ORDINARY POINTS MOD p OF $\mathrm{GL}_n(\mathbb{R})$-LOCALLY SYMMETRIC SPACES

MARK GORESKY AND YUNG SHENG TAI

ABSTRACT. Locally symmetric spaces for $\mathrm{GL}_n(\mathbb{R})$ parametrize polarized complex Abelian varieties with real structure (anti-holomorphic involution). This paper introduces a mod p analog. The authors define an "anti-holomorphic" involution (or "real structure") on an ordinary Abelian variety (defined over a finite field k) to be an involution of the associated Deligne module (T,F,V) that exchanges F (the Frobenius) with V (the Verschiebung). The definition extends to include principal polarizations and level structures. The authors show there are finitely many isomorphism classes of such objects in each dimension, and they give a formula for this number that resembles the Kottwitz "counting formula" (for the number of principally polarized Abelian varieties over k), but the symplectic group in the Kottwitz formula has been replaced by the general linear group.

1. Introduction

1.1. Let $N \geq 3$ be an integer and let $\Gamma_N \subset \mathrm{Sp}_{2n}(\mathbb{Z})$ be the principal level N subgroup consisting of elements that are congruent to the identity modulo N. The locally symmetric space $Y = \Gamma_N \backslash \mathrm{Sp}_{2n}(\mathbb{R})/U(n)$ may be viewed as the set of complex points of the moduli space $\mathcal{A}_{n,[N]}$ of principally polarized complex n dimensional Abelian varieties with level N structure. It admits the structure of a complex algebraic variety and it has an incarnation "modulo p", namely, the moduli space $\mathcal{A}_{n,[N]}(k)$ of principally polarized Abelian varieties (of dimension n with level N structure) over a finite field $k = \mathbb{F}_q$ of characteristic p. The number of points in $\mathcal{A}_{n,[N]}(k)$ was computed by R. Kottwitz [36, 37], proving a reformulation of the conjecture of R. Langlands and M. Rapoport ([38]), following earlier work on this question by J. Milne, W. Waterhouse, R. Langlands, M. Rapoport and others.

For $n \geq 3$ the locally symmetric space $X = \mathrm{GL}_n(\mathbb{Z}) \backslash \mathrm{GL}_n(\mathbb{R})/\mathrm{O}(n)$ does not have a complex structure. Nevertheless in many ways this space behaves something like an algebraic variety, perhaps most spectacularly illustrated by the success ([21, 22, 47, 4, 60, 51]) in associating Galois representations to modular forms on X. This leads to the search for other ways in which the locally symmetric space X behaves like the algebraic variety Y. Is it possible to make sense of the points of X "modulo p", and to provide a concrete description and count for the points of X over the finite field $\mathbb{F}_q$?

With appropriate level structures, finitely many copies of the space X sit inside Y in a natural way. In a previous paper ([17]) the authors showed that the (principally polarized) Abelian varieties corresponding to points $x \in X$ are precisely those which admit a real structure, that is, an anti-holomorphic involution. Therefore one might hope to identify the finite field analog of X as

1991 *Mathematics Subject Classification.* 11FXX, 14G35, 14KXX, 11G25, 14PXX.

a parameter space for principally polarized Abelian varieties over $\mathbb{F}_q$ equipped with an "anti-holomorphic involution", whatever that means.

1.2. A hint is provided by the theory of complex multiplication. If a simple CM Abelian variety A has good reduction to a variety $\overline{A}$ over $\mathbb{F}_q$ then the Frobenius morphism F has a lift to an element $\pi \in \mathrm{End}_{\mathbb{Q}}(A)$. Complex conjugation takes π to $\bar{\pi} = q\pi^{-1}$ (since π is a Weil q-number) which is a lift of the Vershiebung V. Therefore if "complex conjugation" is to make sense on $\overline{A}$ it must switch F and V. Is it possible to enlarge the collection of morphisms for Abelian varieties over $\mathbb{F}_q$ so as to allow for generalized morphisms that switch the Frobenius with the Vershiebung?

1.3. In this paper we show how to make sense of these notions for *ordinary* Abelian varieties over $\mathbb{F}_q$ using P. Deligne's linear algebra description [10] of the category of ordinary Abelian varieties as equivalent to the category of Deligne modules (T, F). We define a real structure on (T, F) to be an involution $\tau : T \to T$ that switches F and $V = qF^{-1}$. This simple, almost trivial definition leads to a wealth of interesting structures. The definition extends naturally to include polarizations (using Howe's theorem [24]) and level structures so we obtain a category of "real" polarized Deligne modules. We show there are finitely many isomorphism classes of real Deligne modules (T, F, τ) (with principal polarization and level structure) over $\mathbb{F}_q$, and we are able to count them. For $n = 1$ in §7.4 we find, asymptotically $C(p)q^{1/2}\log q$ objects, (for q an odd power of p). For general n we show that the method ([36, 37]) of Kottwitz may be modified to give a formula, involving adèlic orbital integrals at p and away from p, that closely resembles the finite adèlic part of the (relative) trace formula.

1.4. Conceptually, the general formula (§10.5) may be described as follows. By appropriate choice of coordinates it turns out that the Frobenius morphism F for an ordinary Abelian variety with real structure (that is, for a polarized Deligne module with involution (T, F, τ)) may be expressed as a semisimple element $\gamma_0 = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right) \in \mathrm{GSp}_{2n}(\mathbb{Q})$ such that B, C are symmetric and A is self-adjoint with respect to the inner product defined by C, and is totally real[1] with eigenvalues of absolute value $< \sqrt{q}$. It turns out that the blocks A, B, C have elegant interpretations: the $\mathrm{GL}_n(\mathbb{Q})$-conjugacy class of A determines the $\overline{\mathbb{Q}}$-isogeny class of (T, F, τ), reflecting the equivalence of conjugacy and stable conjugacy for GL_n. Moreover, the congruence class of C determines the $\mathbb{Q}$-isogeny class of (T, F, τ) within its $\overline{\mathbb{Q}}$-isogeny class (and B is uniquely determined by A, C). The number of isomorphism classes within a $\mathbb{Q}$-isogeny class is given by an orbital integral.

1.5. Our formula differs from that of [36] in that the contribution "at p" is an ordinary orbital integral as opposed to the twisted orbital integral that arises in [36]. In [36] Kottwitz uses a special case of the fundamental lemma to express the twisted integral in terms of (stable) ordinary integrals. In our case we do the reverse: in a second paper ([19]), (which is not restricted to the "ordinary" case) by comparing $\mathbb{Z}_p$-lattices with lattices over the Witt vectors, we show that the contribution "at p" to our formula can also be expressed as a (single) twisted orbital integral, which in turn can be interpreted as counting Dieudonné modules with anti-holomorphic involution.

[1]meaning that its eigenvalues are totally real algebraic integers

1.6. Because we restrict to the "ordinary" case most of the techniques of this paper involve little more than linear algebra. In some sections, for completeness we have provided proofs of results that are known to experts. As a byproduct we obtain an elementary re-proof of the "ordinary" part of the Kottwitz formula (see Theorem 10.2). It is simpler than the general formula because it does not require the Kottwitz invariant $\alpha(\gamma_0;\gamma\delta)$, and does not involve a twisted orbital integral, but we include it because it provides a useful comparison with the formula §10.5 in the "real" case, in which the symplectic group has been replaced by the general linear group.

1.7. Acknowledgments. We wish to thank R. Guralnick for useful conversations about the symplectic group and P. Deligne for his comments on the complex case. We would like to thank the Editor, Don Blasius, and an anonymous referee for their suggestions and help with this paper. We are particularly grateful to the Defense Advanced Research Projects Agency for their support under grant no. HR0011-09-1-0010 and to our program officer at the time, Ben Mann. The first author was also partially supported by the Institute for Advanced Study through a grant from the Simonyi Foundation. An earlier version of this paper (with more details) was posted at [18].

1.8. Notation. If E is an algebraic number field we use $\mathcal{O}_E$ to denote its full ring of integers. Throughout this paper we fix a finite field $k = \mathbb{F}_q$ of characteristic $p > 0$. If R is an integral domain and $n \geq 1$ the *standard symplectic form* $\omega_0 : R^{2n} \times R^{2n} \to R$ is the bilinear map whose matrix is $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$. The general symplectic group, which we denote by $G(R) = \mathrm{GSp}_{2n}(R)$ consists of elements $A \in \mathrm{GL}_{2n}(R)$ such that $\omega_0(Ax, Ay) = \lambda\omega_0(x, y)$ for some $\lambda \in R^\times$ in which case λ is a character, called the *multiplier*. The *standard involution* (see Appendix B) on R^{2n} is the map $\tau_0(x, y) = (-x, y)$. If $g \in G(R)$ we set $\tilde{g} = \tau_0 g \tau_0^{-1}$. The subgroup fixed under this involution is denoted $\mathrm{GL}_n^*(R)$ (cf. §5.4). The finite adèles of $\mathbb{Q}$ is denoted $\mathbb{A}_f$. Let $\mathbb{A}_f^p = \prod'_{v\neq p,\infty} \mathbb{Q}_p$ denote the adèles away from p, let $\widehat{\mathbb{Z}}^p = \prod_{v\neq p,\infty} \mathbb{Z}_v$ so that $\widehat{\mathbb{Z}} = \mathbb{Z}_p.\widehat{\mathbb{Z}}^p$. Let $K_N \subset \mathrm{GSp}_{2n}(\mathbb{Z})$ and $K_N^0 \subset \mathrm{Sp}_{2n}(\mathbb{Z})$ denote the principal congruence subgroups of level N and similarly

$$\widehat{K}_N^0 = \ker\Big(\mathrm{Sp}_{2n}(\widehat{\mathbb{Z}}) \to \mathrm{Sp}_{2n}(\mathbb{Z}/M\mathbb{Z})\Big)$$

$$\widehat{K}_N = \ker\Big(\mathrm{GSp}_{2n}(\widehat{\mathbb{Z}}) \to \mathrm{GSp}_{2n}(\mathbb{Z}/N\mathbb{Z})\Big) = \widehat{K}_N^p K_p \tag{1.8.1}$$

where $\widehat{K}_N^p = \mathrm{GSp}_{2n}(\widehat{\mathbb{Z}}^p) \cap \widehat{K}_N$ and $K_p = \mathrm{GSp}_{2n}(\mathbb{Z}_p)$. If S is a commutative ring with 1 and $\mathcal{C}$ is a $\mathbb{Z}$-linear Abelian category the associated category *up to S-isogeny* ([11, 36]) is the category with the same objects but with morphisms

$$\mathrm{Hom}_S(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B) \otimes_{\mathbb{Z}} S.$$

An S-isogeny is an isomorphism in this category, that is, an invertible element in this set.

2. The complex case

2.1. We briefly recall several aspects of the theory of moduli of real Abelian varieties, which serve as a partial motivation for the results in this paper. Recall that a real structure on a complex Abelian variety A is an anti-holomorphic involution of A. It has been observed [55, 56, 8, 54, 44, 2, 20, 16]

that principally polarized Abelian varieties (of dimension n) with real structure correspond to "real points" of the coarse moduli space

$$Y = \mathrm{Sp}_{2n}(\mathbb{Z})\backslash\mathfrak{h}_n$$

of all principally polarized Abelian varieties, where $\mathfrak{h}_n$ is the Siegel upper halfspace. On this variety, complex conjugation is induced from the mapping on $\mathfrak{h}_n$ that is given by $Z \mapsto \tilde{Z} = -\bar{Z}$ which is in turn induced from the "standard involution" τ_0.

