposé 352.
- [Z1] T. Zink, *Über die schlechte Reduktion einiger Shimuramannigfaltigkeiten*, Compositio Math. **45** (1981), 15–107.
- [Z2] ———, *Isogenieklassen von Punkten von Shimuramannigfaltigkeiten mit Werten in einem endlichen Körper*, Math. Nachr. **112** (1983), 103–124.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO, CHICAGO, ILLINOIS 60637