However, a given principally polarized Abelian variety A may admit several non-isomorphic real structures ([55]). Thus, the coarse moduli space of principally polarized Abelian varieties with real structure is not a subset of Y but rather, it maps to Y by a finite mapping. This multiplicity may be removed by replacing Y with the moduli space of principally polarized Abelian varieties with a sufficiently high level structure. More generally let $K_f \subset \mathrm{Sp}_{2n}(\mathbb{A}_f)$ be a compact open subgroup of the finite adèlic points of Sp_{2n} that is preserved by the involution τ_0 and is sufficiently small that $K_f \cap \mathrm{Sp}_{2n}(\mathbb{Q})$ is torsion free. (We use Sp rather than GSp for expository purposes because the argument for GSp is similar but slightly messier.) As in [50], the fixed points of the involution τ_0 on double coset space

$$Y = \mathrm{Sp}_{2n}(\mathbb{Q})\backslash\mathrm{Sp}_{2n}(\mathbb{A})/K_f U(n)$$

are classified by classes[2] in the non-Abelian cohomology $H^1(\langle\tau_0\rangle, K_f)$.

2.2. Proposition. [16] *Conjugation by τ_0 on Sp_{2n} passes to an anti-holomorphic involution $\eta : Y \to Y$ whose fixed point X is isomorphic to the finite disjoint union,*

$$X \;\cong \coprod_{\alpha\in H^1(\langle\tau_0\rangle,K_f)} X_\alpha$$

over cohomology classes α, where

$$X_\alpha = \mathrm{GL}_n(\mathbb{Q})\backslash\,\mathrm{GL}_n(\mathbb{A})/K_\alpha O(n)$$

is an arithmetic quotient of $\mathrm{GL}_n(\mathbb{R})$ and K_α is a certain[3] compact open subgroup of $\mathrm{GL}_n(\mathbb{A}_f)$. If $4|N$ and if $K_f = \widehat{K}^0_N$ is the principal congruence subgroup of $\mathrm{Sp}_{2n}(\widehat{\mathbb{Z}})$ of level N then $K_\alpha = \widehat{K}'_N$ is independent of the cohomology class α, and X may be identified with the parameter space (or coarse moduli space) of principally polarized Abelian varieties with real structure and level N structure. □

In this paper, by restricting to the case of ordinary Abelian varieties, we make a first attempt at finding a finite field analog of Proposition 2.2.

2.3. The Siegel space $\mathfrak{h}_n$ admits another interesting anti-holomorphic involution. In [17] this involution is described on $\mathfrak{h}_2$ whose fixed point set is hyperbolic 3-space (cf. [46]). After appropriate choice of level structure, it passes to an involution of the moduli space Y whose fixed point set is a union of arithmetic hyperbolic 3-manifolds which may be interpreted as constituting a coarse moduli space for Abelian varieties with "anti-holomorphic multiplication" by an order in an imaginary quadratic number field. A finite field analog for this result, along the same lines as the rest of this paper, which applies to the case of ordinary Abelian varieties, is described in §12.

[2]If $x \in \mathrm{Sp}_{2n}(\mathbb{A})$ maps to a fixed point in Y there exists $\gamma \in \mathrm{Sp}_{2n}(\mathbb{Q})$, $k \in K_f$ and $m \in K_\infty$ such that $\tilde{x} = \gamma x k m$, hence $x = \tilde{\gamma}\gamma x k\tilde{k}m\tilde{m}$. Then $k\tilde{k} = I$ since K_f is sufficiently small, so k defines a 1-cocycle.

[3]The class α vanishes in $H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\mathbb{A}_f))$ so there exists $h \in \mathrm{Sp}_{2n}(\mathbb{A}_f)$ such that $\alpha = [h^{-1}\tilde{h}]$. Then $K_\alpha = (h^{-1}K_f h) \cap \mathrm{Sp}_{2n}(\mathbb{A}_f)$ and right translation by h^{-1} maps $\mathrm{GL}_n(\mathbb{Q})\backslash\,\mathrm{GL}_n(\mathbb{A})/O(n).K_\alpha$ to Y.

3. Deligne modules, polarizations and viable elements

3.1. Ordinary Abelian varieties. Throughout this section we fix a finite field $k = \mathbb{F}_q$ of characteristic p. Let A/k be a dimension n Abelian variety. Recall that A is *ordinary* if any of the following equivalent conditions is satisfied.

(1) If $\cdot p : A(\bar{k}) \to A(\bar{k})$ denotes the multiplication by p then its kernel has exactly p^g points.
(2) the local-local component of the p-divisible group $A(p^\infty) = \varprojlim A[p^r]$ is trivial.
(3) The middle coefficient of the characteristic polynomial h_A of the Frobenius endomorphism of A is not divisible by p.
(4) Exactly half of the roots of h_A in $\overline{\mathbb{Q}}_p$ are p-adic units.

3.2. Recall the basic definitions of Deligne [10]. A *Deligne module* of rank $2n$ over the field $k = \mathbb{F}_q$ of q elements is a pair (T, F) where T is a free $\mathbb{Z}$-module of dimension $2n$ and $F : T \to T$ is an endomorphism such that the following conditions are satisfied:

(1) The mapping F is semisimple and all of its eigenvalues in $\mathbb{C}$ have magnitude $\sqrt{q}$.
(2) Exactly half of the eigenvalues of F in $\overline{\mathbb{Q}}_p$ are p-adic units and half of the eigenvalues are divisible by q. (So $\pm\sqrt{q}$ is not an eigenvalue.)
(3) The middle coefficient of the characteristic polynomial of F is coprime to p.
(4) There exists an endomorphism $V : T \to T$ such that $FV = VF = q$.

A morphism $(T, F) \to (T', F')$ of Deligne modules is a group homomorphism $\phi : T \to T'$ such that $F'\phi = \phi F$.

3.3. Let $W(k)$ be the ring of (infinite) Witt vectors over k. In [10] Deligne chooses an an embedding

$$\varepsilon : W(\bar{k}) \to \mathbb{C} \tag{3.3.1}$$

("once and for all") which we henceforth refer to as *Deligne's embedding*. By a theorem of Serre and Tate, [13, 32, 42, 58] the ordinary Abelian variety A has a canonical lift $\bar{A}$ over $W(k)$ which, using (3.3.1) gives rise to a complex variety $A_{\mathbb{C}}$ over $\mathbb{C}$. Let $F \in \mathrm{Gal}(\bar{k}/k)$ denote the Frobenius. The geometric action of F on A lifts to an automorphism F_A on

$$T = T_A = H_1(A_{\mathbb{C}}, \mathbb{Z}).$$

3.4. Theorem. [10] *The association $A \to (T_A, F_A)$, determined by Deligne's embedding (3.3.1), induces an equivalence of categories between the category of n-dimensional ordinary Abelian varieties over $k = \mathbb{F}_q$ and the category of Deligne modules over k of rank $2n$.*

3.5. Endomorphism algebra and CM types. If A is an ordinary Abelian variety over the finite field $k = \mathbb{F}_q$ of characteristic p, then A is $\mathbb{Q}$-isogenenous $A \sim A_1 \times A_2 \times \cdots \times A_r$ to a product of ordinary Abelian varieties over k such that

(1) For $1 \le i \le r$ there exists a positive integer d_i and a simple ordinary Abelian variety B_i over k and a $\mathbb{Q}$-isogeny $A_i \sim B_i^{d_i}$
(2) $\mathrm{Hom}_{\mathbb{Q}}(B_i, B_j) = 0$ for $i \ne j$.

The endomorphism algebra $K_i = \mathrm{End}_{\mathbb{Q}}(B_i)$ is a CM field (that is, an imaginary quadratic extension of a maximal totally real subfield L_i) of degree $[K_i : \mathbb{Q}] = 2\dim(B_i)$. It is the center of the algebra

$\mathrm{End}_{\mathbb{Q}}(A_i) \cong M_{d_i \times d_i}(K_i)$. The center of $\mathrm{End}_{\mathbb{Q}}(A)$ is therefore isomorphic to the CM algebra (that is, the product of CM fields) $K = K_1 \times \cdots \times K_r$.

A CM type Φ_i on K_i is a collection of embeddings $\phi : K_i \to \mathbb{C}$, one from each complex conjugate pair. It induces a real vector space isomorphism

$$\prod_{\phi \in \Phi_i} : K_i \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}^{[K_i:\mathbb{Q}]/2}$$

which defines a complex structure on $K_i \otimes_{\mathbb{Q}} \mathbb{R}$. A CM type on K is a collection of nontrivial homomorphism $\phi : K \to \mathbb{C}$, one from each complex conjugate pair, or equivalently, it is a choice of CM type for each K_i. Using Theorem 3.4 these statements become the following.

If (T, F) is the Deligne module corresponding to A then there is a decomposition

$$T_{\mathbb{Q}} = T \otimes_{\mathbb{Z}} \mathbb{Q} \cong T_{1,\mathbb{Q}} \oplus \cdots \oplus T_{r,\mathbb{Q}},$$

preserved by F, say $F = F_1 \oplus \cdots \oplus F_r$, and an isomorphism $\mathbb{Q}[F] \cong K_1 \times \cdots K_r$ of the center of $\mathrm{End}_{\mathbb{Q}}(T, F) = \mathrm{End}_F(T \otimes \mathbb{Q})$ with the CM algebra K. Then $T_{i,\mathbb{Q}}$ is a vector space of dimension d_i over the CM field $K_i = \mathbb{Q}[F_i]$. A CM type for $\mathbb{Q}[F]$ defines a complex structure on $T \otimes \mathbb{R}$. The minimum polynomial of (T, F) is the product of the minimum polynomials $h_i(x)$ of the $(T_{i,\mathbb{Q}}, F_i)$. It is an ordinary Weil q-polynomial (see §A.1).

Deligne's embedding $\varepsilon : W(\bar{k}) \to \mathbb{C}$ induces a valuation val_p on $\overline{\mathbb{Q}} \subset \mathbb{C}$ extending the p-adic valuation of $W(k)$ (which explains the use of $W(\bar{k})$ rather than $W(k)$). This determines a canonical CM type for every Deligne module (and every CM algebra), which we refer to as *Deligne's CM type* as follows. If (T, F) is a Deligne module, define

$$\Phi_\varepsilon = \{\phi : \mathbb{Q}[F] \to \mathbb{C} \mid \mathrm{val}_p(\phi(F)) > 0\}. \tag{3.5.1}$$

Then Φ_ε is a CM type for the CM algebra $\mathbb{Q}[F]$. The resulting complex structure on $T \otimes_{\mathbb{Z}} \mathbb{R}$ is the unique complex structure such that the action of F is complex linear and so that $\mathrm{val}_p(\alpha) > 0$ for every eigenvalue α of F (see [10] p. 242). It agrees with the complex structure on $T_0 A_{\mathbb{C}}$ in the case when $(T, F) = (T_A, F_A)$ is the Deligne module associated to an ordinary Abelian variety A. The complex structure gives a Hodge structure on $T_0 A_{\mathbb{C}}$ which corresponds to an $\mathbb{R}$ homomorphism $\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \to \mathrm{GL}(T \otimes \mathbb{R})$.

3.6. Let (T, F) be a Deligne module. We are grateful to the referee for pointing out that not every CM type on $\mathbb{Q}[F]$ will arise as $\Phi_{\varepsilon'}$ for different embeddings $\varepsilon' : W(\bar{k}) \to \mathbb{C}$. Suppose as above that $K = \mathbb{Q}[F] \cong K_1 \times \cdots \times K_r$ is a decomposition into a product of CM fields, with the corresponding decomposition $L = L_1 \times \cdots L_r$ of maximal totally real subfields. Each p-adic place of L_i splits in K_i but the prime p may ramify in L_i. A CM type arising from an embedding $\epsilon' : W(\bar{k}) \to \mathbb{C}$ will correspond to a choice, for each i and for each p-adic place in L_i, of one of the two places in K_i over it. Let us say that such a CM type is *eligible*. Thus the total number of eligible CM types for $\mathbb{Q}[F]$ is 2^s where s is the number of p-adic places of $L_1 \times \cdots \times L_r$ (whereas the full number of CM types is 2^t where $t = \sum_i [L_i : \mathbb{Q}]$).

For Howe's theorem (§3.9 below) and all of §6 through §10 we consider only eligible CM types on $\mathbb{Q}[F]$, and in fact, we use only Deligne's CM type Φ_ϵ. For Howe's theorem, this is crucial. However the results in §6 through §9 are "linear algebra" statements that can be extended in a straight forward manner to include arbitrary CM types using §3.8 and Lemma 3.10(b),(c).

3.7. Polarizations. For a complex n dimensional Abelian variety X a polarization may be considered to be a Hermitian form $H = R + i\omega$ defined on the (complex n dimensional) tangent space T_0X, meaning that ω is a (real valued) symplectic form on the underlying real vector space $(T_0X)_{\mathbb{R}}$ such that the inner product

$$R(x, y) = \omega(x, \sqrt{-1}.y)$$

is symmetric and positive definite. In [24], E. Howe defines the notion of a polarization of a Deligne module (T, F) in a similar way but the "positive definite" condition requires a replacement for the notion of multiplication by $\sqrt{-1}$.

If Φ is any CM type on $\mathbb{Q}[F]$ we will say (following [24]) that an element $\iota \in \mathbb{Q}[F]$ is Φ-totally positive imaginary if $\phi(\iota)$ is a positive multiple of $\sqrt{-1}$ for all $\phi \in \Phi$. A polarization ω of the Deligne module (T, F) that is *positive with respect to the CM type* Φ is defined to be an alternating bilinear form $\omega : T \times T \to \mathbb{Z}$ such that

(0) $\omega(x, y) = -\omega(y, x)$ for all $x, y \in T$,
(1) $\omega : T_{\mathbb{Q}} \times T_{\mathbb{Q}} \to \mathbb{Q}$ is nondegenerate,
(2) $\omega(Fx, y) = \omega(x, Vy)$ for all $x, y \in T$,

as well as the following Φ-*positivity condition* (see §3.11)

(*) the bilinear form $R(x, y) = \omega(x, \iota y)$ is symmetric and positive definite, for some (and hence any) totally Φ-positive imaginary element $\iota \in \mathbb{Q}[F]$,

and we say that (T, F, ω) is *a Φ-positively polarized Deligne module*. (See also §3.11.)

Let us say that a symplectic form ω on a Deligne module (T, F) satisfying (1) and (2) above is a *polarization* if there exists a CM type Φ on $\mathbb{Q}[F]$ such that ω is a Φ-positive polarization on (T, F). (Most of this paper involves Deligne modules that are positively polarized with respect to Deligne's CM type Φ_ε.)

3.8. Suppose (T_1, F_1, ω_1) is Φ_1-positively polarized and (T_2, F_2, ω_2) is Φ_2-positively polarized, where Φ_1, Φ_2 are CM types on $\mathbb{Q}[F_1]$, $\mathbb{Q}[F_2]$ respectively. If $g : (T_1, F_1) \to (T_2, F_2)$ is a morphism of Deligne modules that is compatible with the polarizations (meaning that $g^*(\omega_2) = \omega_1$) then it also follows that $g^*(\Phi_2) = \Phi_1$. Therefore we may speak of a morphism of polarized Deligne modules without necessarily referring to the CM type. (See also Lemma 3.10).

Let S be a commutative ring with 1. An S-isogeny of Φ-positively polarized Deligne modules $\phi : (T_1, F_1, \omega_1) \to (T_2, F_2, \omega_2)$ is defined to be an S-isogeny (cf. §1.8) $\phi : (T_1, F_1) \to (T_2, F_2)$ for which there exists $c \in S^\times$ such that $\phi^*(\omega_2) = c\omega_1$, in which case c is called the *multiplier* of the isogeny ϕ. If $S \subset \mathbb{R}$ then any S-isogeny of Φ-positively polarized Deligne modules has positive multiplier.

3.9. Howe's theorem. If (T, F) is a Deligne module then the *dual* Deligne module $(\widehat{T}, \widehat{F})$ is defined by $\widehat{T} = \mathrm{Hom}(T, \mathbb{Z})$ and $\widehat{F}(\phi)(x) = \phi(Vx)$ for all $\phi \in \widehat{T}$.

Let A be an ordinary Abelian variety with associated Deligne module (T_A, F_A) that is determined by the embedding ε of (3.3.1). Then there is a canonical isomorphism of Deligne modules, $(\widehat{T}_A, \widehat{F}_A) \cong (T_{\widehat{A}}, F_{\widehat{A}})$. Let $\omega : T_A \times T_A \to \mathbb{Z}$ be an alternating bilinear form that satisfies conditions (1) and (2) of §3.7. It induces an isomorphism $\lambda : (T_A \otimes \mathbb{Q}, F) \to (\widehat{T}_A \otimes \mathbb{Q}, \widehat{F})$ and hence an isogeny $\lambda_A : A \to \widehat{A}$. Then Howe proves ([24]) that ω is positive *with respect to the CM type* Φ_ε if and

only if λ_A is a polarization of the Abelian variety A. Consequently, *the equivalence of categories in Theorem 3.4 (which depends on the choice of ε) extends to an equivalence between the category of polarized n-dimensional Abelian varieties over $\mathbb{F}_q$ with the category of Φ_ε-positively polarized Deligne modules (over $\mathbb{F}_q$) of rank $2n$.*

3.10. Existence Lemma. (see also Lemma 4.4.)
(a) *Let $K = \mathbb{Q}[\pi]$ be a CM field and let Φ be a CM type for K. Then there exists an integral symplectic form $\omega : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}$ which satisfies the Φ-positivity condition (*) of §3.7, that is, the bilinear form $R(x,y) = \omega(x, \iota y)$ is positive definite and symmetric, for any Φ-totally positive imaginary element $\iota \in K$. The form ω may be chosen so that $\omega(ax, y) = \omega(x, \bar{a}y)$ for any $a \in K$ (where bar denotes complex conjugation), hence $\omega(\bar{x}, \bar{y}) = -\omega(x,y)$. If π is an ordinary Weil q-number*[4] *then $(\mathcal{O}_K, \pi, \omega)$ is a Φ-positively polarized Deligne module.*
(b) *Let (T,F) be a Deligne module. For any CM type Φ on $\mathbb{Q}[F]$ there exists a Φ-positive polarization ω of (T,F), hence (T,F,ω) is a Φ-positively polarized Deligne module.*
(c) *Suppose (T,F) is a Deligne module and suppose $\omega : T \times T \to \mathbb{Z}$ is a symplectic form such that $\omega(Fx, y) = \omega(x, Vy)$. Then there exists a unique CM type Φ on $\mathbb{Q}[F]$ such that ω is Φ-positive, hence (T,F,ω) is a Φ-positively polarized Deligne module.*

Proof. A polarization that is positive with respect to Φ and compatible with complex conjugation is described in [53] §6.2 and [52] §6.2; see also [43] Prop. 10.2 p. 335; we repeat the definition here. Let $\alpha \in \mathcal{O}_K$ be totally Φ-positive imaginary and for all $x, y \in K$ set

$$\omega_K(x,y) = \mathrm{Trace}_{K/\mathbb{Q}}(\alpha x.\overline{y}).$$

Then $\omega_K : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}$ is antisymmetric, the bilinear form $R(x,y) = \omega_K(x, \alpha y)$ is symmetric and positive definite, $\omega_K(\pi x, \pi y) = q\omega_K(x,y)$, and $\omega_K(\bar{x}, \bar{y}) = -\omega_K(x,y)$.

Part (b) follows from part (a) by decomposition into simple Deligne modules.

For part (c) we may also suppose (T,F) is $\mathbb{Q}$-simple and $\omega : T \times T \to \mathbb{Z}$ is alternating and nondegenerate over $\mathbb{Q}$ with $\omega(Fx,y) = \omega(x, Vy)$. A choice of a F-cyclic vector gives an isomorphism of $\mathbb{Q}[F]$-modules, $T \otimes \mathbb{Q} \cong \mathbb{Q}[F]$. Using this isomorphism, the mapping $x \mapsto \omega(x,1)$ is $\mathbb{Q}$-linear, so is given by $\mathrm{Trace}_{K/\mathbb{Q}}(\alpha x)$ for some uniquely deteremined $\alpha \in K$. It follows that $\bar{\alpha} = -\alpha$ and

$$\omega(x,y) = \mathrm{Trace}_{K/\mathbb{Q}}(\alpha x \bar{y}).$$

This element α determines a CM type $\Phi = \Phi_\alpha$ for K: for any embedding $K \to \mathbb{C}$ the image of α is purely imaginary so there is a unique choice ϕ from each pair of complex conjugate embeddings such that $\phi(\alpha)$ is positive imaginary. It is easy to check that ω is Φ_α-positive. For uniqueness, if $\beta \in \mathbb{Q}[F]$ is any other element such that $(x,y) \to \omega(x, \beta y)$ is symmetric and positive definite then $\bar{\beta} = -\beta$ so $\phi(\beta)$ is purely imaginary for every $\phi \in \Phi_\alpha$. Moreover,

$$\omega(x, \beta x) = \sum_{\phi \in \Phi_\alpha} \phi(\alpha\bar{\beta}x\bar{x}) + \overline{\phi}(\alpha\bar{\beta}x\bar{x}) = 2\sum_{\phi \in \Phi_\alpha} \phi(\alpha\bar{\beta}x\bar{x}) > 0$$

for all $x \in \mathbb{Q}[F]^\times$. This implies that $\phi(\alpha)\phi(\bar{\beta}) = -\phi(\alpha)\phi(\beta) > 0$ for each $\phi \in \Phi_\alpha$, hence $\phi(\beta)$ is also positive imaginary, that is, $\Phi_\alpha = \Phi_\beta$. □

[4] meaning that $\mathbb{Q}[\pi]$ has no real embeddings, that $\phi(\pi)\bar{\phi}(\pi) = q$ for each complex embedding $\phi : \mathbb{Q}[\pi] \to \mathbb{C}$, and that the middle coefficient of the characteristic polynomial of π is not divisible by p, cf. Appendix A.

3.11. Viable elements. Let $\gamma_0 \in \mathrm{GSp}_{2n}(\mathbb{Q})$ be a semisimple element whose characteristic polynomial is an ordinary Weil q-polynomial. If $\gamma, \gamma_0 \in \mathrm{GSp}_{2n}(\mathbb{Q})$ are stably conjugate[5] then conjugation defines a unique isomorphism $\mathbb{Q}[\gamma] \cong \mathbb{Q}[\gamma_0]$. Let $\mathcal{C} \subset \mathrm{GSp}_{2n}(\mathbb{Q})$ be the stable conjugacy class of γ_0 let Φ be a CM type on the CM algebra $K = K(\mathcal{C}) = \mathbb{Q}[\gamma_0]$. An element $\gamma \in \mathcal{C}$ will be said to be Φ-*viable* if the pair (γ, ω_0) satisfies the following positivity condition (where ω_0 is the standard symplectic form on $\mathbb{Q}^{2n}$):

(**) The bilinear form $R(x, y) = \omega_0(x, \iota y)$ is symmetric and positive definite on $\mathbb{Q}^{2n}$, for any totally Φ-positive imaginary element $\iota \in \mathbb{Q}[\gamma]$

3.12. Proposition. (See also Lemma 4.4.) *Let $\mathcal{C} \subset \mathrm{GSp}_{2n}(\mathbb{Q})$ be a stable conjugacy class of semisimple elements whose characteristic polynomial is an ordinary Weil q polynomial and let Φ be a CM type on the associated CM algebra $K = K(\mathcal{C})$.*

(1) An element $\gamma \in \mathcal{C}$ is Φ-viable if and only if there exists a Φ-positively polarized Deligne module of the form (L, γ, ω_0) for some lattice $L \subset \mathbb{Q}^{2n}$.
(2) the set of Φ-viable elements in $\mathcal{C}$ is non empty and forms a unique $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugacy class[6] within $\mathcal{C}$.

Proof. For part (1), given a Φ-viable element $\gamma \in \mathcal{C}$ we may reduce to the case that the characteristic polynomial of γ is irreducible and $K = \mathbb{Q}[\gamma]$ is a CM field. We need to construct a lattice $L \subset \mathbb{Q}^{2n}$ which is preserved by γ and by $q\gamma^{-1}$, such that the symplectic form ω_0 take integer values on L.

Let $v_0 \in \mathbb{Q}^{2n}$ be a cyclic vector for the action of γ, that is, a generator of $\mathbb{Q}^{2n}$ as a one dimensional $K = \mathbb{Q}[\gamma]$ module and let $\psi : K \to \mathbb{Q}^{2n}$ be the unique K-equivariant mapping such that $\psi(1) = v_0$.

Let $\omega_K = \psi^*(\omega_0)$. Then $\omega_K(x, 1)$ is linear in x so it is given by $\mathrm{Trace}_{K/\mathbb{Q}}(\alpha x)$ for some unique element $\alpha \in K$. It follows that $\omega_K(x, y) = \mathrm{Trace}_{K/\mathbb{Q}}(\alpha x \bar{y})$, that $\bar{\alpha} = -\alpha$ and that α is totally Φ-positive imaginary. If we change v_0 to $x.v_0$ (with $x \in \mathbb{Q}[\gamma]$) then α changes to $x\bar{x}\alpha$. It follows that we may choose v_0 so that $\alpha \in K$ is an algebraic integer. Therefore multiplication by α preserves $\mathcal{O}_K$ so ω_K is integer valued on $\mathcal{O}_K$. Hence, we may take $L = \psi(\mathcal{O}_K)$.

For part(2), by Lemma 3.10(c), there exist a Φ-viable element $\gamma_0 \in \mathcal{C}$, and there exists a Φ-positively polarized Deligne module of the form $(L_0, \gamma_0, \omega_0)$ (where $L_0 \subset \mathbb{Q}^{2n}$). Now let $\gamma \in \mathcal{C}$. We must show that γ is Φ-viable iff it is $\mathrm{Sp}_{2n}(\mathbb{R})$ conjugate to γ_0.

First, suppose that γ is Φ-viable, hence (L, γ, ω_0) is a Φ-positively polarized Deligne module, for some lattice $L \subset \mathbb{Q}^{2n}$. Since γ, γ_0 have the same characteristic polynomial, there exists $\phi \in \mathrm{GL}_{2n}(\mathbb{Q})$ with $\gamma_0 = \phi^{-1}\gamma\phi$ which therefore induces an identification $\mathbb{Q}[\gamma] \cong \mathbb{Q}[\gamma_0]$. So $(\phi^{-1}(L), \phi^*(\gamma) = \gamma_0, \phi^*(\omega_0))$ is a Φ-positively polarized Deligne module. Choose $c \in \mathbb{Q}$, $c > 0$ so that $c\phi^*(\omega_0)$ takes integer values on L_0. Then $c\phi^*(\omega_0)$ is a second polarization of the Deligne module (L_0, γ_0). By Lemma C.1 there is an $\mathbb{R}$-isogeny $\psi : (L_0, \gamma_0, \omega_0) \to (L_0, \gamma_0, c\phi^*(\omega_0))$ with multiplier equal to 1, which implies that $\psi^*\phi^*(c\omega_0) = \omega_0$. Thus, conjugation by $\phi \circ \psi$ takes γ_0 to γ, and $\phi \circ \psi \in \mathrm{GSp}_{2n}(\mathbb{R})$ has multiplier $c > 0$. Therefore conjugation by $\frac{1}{\sqrt{c}}\phi \circ \psi \in \mathrm{Sp}_{2n}(\mathbb{R})$ also takes γ_0 to γ. The converse is similar (but easier). □

[5]meaning that there exists $g \in \mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ such that $\gamma = g^{-1}\gamma_0 g$

[6]meaning the intersection of an $\mathrm{Sp}_{2n}(\mathbb{R})$ conjugacy class with $\mathcal{C}$

4. Real structures

4.1. Definition. Fix a Deligne module (T, F) over $k = \mathbb{F}_q$ of dimension $2n$. A *real structure* on (T, F) is a $\mathbb{Z}$-linear homomorphism $\tau : T \to T$ such that $\tau^2 = I$ and such that $\tau F \tau^{-1} = V$. A (real) morphism $\phi : (T, F, \tau) \to (T', F', \tau')$ of Deligne modules with real structures is a group homomorphism $\phi : T \to T'$ so that $\phi F = F'\phi$ and $\phi\tau = \tau'\phi$. A real structure τ is compatible with a polarization $\omega : T \times T \to \mathbb{Z}$ if, for all $x, y \in T$,

$$\omega(\tau x, \tau y) = -\omega(x, y). \tag{4.1.1}$$

Let $N \geq 1$ and assume $p \nmid N$. A *(principal) level N structure* on (T, F) is an isomorphism $\beta : T/NT \to (\mathbb{Z}/N\mathbb{Z})^{2n}$ such that $\beta \circ \overline{F} = \beta$ where $\overline{F} = F \pmod N$. (If a level N structure exists, it implies that $F \equiv I \pmod N$, which places further restrictions on N.) A level N structure is said to be compatible with a polarization $\omega : T \times T \to \mathbb{Z}$ if $\beta_*(\omega) = \bar{\omega}_0$ is the reduction modulo N of the standard symplectic form (cf. §1.8).

If (T, F, τ) is a Deligne module with real structure then a level N structure β on (T, F) is *compatible with* τ if $\beta_*(\tau) = \bar{\tau}_0$ is the reduction modulo N of the standard involution (cf. §1.8 and §D.3). A necessary condition for the existence of a level N structure that is compatible with τ is that $p \equiv 1 \pmod N$, which also implies that $V \equiv I \pmod N$, cf. §5.1.

4.2. In Theorem 7.1 we will prove (for q, N coprime) that there are finitely many isomorphism classes of principally (Φ_ε-positively) polarized Deligne modules of rank $2n$ over $\mathbb{F}_q$ with real structure and with principal level N structure. In §11.1 we add a few remarks concerning the fixed point lattice T^τ (or "real sublattice") of a Deligne module (T, F) with real structure τ.

4.3. Lemma. *The category of Deligne modules (resp. polarized Deligne modules) with real structure, up to $\mathbb{Q}$-isogeny is semisimple. If (T, F, τ) is $\mathbb{Q}$-simple then either (a) $T_\mathbb{Q} = T \otimes \mathbb{Q}$ is a simple $\mathbb{Q}[F]$ module or (b) there exists a simple $\mathbb{Q}[F]$ module W so that $T_\mathbb{Q} \cong W \oplus \tau(W)$.*

Proof. The proof is more or less standard. For the first statement, it suffices to check complete reducibility. Let (T, F, τ) be a Deligne module, and let (T_1, F, τ) be a submodule. Since F is semisimple the ring $\mathbb{Q}[F]$ is isomorphic to a product of number fields. It follows that (T, F, τ) decomposes into a sum of modules over these constituent fields. So we may assume that $\mathbb{Q}[F]$ is a field. Set $W = T \otimes \mathbb{Q}$ and let $W_1 = T_1 \otimes \mathbb{Q}$. Choose any decomposition of W into simple $\mathbb{Q}[F]$-submodules so that W_1 is a summand. The resulting projection $\pi : W \to W_1$ is $\mathbb{Q}[F]$-equivariant. Let $e = \pi + \tau\pi\tau : W \to W_1$. Then e is surjective (since its restriction to W_1 coincides with multiplication by 2) and $W_1' := \ker(e)$ is preserved by F and by τ. Thus, the decomposition $W = W_1 \oplus W_1'$ is preserved by F and by τ. For any choice of lattice $T_1' \subset W_1'$ preserved by F and τ the module $(T_1 \oplus T_1', F, \tau)$ is $\mathbb{Q}$-isogenous to (T, F, τ). The statement about simple modules follows.

Similarly suppose (T, F, ω, τ) is a Deligne module with real structure and Φ-positive polarization with respect to a choice Φ of CM type on $\mathbb{Q}[F]$. Let $W = T \otimes \mathbb{Q}$ and suppose that $W_1 \subset W$ is a subspace preserved by F and by τ. Set $F_1 = F|W_1$. It follows that

(1) the restriction of ω to W_1 is nondegenerate and is Φ_1-positive, where Φ_1 is the CM type on $\mathbb{Q}[F_1]$ that is induced from Φ,

(2) the subspace $W_2 = \{y \in W |\ \omega(w, y) = 0 \text{ for all } w \in W_1\}$ is also preserved by F and by τ and it is Φ_2-positively polarized by the restriction $\omega|W_2$ where Φ_2 is the CM type induced from Φ on $\mathbb{Q}[F_2]$ (where $F_2 = F|W_2$), and
(3) The module W decomposes as an orthogonal sum $W = W_1 \oplus W_2$. □

4.4. Existence Lemma. *The Φ-positively polarized Deligne module $(\mathcal{O}_K, \pi, \omega)$ defined in part (a) of Lemma 3.10 admits a canonical real structure given by complex conjugation. Statement (b) of Lemma 3.10 remains true if the Deligne module (T, F) is replaced by a Deligne module with real structure (T, F, τ), in which case the resulting polarization ω is compatible with the real structure. Statement (c) remains true if the Deligne module (T, F) has a real structure.*

Let $\mathcal{C} \subset \mathrm{GSp}_{2n}(\mathbb{Q})$ be a stable conjugacy class as in Proposition 3.12, and let Φ be a CM type on the CM algebra $K = K(\mathcal{C})$. Let $\gamma \in \mathcal{C}$ be Φ-viable and also q-inversive (see §5 below). Then there exists a lattice $L \subset \mathbb{Q}^{2n}$ that is preserved by γ, $q\gamma^{-1}$, and by the standard involution τ_0 so that $(L, \gamma, \omega_0, \tau_0)$ is a Φ-positively polarized Deligne module with real structure.

Proof. The first three statements are easy to verify. The last statement follows from the same proof as that of Lemma 3.10 and Proposition 3.12, using Lemma 4.3 to reduce to the simple case. □

5. q-inversive elements

5.1. Let R be an integral domain. Let us say that an element $\gamma \in \mathrm{GSp}_{2n}(R)$ is *q-inversive* if it is semisimple, has multiplier q and if[7]

$$\tau_0 \gamma \tau_0^{-1} = q\gamma^{-1},$$

or equivalently if $\gamma = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right) \in \mathrm{GSp}_{2n}(R)$ and B, C are symmetric, and $A^2 - BC = qI$. It follows that $B\,{}^tA = AB$ and $CA = {}^tAC$. In Lemma 6.3 below, it is explained that the endomorphism F of a polarized Deligne module with real structure may be represented by a q-inversive element.

5.2. Lemma. *Let $\gamma = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right) \in \mathrm{GSp}_{2n}(\mathbb{Q})$ be q-inversive. Then the following statements are equivalent.*

(1) The matrices A, B, and C are nonsingular.
(2) The element γ has no eigenvalues in the set $\{\pm\sqrt{q}, \pm\sqrt{-q}\}$.

If these properties hold then the matrix A is semisimple, and the characteristic polynomial of A is $h(2x)$, where $h(x)$ is the real counterpart (see §A.2) to $g(x)$, the characteristic polynomial of γ. If $g(x)$ is also an ordinary Weil q-polynomial then $p \nmid \det(A)$ and every eigenvalue β of A satisfies

$$|\beta| < \sqrt{q}. \tag{5.2.1}$$

Conversely, let $A \in \mathrm{GL}_n(\mathbb{Q})$ be semisimple and suppose that its eigenvalues $\beta_1, \cdots, \beta_n$ (not necessarily distinct) are totally real and that $|\beta_r| < \sqrt{q}$ for $1 \le r \le n$. Then for any symmetric nonsingular matrix $C \in \mathrm{GL}_n(\mathbb{Q})$ such that ${}^tAC = CA$, the following element

$$\gamma = \begin{pmatrix} A & (A^2 - qI)C^{-1} \\ C & {}^tA \end{pmatrix} \in \mathrm{GSp}_{2n}(\mathbb{Q}) \tag{5.2.2}$$

[7]Compare the equation $\tau F \tau^{-1} = V$ of §4.1

is q-inversive and its eigenvalues are the Weil q-numbers:

$$\alpha_r = \beta_r \pm \sqrt{\beta_r^2 - q} \quad (1 \leq r \leq n), \tag{5.2.3}$$

Proof. These statements are direct consequences of the following observation: if $w = \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ is an eigenvector of γ with eigenvalue λ then

(a) $\tau_0(w) = \left(\begin{smallmatrix} -u \\ v \end{smallmatrix}\right)$ is an eigenvector of γ with eigenvalue q/λ
(b) u is an eigenvector of A with eigenvalue $\frac{1}{2}\left(\lambda + \frac{q}{\lambda}\right)$
(c) v is an eigenvector of ${}^tA$ with eigenvalue $\frac{1}{2}\left(\lambda + \frac{q}{\lambda}\right)$. □

5.3. Joint signature. Let $E_n(\mathbb{R})$ denote the set of pairs (A, C) where $A \in \mathrm{GL}_n(\mathbb{R})$ is semisimple with all eigenvalues real, where $C \in \mathrm{GL}_n(\mathbb{R})$ is symmetric, and where A is self adjoint with respect to the inner product $\langle \cdot, \cdot \rangle_C$ defined by C, that is, ${}^tAC = CA$. If $\beta \neq \mu$ are eigenvalues of A then the eigenspaces V_β and V_μ are orthogonal with respect to $\langle \cdot, \cdot \rangle_C$. Therefore $\langle \cdot, \cdot \rangle_C$ decomposes as a direct sum of bilinear forms $\oplus_{\beta \in \mathrm{Spec}(A)} \langle \cdot, \cdot \rangle_\beta$ with respect to the eigenspace decomposition $\mathbb{R}^n = \oplus_{\beta \in \mathrm{Spec}(A)} V_\beta$ where $\mathrm{Spec}(A) \subset \mathbb{R}$ denotes the spectrum of A. Define

$$\mathrm{sig}(A; C) = \{\mathrm{sig}\ \langle \cdot, \cdot \rangle_\beta\}_{\beta \in \mathrm{Spec}(A)}$$

to be the ordered collection of signatures of each of these bilinear forms. The elements of $\mathrm{sig}(A; C)$ correspond to class in the Galois cohomology set $H^1(\mathbb{C}/\mathbb{R}, Z_A \cap O(C))$ of the centralizer of A intersected with the orthogonal group of C.

The group $\mathrm{GL}_n(\mathbb{R})$ acts on $E_n(\mathbb{R})$ by

$$X.(A, C) = (XAX^{-1},\ {}^tX^{-1}CX^{-1}).$$

Two elements (A, C) and (A', C') are in the same orbit if and only if A, A' have the same characteristic polynomial and $\mathrm{sig}(A, C) = \mathrm{sig}(A', C')$. In fact, the stabilizer of A in $\mathrm{GL}_n(\mathbb{R})$ is $\prod_{\beta \in \mathrm{Spec}(A)} \mathrm{GL}(V_\beta)$ and within each V_β the congruence class[8] of C_β is determined by the signature of $\langle \cdot, \cdot \rangle_\beta$.

5.4. Conjugacy of q-inversive elements. In this section we consider GL_n versus Sp_{2n} conjugacy of q-inversive elements. Let $L \supset \mathbb{Q}$ be a field. The subgroup of $\mathrm{GSp}_{2n}(L)$ that is fixed under conjugation by the standard involution τ_0 is denoted $\mathrm{GL}_n^*(L)$, and it is the image of the *standard embedding*

$$\delta : L^\times \times \mathrm{GL}_n(L) \to \mathrm{GSp}_{2n}(L); \quad \delta(\lambda, x) = \begin{pmatrix} \lambda X & 0 \\ 0 & {}^tX^{-1} \end{pmatrix}.$$

(For $\lambda = 1$ we use the same notation $\delta : \mathrm{GL}_n \to \mathrm{Sp}_{2n}$.) Say that two elements of GSp_{2n} are GL_n^* (resp. GL_n)-conjugate if the conjugating element lies in the image of δ (resp. $\delta(1 \times \mathrm{GL}_n)$). Then GL_n^*-conjugation preserves q-inversive elements.

[8]Symmetric matrices S and T are *congruent* if there exists a matrix X so that $T = XS\,{}^tX$.

5.5. Proposition. *Let $\gamma_1, \gamma_2 \in \mathrm{GSp}_{2n}(\mathbb{Q})$ be q-inversive, say $\gamma_i = \left(\begin{smallmatrix} A_i & B_i \\ C_i & {}^tA_i \end{smallmatrix}\right)$. Then*

$$\begin{aligned}
&\gamma_1, \gamma_2 \text{ are } \mathrm{GSp}_{2n}(\overline{\mathbb{Q}})\text{-conjugate} &&\iff A_1, A_2 \text{ are } \mathrm{GL}_n(\mathbb{Q})\text{-conjugate}\\
&&&\iff \gamma_1, \gamma_2 \text{ are } \mathrm{GL}_n(\overline{\mathbb{Q}})\text{-conjugate}\\
&\gamma_1, \gamma_2 \text{ are } \mathrm{Sp}_{2n}(\mathbb{R})\text{-conjugate} &&\iff \gamma_1, \gamma_2 \text{ are } \mathrm{GL}_n(\mathbb{R})\text{-conjugate}\\
&&&\iff A_1, A_2 \text{ are } \mathrm{GL}_n(\mathbb{Q})\text{-conjugate and}\\
&&&\quad \mathrm{sig}(A_1; C_1) = \mathrm{sig}(A_2; C_2).
\end{aligned}$$

Proof. Conjugacy by $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ is the same as conjugacy by $\mathrm{Sp}_{2n}(\overline{\mathbb{Q}})$ and, among semisimple elements, is determined by the characteristic polynomial. From Lemma 5.2 the characteristic polynomial of γ_i determines that of A_i and vice versa. Conjugacy of semisimple rational matrices A_1, A_2 is determined by the characteristic polynomial. The proves the first statement. Using $\mathrm{GL}_n(\overline{\mathbb{Q}})$ it is possible to diagonalize A_i and to reduce C_i to the identity, which proves the second statement.

For the third implication ($\Longleftarrow$), equality of the signatures guarantees the existence of $X \in \mathrm{GL}_n(\mathbb{R})$ so that $X.(A_1, C_1) = (A_2, C_2) \in E_n(\mathbb{R})$ as explained in §5.3. Then γ_1, γ_2 are conjugate by $\left(\begin{smallmatrix} X & 0 \\ 0 & {}^tX^{-1} \end{smallmatrix}\right) \in \mathrm{Sp}_{2n}(\mathbb{R})$.

Now suppose that γ_1, γ_2 are $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugate. Then A_1, A_2 are $\mathrm{GL}_n(\mathbb{Q})$-conjugate since they have the same characteristic polynomial, so we need to show that $\mathrm{sig}(A_1; C_1) = \mathrm{sig}(A_2; C_2)$ or equivalently, that γ_1, γ_2 are conjugate by an element of $\delta(\mathrm{GL}_n(\mathbb{R}))$. As in §5.3, conjugating by elements of $\delta(\mathrm{GL}_n(\mathbb{R}))$ and by decomposing with respect to the eigenspace decompositions of A_1, A_2, we may reduce to the case that $A_1 = A_2 = \lambda I_n$, and that C_1, C_2 are diagonal matrices consisting of ± 1.

So, let us assume that $C_1 = I_r$ consists of r copies of $+1$ and $n - r$ copies of -1 along the diagonal, and that $C_2 = I_s$. This determines $B_1 = dI_r$ and $B_2 = dI_s$ where $d = \lambda^2 - q$. Assuming that γ_1, γ_2 are $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugate, we need to prove that $r = s$.

Suppose $h = \left(\begin{smallmatrix} X & Y \\ Z & W \end{smallmatrix}\right) \in \mathrm{Sp}_{2n}(\mathbb{R})$ and $\gamma_2 = h\gamma_1 h^{-1}$. Subtracting $\lambda I_{2n\times 2n}$ from both sides of this equation leaves

$$\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} \begin{pmatrix} 0 & dI_r \\ I_r & 0 \end{pmatrix} = \begin{pmatrix} 0 & dI_s \\ I_s & 0 \end{pmatrix} \begin{pmatrix} X & Y \\ Z & W \end{pmatrix} \tag{5.5.1}$$

or $W = I_s X I_r$ and $Z = d^{-1} I_s Y I_r$. Let $H = X + \frac{1}{\sqrt{d}} Y I_r \in \mathrm{GL}_{2n}(\mathbb{C})$. Then

$$H I_r\, {}^t\bar{H} = (X + \tfrac{1}{\sqrt{d}} Y I_r) I_r\, {}^t(X - \tfrac{1}{\sqrt{d}} Y I_r) = I_s$$

for the real part of this equation comes from $X\, {}^tW - Y\, {}^tZ = I$ (B.1.3) and the imaginary part follows similarly because $h \in \mathrm{Sp}_{2n}(\mathbb{R})$. But I_r and I_s are Hermitian matrices so this equation implies that their signatures are equal, that is, $r = s$. □

5.6. Let $h(x) \in \mathbb{Z}[x]$ be a real, ordinary Weil q-polynomial, (Appendix A), that is,

(h1) $h(0)$ is relatively prime to q

(h2) the roots $\beta_1, \beta_2, \cdots, \beta_n$ of h are totally real and $|\beta_i| < 2\sqrt{q}$ for $1 \le i \le n$.

Let $\mathcal{S}(h)$ be the algebraic variety, defined over $\mathbb{Q}$, consisting of all pairs (A_0, C) where $A_0, C \in \mathrm{GL}_n$, where A_0 is semisimple and its characteristic polynomial is equal to $h(2x)$, where C is symmetric

and ${}^tA_0C = CA_0$. As in Lemma 5.2 there is a natural mapping

$$\theta : \mathcal{S}(h) \to \mathrm{GSp}_{2n}, \quad (A_0, C) \mapsto \begin{pmatrix} A_0 & B \\ C & {}^tA_0 \end{pmatrix} \tag{5.6.1}$$

where $B = (A_0^2 - qI)C^{-1}$. The image $\theta(\mathcal{S}(h)_{\mathbb{Q}})$ of the set of rational elements consists of all q-inversive elements whose characteristic polynomial is the ordinary Weil q-polynomial $p(x) = x^n h(x+q/x)$ (see Appendix A). The image of θ is preserved by the action of GL_n, which corresponds to the action

$$X.(A_0, C) = (XA_0X^{-1}, {}^tX^{-1}CX^{-1}) \tag{5.6.2}$$

for $X \in \mathrm{GL}_n$. In the notation of §5.2 above, the orbits of $\mathrm{GL}_n(\mathbb{R})$ on $\mathcal{S}(h)_{\mathbb{R}}$ are uniquely indexed by the values $\mathrm{sig}(A_0; C) = \{\mathrm{sig}(C_\beta)\}$ of the signature of each of the quadratic forms C_β on the eigenspace V_β, as β varies over the distinct roots of $h(x)$. By abuse of terminology we shall refer to the rational elements in the $\mathrm{GL}_n(\mathbb{R})$ orbit of $(A_0, C) \in \mathcal{S}(h)_{\mathbb{Q}}$ as the "$\mathrm{GL}_n(\mathbb{R})$-orbit containing (A_0, C)".

5.7. Let $(A_0, C_0) \in \mathcal{S}(h)_{\mathbb{Q}}$ and set $\gamma = \theta(A_0) \in \mathrm{GSp}_{2n}(\mathbb{Q})$ as in equation (5.6.1). The algebra $K = \mathbb{Q}[\gamma]$ is isomorphic to a product of CM fields (cf. §3.5). Fix a CM type Φ for K.

Recall from Lemma 3.12 (resp. Lemma 4.4) that in order for the pair (γ, ω_0) (resp. the triple $(\gamma, \omega_0, \tau_0)$) to give rise to a Φ-polarized Deligne module (resp. Φ-polarized Deligne module with real structure), it is necessary and sufficient that γ should be Φ-viable.

5.8. Proposition. *Fix $h(x)$ and Φ as in §5.6 and §5.7 above. For any semisimple matrix $A_0 \in \mathrm{GL}_n(\mathbb{Q})$ with characteristic polynomial equal to $h(2x)$ there exists a symmetric nonsingular element $C_0 \in \mathrm{GL}_n(\mathbb{Q})$ so that $(A_0, C_0) \in \mathcal{S}(h)_{\mathbb{Q}}$ and so that $\gamma_0 = \theta(A_0, C_0) \in \mathrm{GSp}_{2n}(\mathbb{Q})$ is Φ-viable. For every $(A, C) \in \mathcal{S}(h)_{\mathbb{Q}}$ the corresponding element $\gamma = \theta(A, C)$ is Φ-viable if and only if it is $\delta(\mathrm{GL}_n(\mathbb{R}))$-conjugate to γ_0.*

Proof. Given A_0 we need to prove the existence of $C_0 \in \mathrm{GL}_n(\mathbb{Q})$ such that $(A_0, C_0) \in \mathcal{S}(h)$ is Φ-viable. By Lemma 4.4 there is a Φ-polarized Deligne module with real structure, (T, F, ω, τ) whose characteristic polynomial is $p(x)$. Use Proposition B.4 to choose a basis $h : T \otimes \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}^{2n}$ so that that $h(T) \subset \mathbb{Q}^{2n}$ is a lattice, so that $h_*(\omega) = \omega_0$ and that $h_*(\tau) = \tau_0$ in which case the mapping F becomes a matrix $\gamma = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right)$. It follows that γ is viable and that the characteristic polynomial of A is equal to that of A_0. So there exists $X \in \mathrm{GL}_n(\mathbb{Q})$ satisfying $A_0 = XAX^{-1}$. Define $C_0 = {}^tX^{-1}CX^{-1}$ so that $(A_0, C_0) = X \cdot (A, C)$. Then $\gamma_0 = \theta(A_0, B_0) = \delta(X)\gamma\delta(X)^{-1}$ is q-inversive, its characteristic polynomial is $p(x)$, and by Proposition 3.12 it is viable.

For the second statement, γ is Φ-viable iff it is $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugate to γ_0, by Proposition 3.12. This holds iff it is $\delta(\mathrm{GL}_n(\mathbb{R}))$-conjugate to γ_0, by Proposition 5.5. □

5.9. Remark. In the notation of the preceding paragraph, $\gamma = \theta(A, C)$ is Φ-viable iff $\mathrm{sig}(A, C) = \mathrm{sig}(A_0, C_0)$. If the roots of $h(x)$ are distinct then the CM field $\mathbb{Q}[\gamma]$ has 2^n different CM types, corresponding to the 2^n possible values of $\mathrm{sig}(A, C)$ (that is, an ordered n-tuple of ± 1). However, if $h(x)$ has repeated roots then there exist elements $(A, C) \in \mathcal{S}(h)_{\mathbb{Q}}$ such that $\gamma = \theta(A, C)$ is not viable for any choice Φ of CM type on $\mathbb{Q}[\gamma]$.

6. $\overline{\mathbb{Q}}$-isogeny classes

The first step in counting the number of (principally polarized) Deligne modules (with or without real structure) is to identify the set of $\overline{\mathbb{Q}}$ isogeny classes of such modules, following the method of Kottwitz [36]. Throughout this and subsequent chapters we shall only consider polarizations that are positive with respect to the CM type Φ_ε as described in §3.7.

6.1. Lemma. *For $i = 1, 2$ let (T_i, F_i) be a Deligne module with (Φ_ε-positive) polarization ω_i. Let p_i be the characteristic polynomial of F_i. Then the following statements are equivalent.*

1. *The characteristic polynomials are equal: $p_1(x) = p_2(x)$.*
2. *The Deligne modules (T_1, F_1) and (T_2, F_2) are $\mathbb{Q}$-isogenous.*
3. *The Deligne modules (T_1, F_1) and (T_2, F_2) are $\overline{\mathbb{Q}}$-isogenous.*
4. *The polarized Deligne modules (T_1, F_1, ω_1) and (T_2, F_2, ω_2) are $\overline{\mathbb{Q}}$-isogenous.*

For $i = 1, 2$ suppose the polarized Deligne module (T_i, F_i, ω_i) admits a real structure τ_i. Then (1), (2), (3), (4) *are also equivalent to the following statements*

5. *The real Deligne modules (T_1, F_1, τ_1) and (T_2, F_2, τ_2) are $\mathbb{Q}$-isogenous*
6. *The real Deligne modules (T_1, F_1, τ_1) and (T_2, F_2, τ_2) are $\overline{\mathbb{Q}}$-isogenous*
7. *The real polarized Deligne modules $(T_1, F_1, \omega_1, \tau_1)$ and $(T_2, F_2, \omega_2, \tau_2)$ are $\overline{\mathbb{Q}}$-isogenous.*

Proof. Clearly, (4) $\Longrightarrow$ (3) $\Longrightarrow$ (1) and (2) $\Longrightarrow$ (1). The implication (1) $\Longrightarrow$ (2) is a special case of a theorem of Tate, but in our case it follows immediately from the existence of rational canonical form (see, for example, [34] p. 443) that is, by decomposing $T_i \otimes \mathbb{Q}$ into F_i-cyclic subspaces ($i = 1, 2$) and mapping cyclic generators in T_1 to corresponding cyclic generators in T_2.

The proof that (2) $\Longrightarrow$ (4) is a special case of Kottwitz [36] p. 206, which proceeds as follows. Given $\phi : (T_1 \otimes \mathbb{Q}, F_1) \to (T_2 \otimes \mathbb{Q}, F_2)$ define $\beta \in \mathrm{End}_{\mathbb{Q}}(T_1, F_1)$ by $\omega_1(\beta x, y) = \omega_2(\phi(x), \phi(y))$. The *Rosati involution* ($\beta \mapsto \beta'$) is the adjoint with respect to ω_1 and it fixes β since

$$\omega_1(\beta' x, y) = \omega_1(x, \beta y) = -\omega_1(\beta y, x) = -\omega_2(\phi(y), \phi(x)) = \omega_1(\beta x, y).$$

By Lemma C.1 there exists $\alpha \in \mathrm{End}_{\mathbb{Q}}(T_1, F_1)$ such that $\beta = \alpha'\alpha$ which gives

$$\omega_1(\alpha'\alpha x, y) = \omega_1(\alpha x, \alpha y) = \omega_2(\phi(x), \phi(y)).$$

Thus $\phi \circ \alpha^{-1} : (T_1 \otimes \overline{\mathbb{Q}}, F_1) \to (T_2 \otimes \overline{\mathbb{Q}}, F_2)$ is a $\overline{\mathbb{Q}}$-isogeny that preserves the polarizations.

Now suppose that real structures τ_1, τ_2 are provided. It is clear that (7) $\Longrightarrow$ (6) and (4); also that (5) $\Longrightarrow$ (6) $\Longrightarrow$ (3). Now let us show (in the presence of τ_1, τ_2)) that (4) $\Longrightarrow$ (7). The involution $\tau_i \in \mathrm{GSp}(T_i, \omega_i)$ has multiplier -1. So by Lemma B.2 and Proposition B.4 there exist $\psi_i : T_i \otimes \mathbb{Q} \to \mathbb{Q}^{2n}$ which takes the symplectic form ω_i to the standard symplectic form ω_0, and which takes the involution τ_i to the standard involution τ_0. It therefore takes F_i to some $\gamma_i \in \mathrm{GSp}_{2n}(\mathbb{Q})$ which is q-inversive with respect to the standard involution τ_0.

By part (4) there is a $\overline{\mathbb{Q}}$ isogeny $\phi : (T_1, F_1, \lambda_1) \to (T_2, F_2, \lambda_2)$. This translates into an element $\theta \in \mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ such that $\gamma_2 = \theta^{-1}\gamma_1\theta$. By Proposition 5.5 there exists an element $\Psi \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ such that $\gamma_2 = \Psi^{-1}\gamma_1\Psi$. In other words, Ψ corresponds to a $\overline{\mathbb{Q}}$-isogeny $(T_1, F_1, \lambda_1, \tau_1) \to (T_2, F_2, \lambda_2, \tau_2)$.

Now let us show that (6) $\Longrightarrow$ (5). Let us suppose that (T_1, F_1, τ_1) and (T_2, F_2, τ_2) are $\overline{\mathbb{Q}}$-isogenous. This implies that the characteristic polynomials $p_1(x)$ and $p_2(x)$ of F_1 and F_2 (respectively) are equal. Moreover, the ± 1 eigenspaces of τ_1 have the same dimension because $T \otimes \overline{\mathbb{Q}}_p$

decomposes as a direct sum of two subspaces that are exchanged by τ_1, cf. [10]§7. Set $V_1 = T_1 \otimes \mathbb{Q}$ and $V_2 = T_2 \otimes \mathbb{Q}$ and denote these eigenspace decompositions as follows,

$$V_1 \cong V_1^+ \oplus V_1^- \quad \text{and} \quad V_2 \cong V_2^+ \oplus V_2^-.$$

First let us consider the case that the characteristic polynomial $p_1(x)$ of F_1 is irreducible. In this case every non-zero vector in V_1 is a cyclic generator of V_1. Choose nonzero cyclic generators $v \in V_1^+$ and $w \in V_2^+$, and define $\psi : V \to V_2$ by

$$\psi(F_1^r v) = F_2^r w$$

for $1 \leq r \leq \dim(T)$. This mapping is well defined because F_1 and F_2 satisfy the same characteristic polynomial. Clearly, $\psi \circ F_1 = F_2 \circ \psi$. However we also claim that $\psi \circ \tau_1 = \tau_2 \circ \psi$. It suffices to check this on the cyclic basis which we do by induction. By construction we have that $\psi\tau_1 v = \tau_2 \psi v = \tau_2 w$ so suppose we have proven that $\psi\tau_1 F_1^m v = \tau_2 \psi F_1^m v = \tau_2 F_2^m w$ for all $m \leq r-1$. Then

$$\begin{aligned}\psi\tau_1 F_1^r v &= \psi\tau_1 F_1 \tau_1^{-1}\tau_1 F_1^{r-1} v = q\psi F_1^{-1}\tau_1 F_1^{r-1} v \\ &= qF_2^{-1}\psi\tau_1 F_1^{r-1} v = qF_2^{-1}\tau_2\psi F_1^{r-1} v \\ &= \tau_2 F_2 \psi F_1^{r-1} v = \tau_2 \psi F_1^r v.\end{aligned}$$

Thus we have constructed a $\mathbb{Q}$ isogeny between these two real Deligne modules.

If the characteristic polynomial $p_1(x)$ is reducible then V_i $(i = 1, 2)$ may be decomposed as a direct sum of F_i-cyclic subspaces, each of which is preserved by the involution τ_i, thus reducing the problem to the case of irreducible characteristic polynomial. □

6.2. Proposition. *Associating the characteristic polynomial to each Deligne module induces a canonical one to one correspondence between the following objects*

(a) *The set of ordinary Weil q-polynomials $p(x) \in \mathbb{Z}[x]$ of degree $2n$ (see Appendix A)*
(b) *The set of $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$-conjugacy classes of semisimple elements $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ whose characteristic polynomial is an ordinary Weil q-polynomial*
(c) *The set of $\mathbb{Q}$-isogeny classes of Deligne modules (T, F)*
(d) *The set of $\overline{\mathbb{Q}}$-isogeny classes of (Φ_ε-positively) polarized Deligne modules (T, F, λ)*

and a one to one correspondence between the following objects

(a′) *The set of ordinary real Weil q-polynomials (see Appendix A) of degree n*
(b′) *The set of $\mathrm{GL}_n(\mathbb{Q})$-conjugacy classes of semisimple elements $A_0 \in \mathrm{GL}_n(\mathbb{Q})$ whose characteristic polynomial is $h(2x)$ where h is an ordinary real Weil q-polynomial.*
(c′) *The set of $\mathbb{Q}$-isogeny classes of Deligne modules (T, F, τ) with real structure*
(d′) *The set of $\overline{\mathbb{Q}}$-isogeny classes of (Φ_ε-positively) polarized Deligne modules (T, F, ω, τ) with real structure.*

Proof. The correspondence (a)→(b) is given by Proposition A.5 (companion matrix for the symplectic group) while (b)→(a) associates to γ its characteristic polynomial. This correspondence is one-to-one because semisimple elements in $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ are conjugate iff their characteristic polynomials are equal. Items (b) and (c) are identified by the Honda-Tate theorem ([59]), but can also be seen directly. Given γ one constructs a lattice $T \subset \mathbb{Q}^{2n}$ that is preserved by γ and by $q\gamma^{-1}$ by considering one cyclic subspace at a time (cf. Lemma 4.3) and taking T to be the lattice spanned

by $\{\gamma^m v_0\}$ and by $\{(q\gamma)^m v_0\}$ where v_0 is a cyclic vector. Lemma 6.1 may be used to complete the proof that the correspondence is one to one. Items (c) and (d) correspond by Proposition 3.10 (existence of a polarization) and by Lemma 6.1.

The correspondence (a′)↔(b′) is standard. For the correspondence (a′)→(c′), each ordinary real Weil q-polynomial $h(x)$ is the real counterpart of an ordinary Weil q-polynomial $p(x)$ by Appendix A. It suffices to consider the case that $p(x)$ is irreducible. Let π be a root of $p(x)$ so that $K = \mathbb{Q}[\pi]$ is a CM field. Set $T = \mathcal{O}_K$ (the full ring of integers), let $F = \pi : T \to T$ be multiplication by π and let τ denote complex conjugation. Then τ preserves $\mathcal{O}_K$ and $\tau F \tau = qF^{-1}$ because $\pi\bar{\pi} = q$. Hence (T, F, π) is a Deligne module with real structure whose characteristic polynomial is $p(x)$. Lemma 6.1 says that this association (a′)→(c′) is one to one and onto. A mapping (c′)→(d′) is given by Lemma 4.4 (existence of a polarization) and this mapping is one to one and onto by Lemma 6.1. □

In order to "count" the number of real Deligne modules it is necessary to describe them, up to isomorphism (rather than isogeny) in terms of algebraic groups as follows.

6.3. Lemma. *Let (T, F, ω, τ) be a rank $2n$ Deligne module with Φ_ε-positive polarization and real structure. Then it is isomorphic to one of the form*

$$(L, \gamma, \omega_0, \tau_0)$$

where $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ is q-inversive and its characteristic polynomial is an ordinary Weil q-polynomial; where $L \subset \mathbb{Q}^{2n}$ is a lattice that is preserved by γ, by $q\gamma^{-1}$ and by τ_0, and where the standard symplectic form ω_0 takes integer values on L. The group of self $\mathbb{Q}$-isogenies of (T, F, ω) (resp. (T, F, ω, τ)) is isomorphic to the centralizer $Z_\gamma(\mathbb{Q})$ in $\mathrm{GSp}_{2n}(\mathbb{Q})$ (resp. in $\mathrm{GL}_n^*(\mathbb{Q})$). Every element $\phi \in Z_\gamma(\mathbb{Q})$ has positive multiplier $c(\phi) > 0$.

If (T, F, ω, τ) is principally polarized then it is isomorphic to a principally polarized Deligne module of the form

$$(L_0, \gamma, \omega_0, \tau_1)$$

where $L_0 = \mathbb{Z}^{2n}$ is the standard lattice, where $\tau_1 \in \mathrm{GSp}_{2n}(\mathbb{Z})$ is an involution with multiplier -1, where $\gamma, q\gamma^{-1} \in \mathrm{GSp}_{2n}(\mathbb{Q}) \cap M_{2n\times 2n}(\mathbb{Z})$ preserve the integral lattice L_0 and where $\tau_1\gamma\tau_1^{-1} = q\gamma^{-1}$.

Proof. By Lemma B.2 and Proposition B.4 there is a basis $\phi : T \otimes \mathbb{Q} \to \mathbb{Q}^{2n}$ of $T \otimes \mathbb{Q}$ so that ω becomes ω_0 and so that τ becomes τ_0. Take $L = \phi(T)$ and $\gamma = \phi F \phi^{-1}$. This induces an isomorphism $\mathbb{Q}[F] \cong \mathbb{Q}[\gamma]$ preserving the CM type Φ_ε on each, such that ω_0 is Φ_ε-positive. The centralizer statements are clear. If $\phi \in Z_\gamma(\mathbb{Q})$ and if $\iota \in \mathbb{Q}[\gamma]$ is a Φ_ε-totally positive imaginary element then

$$R(\phi(x), \phi(x)) = \omega_0(\phi x, \iota\phi x) = \omega_0(\phi x.\phi\iota x) = c(\phi)R(x, x) > 0.$$

If the original polarization ω of (T, F, τ) is principal then Lemma B.2 provides an isomorphism $(T, \omega) \cong (L_0, \omega_0)$ which takes F to some element γ and takes the involution τ to some involution τ_1, both of which preserve the lattice L_0. □

7. Finiteness

Throughout this section, all polarizations are considered to be Φ_ε-positive. As in §3, let $\mathbb{F}_q$ be a finite field of characteristic $p > 0$, fix $N \geq 1$ not divisible by p, and let $n \geq 1$. We refer to §D.3 for the definition of a level N structure.

7.1. Theorem. *Assume $q, N \geq 1$ are coprime. There are finitely many isomorphism classes of principally (Φ_ε-positively) polarized Deligne modules of rank $2n$ over $\mathbb{F}_q$ with real structure and with principal level N structure.*

Proof. It follows from Proposition 6.2 that there are finitely many $\overline{\mathbb{Q}}$-isogeny classes of (Φ_ε-positively) polarized Deligne modules with real structure. Moreover, it is easy to see that each isomorphism class (of principally polarized Deligne modules with real structure) contains at most finitely many level N structures. So, for simplicity, we may omit the level structure, and it suffices to show that each $\overline{\mathbb{Q}}$-isogeny class (of Φ_ε-positively polarized Deligne modules with real structure) contains at most finitely many isomorphism classes of principally polarized modules. Therefore, let us fix a Φ_ε-positive principally polarized Deligne module with real structure, which by Lemma 6.3 may be taken to be of the form $(L_0, \gamma, \omega_0, \eta_0)$ where: $\eta_0 \in \mathrm{GSp}_{2n}(\mathbb{Z})$ is an involution with multiplier -1, where $\gamma_0 \in \mathrm{GSp}_{2n}(\mathbb{Q}) \cap M_{2n\times 2n}(\mathbb{Z})$ and its characteristic polynomial is an ordinary Weil q-polynomial, and where $\eta_0\gamma_0\eta_0^{-1} = q\gamma_0^{-1}$.

The group $G' = \mathrm{Sp}_{2n}$ acts on $V = M_{2n\times 2n} \times M_{2n\times 2n}$ by $g.(\gamma, \eta) = (g\gamma g^{-1}, g\eta g^{-1})$. Let $\Gamma = \mathrm{Sp}_{2n}(\mathbb{Z})$ be the arithmetic subgroup that preserves the lattice

$$L = M_{2n\times 2n}(\mathbb{Z}) \times M_{2n\times 2n}(\mathbb{Z})$$

of integral elements. It also preserves the set of pairs (γ, η) such that $\eta \in \mathrm{GSp}_{2n}(\mathbb{Z})$, $\eta^2 = I$, $\eta\gamma\eta^{-1} = q\gamma^{-1}$. Let $v_0 = (\gamma_0, \eta_0)$. We claim

(1) the orbit $G'_{\mathbb{C}}.v_0$ is closed in $V_{\mathbb{C}}$, and
(2) there is a natural injection from
   (a) the set of isomorphism classes of principally polarized Abelian varieties with real structure within the $\overline{\mathbb{Q}}$-isogeny class of $(T_0, \gamma_0, \omega_0, \eta_0)$ to
   (b) the set of Γ-orbits in $L \cap G'_{\overline{\mathbb{Q}}}.v_0$.

Using claim (1) we may apply Borel's theorem[9] [5] (§9.11) and conclude that there are finitely many Γ orbits in $L \cap G'_{\overline{\mathbb{Q}}}.v_0$ which implies, by claim (2) that there are finitely many isomorphism classes.

Proof of claim (2). Consider a second principally polarized "real" Deligne module, $(L_0, \gamma_1, \omega_0, \eta_1)$, within the same $\overline{\mathbb{Q}}$-isogeny class. By Proposition 6.2, a $\overline{\mathbb{Q}}$-isogeny between these two Deligne modules is an element $X \in \mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ such that $\gamma_1 = X\gamma_0X^{-1}$ and $\eta_1 = X\eta_0X^{-1}$. In particular this means that the pair (γ_1, η_1) is in the orbit $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}}).v_0$, which coincides with the orbit $G'(\overline{\mathbb{Q}}).v_0 = \mathrm{Sp}_{2n}(\overline{\mathbb{Q}}).v_0$. Moreover, such an isogeny X is an isomorphism (of principally polarized Deligne

[9]Let M be a reductive algebraic group defined over $\mathbb{Q}$ and let $\Gamma \subset M_{\mathbb{Q}}$ be an arithmetic subgroup. Let $M_{\mathbb{Q}} \to \mathrm{GL}(V_{\mathbb{Q}})$ be a rational representation of M on some finite dimensional rational vector space. Let $L \subset V_{\mathbb{Q}}$ be a lattice that is stable under Γ. Let $v_0 \in V$ and suppose that the orbit $M_{\mathbb{C}}.v_0$ is closed in $V_{\mathbb{C}} = V_{\mathbb{Q}} \otimes \mathbb{C}$. Then $L \cap M_{\mathbb{C}}.v_0$ consists of a finite number of orbits of Γ.

modules with real structure) if and only if X and X^{-1} preserve the lattice L_0 and the symplectic form ω_0, which is to say that $X \in \Gamma$.

We remark that the mapping from (2a) to (2b) above is not necessarily surjective for the following reason. The element γ_0 is (Φ_ε-)*viable* (see §3.11), that is, it satisfies the "positivity" condition (*) of §3.7, because it comes from a polarized Abelian variety. However, if $(\gamma, \eta) \in L \cap G'_{\overline{\mathbb{Q}}}.v_0$ is arbitrary then γ may fail to be Φ_ε-viable.

Proof of claim (1). Since γ_0 and η_0 are both semisimple, the conjugacy class

$$(G'_{\mathbb{C}}.\gamma_0) \times (G'_{\mathbb{C}}.\eta_0) \subset M_{2n\times 2n}(\mathbb{C}) \times M_{2n\times 2n}(\mathbb{C})$$

is closed ([29] §18.2). We claim that the orbit $G'_{\mathbb{C}}.v_0$ coincides with the closed subset

$$S = \left\{(\gamma, \tau) \in (G'_{\mathbb{C}}.\gamma_0) \times (G'_{\mathbb{C}}.\tau_0) |\ \tau\gamma\tau^{-1} = q\gamma^{-1}\right\}.$$

Clearly, $G'_{\mathbb{C}}.v_0 \subset S$. If $(\gamma, \eta) \in (G'_{\mathbb{C}}.\gamma_0) \times (G'_{\mathbb{C}}.\eta_0)$ lies in the subset S then by Proposition B.4, conjugating by an element of $G'_{\mathbb{C}}$ if necessary, we may arrange that $\eta = \tau_0$ is the standard involution. Consequently, $\tau_0\gamma\tau_0^{-1} = q\gamma^{-1}$, which is to say that γ is q-inversive. By assumption it is also $G'_{\mathbb{C}}$-conjugate to γ_0. According to Proposition 5.5, $G'_{\mathbb{C}}$-conjugacy of q-inversive elements coincides with $\delta(\mathrm{GL}_n(\mathbb{C}))$-conjugacy. Thus there exists $g \in \delta(\mathrm{GL}_n(\mathbb{C}))$ so that $(g\gamma g^{-1}, g\tau_0 g^{-1}) = (\gamma_0, \tau_0)$. In summary, the element (γ, η) lies in the $G'_{\mathbb{C}}$-orbit of (γ_0, τ_0). This concludes the proof of Theorem 7.1. □

7.2. The case $n = 1$. Fix $q = p^m$ and let $\mathbb{F}_q$ denote the finite field with q elements. According to Proposition 6.2 the set of $\overline{\mathbb{Q}}$-isogeny classes of Deligne modules (T, F) of rank 2, over $\mathbb{F}_q$ is determined by a quadratic ordinary Weil q-number π, which we now fix. This means that π satisfies an equation

$$\pi^2 + B\pi + q = 0$$

where $p \nmid B$. Let $D = B^2 - 4q$. Then $D \equiv 0, 1 \pmod 4$ and $-4q < D < 0$. The pair $\{\pi, \bar\pi\}$ determines D and vice versa.

Isomorphism classes of polarized Deligne modules with real structure fall into orbits that are identified by certain cohomology classes as described in Proposition D.7 or equivalently by integral conjugacy classes of involutions as described in Proposition D.2. For $n = 1$ there are two involutions (see Lemma B.5) to consider, namely

$$\tau_0 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}.$$

7.3. Proposition. *Over the finite field $\mathbb{F}_q$, the number of (real isomorphism classes of) principally polarized Deligne modules (T, F, λ, η) with real structure and rank 2, such that the eigenvalues of F are $\{\pi, \bar\pi\}$, which correspond to the cohomology class of the standard involution τ_0 is:*

$$\begin{cases} \sigma_0(-D/4) & \text{if } D \equiv 0 \pmod 4 \\ 0 & \text{otherwise} \end{cases}$$

where $\sigma_0(m)$ denotes the number of positive divisors of $m > 0$. The number of isomorphism classes which correspond to the cohomology class of τ_1 is:

$$\begin{cases} \sigma_0(-D) & \text{if } D \equiv 1 \pmod 4 \\ \sigma_0'(-D/4) & \text{if } D \equiv 0 \pmod 4 \end{cases}$$

where $\sigma_0'(m)$ denotes the number of ordered factorizations $m = uv$ such that $u, v > 0$ have the same parity.

Proof. According to Proposition 6.2 the isomorphism classes of principally polarized Deligne modules with real structures correspond to q-inversive pairs (γ, η) where the eigenvalues of $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ are π and $\bar\pi$. For the involution τ_0 , the pair (γ, τ_0) is q-inversive if $\gamma = \left(\begin{smallmatrix} a & b \\ c & a \end{smallmatrix}\right)$ and $\det(\gamma) = q$. This implies that $a = -B/2$, so B is even and $D \equiv 0 \pmod 4$. Then $bc = a^2 - q = D/4$ has a unique solution for every (signed) divisor b of $D/4$. Half of these will be viable (see §3.11) so the number of solutions is equal to the number of positive divisors of $-D/4$.

For the involution τ_1, the pair (γ, τ_1) is q-inversive if $\gamma = \left(\begin{smallmatrix} a & b \\ c & a-b \end{smallmatrix}\right)$. This implies that $D = B^2 - 4q = b(b+4c)$. Let us first consider the case that b is odd or equivalently, that $D \equiv 1 \pmod 4$. For every divisor $b|D$ we can solve for an integer value of c so we conclude that the number of viable solutions in this case is equal to $\sigma_0(-D)$. Next, suppose that b is even, say, $b = 2b'$. Then D is divisible by 4, say, $D = 4D'$ and $D' = b'(b' + 2c)$ is an ordered factorization of D' with factors of the same parity. So in this case the number of viable solutions is $\sigma_0'(-D/4)$. □

7.4. It follows that the total number of real isomorphism classes over $\mathbb{F}_q$, $q = p^m$, corresponding to the trival cohomology class, is $N = 2\sum_{1 \le a \le q-1} \sigma_0(q - a^2)$, a number whose asymptotics was determined by Ingham [31] and Hooley [23],

$$N \sim \begin{cases} \frac{6}{\pi^2}\left(\sqrt{q}(\log(q))^2 + 3\log 2 \log q\right) & m \text{ even} \\ C(p)\sqrt{q}\log q & m \text{ odd} \end{cases}.$$

7.5. For any totally positive imaginary integer $\alpha \in L = \mathbb{Q}(\pi)$ the bilinear form $\omega(x, y) = \mathrm{Trace}_{L/\mathbb{Q}}(\alpha x \bar y)$ is symplectic. If $\Lambda \subset L$ is a lattice then α may be chosen so that the form ω takes integer values on Λ. Modifying Λ by a homothety if necessary, it can also be arranged that ω is a principal polarization, hence (Λ, π, ω) is a principally polarized Deligne module. If complex conjugation on $L = \mathbb{Q}(\pi)$ preserves Λ then it defines a real structure on this Deligne module.

7.6. Proposition. *The set of isomorphism classes of Φ_ε-positive principally polarized Deligne modules (of rank 2) with real structure and with eigenvalues $\{\pi, \bar\pi\}$ may be identified with the set of homothety classes of lattices $\Lambda \subset \mathbb{Q}(\pi)$ that are preserved by complex conjugation and by multiplication by π.*

Proof. The most natural proof, which involves considerable checking, provides a map back from lattices Λ to Deligne modules: Deligne's CM type determines an isomorphism $\Phi : \mathbb{Q}(\pi) \otimes \mathbb{R} \to \mathbb{C}$. Then realize the elliptic curve $\mathbb{C}/\Phi(\Lambda)$ as the complex points of the canonical lift of an ordinary elliptic curve over $\mathbb{F}_q$ whose associated Deligne module is (Λ, π). Then check that complex conjugation is compatible with these constructions.

A simpler but less illuminating proof is simply to count the number of homothety classes of lattices and to see that this number coincides with the number in Proposition 7.3. □

8. $\mathbb{Q}$-isogeny classes within a $\overline{\mathbb{Q}}$ isogeny class

8.1. Let us fix a (Φ_ε-positively) polarized Deligne module with real structure, $(L_1, \gamma_1, \omega_0, \tau_0)$ where

$$\gamma_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & {}^tA_1 \end{pmatrix}$$

is q-inversive, ω_0 is the standard symplectic form, τ_0 is the standard involution, and $L_1 \subset \mathbb{Q}^{2n}$ is a lattice preserved by τ_0, by γ_1 and by $q\gamma_1^{-1}$, on which ω_0 takes integer values, cf. Lemma 6.3 . Let $Z_{\mathrm{GL_n}(\mathbb{Q})}(A_1)$ denote the set of elements in $\mathrm{GL}_n(\mathbb{Q})$ that commute with A_1.

8.2. Proposition. *The association $C \mapsto \gamma = \left(\begin{smallmatrix} A_1 & B \\ C & {}^tA_1 \end{smallmatrix}\right)$, where $B = (A_1 - qI)C^{-1}$, determines a one to one correspondence between the following sets,*

1. *elements $C \in \mathrm{GL}_n(\mathbb{Q})$, one from each $Z_{\mathrm{GL_n}(\mathbb{Q})}(A_1)$-congruence class of symmetric matrices such that ${}^tA_1C = CA_1$ and $\mathrm{sig}(A_1; C) = \mathrm{sig}(A_1; C_1)$.*
2. *The set of $\mathbb{Q}$ isogeny classes of real (Φ_ε-positively) polarized Deligne modules (T, F, λ, τ) within the $\overline{\mathbb{Q}}$ isogeny class of $(L_1, \gamma_1, \omega_0, \tau_0)$*
3. *The set of $\mathrm{GL}_n^*(\mathbb{Q})$-conjugacy classes of elements $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ such that γ, γ_1 are conjugate by some element in $\mathrm{GL}_n^*(\mathbb{R}) \subset \mathrm{Sp}_{2n}(\mathbb{R})$*
4. *the elements of $\ker\left(H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), I_1) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), I_1)\right)$*

where I_1 denotes the group of self isogenies of $(L_1, \gamma_1, \omega_0, \tau_0)$, that is,

$$I_1 = Z_{\mathrm{GL}_n^*}(\gamma_1) \cong Z_{\mathrm{GL}_n}(A_1) \cap \mathrm{GO}(C_1) \tag{8.2.1}$$

where

$$\mathrm{GO}(C_1) = \left\{X \in \mathrm{GL}_n \mid {}^tXC_1X = \mu C_1 \ (\exists \mu \neq 0)\right\}$$

denotes the general orthogonal group defined by the symmetric matrix C_1.

Proof. To describe the correspondence (1)→(3), given C set $\gamma = \left(\begin{smallmatrix} A_1 & B \\ C & {}^tA_1 \end{smallmatrix}\right)$ where $B = (A^2 - qI)C^{-1}$. Since $\mathrm{sig}(A_1; C) = \mathrm{sig}(A_1; C_1)$, Proposition 5.5 implies that γ, γ_1 are conjugate by an element of $\delta(\mathrm{GL}_n(\mathbb{R})) \subset \mathrm{GL}_n^*(\mathbb{R})$.

Conversely, let $\gamma = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right) \in \mathrm{GSp}_{2n}(\mathbb{Q})$ be q-inversive and $\mathrm{GL}_n^*(\mathbb{R})$-conjugate to γ_1. Then A, A_1 are conjugate by an element of $\mathrm{GL}_n(\mathbb{R})$ so they are also conjugate by some element $Y \in \mathrm{GL}_n(\mathbb{Q})$. Replacing γ with $\delta(Y)\gamma\delta(Y)^{-1}$ we may therefore assume that $A = A_1$. Proposition 5.5 then says that $\mathrm{sig}(A_1; C) = \mathrm{sig}(A_1; C_1)$. So we have a one to one correspondence (1)↔(3).

For(2)→(3), let $(L, \gamma, \omega_0, \tau_0)$ be a Φ_ε-positively polarized Deligne module with real structure that is $\overline{\mathbb{Q}}$-isogenous to $(L_1, \gamma_1, \omega_0, \tau_0)$. Then γ_1, γ_2 are Φ_ε-viable so by Proposition 3.12 they are also $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugate. Proposition 5.5 says they are $\mathrm{GL}_n^*(\mathbb{R})$-conjugate. A choice of $\overline{\mathbb{Q}}$ isogeny $\phi : (L, \gamma, \omega_0, \tau_0) \to (L_1, \gamma_1, \omega_0, \tau_0)$ is an element $X \in \mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ such that $\gamma = X\gamma_1X^{-1}$ and $\tau_0 X \tau_0^{-1} = X$, hence $X \in \mathrm{GL}_n^*(\overline{\mathbb{Q}})$. The isogeny ϕ is a $\mathbb{Q}$-isogeny if and only if $X \in \mathrm{GL}_n^*(\mathbb{Q})$.

For (3)→(2), start with the basepoint $(L_1, \gamma_1, \omega_0, \tau_0)$ and choose any element $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ that is $\mathrm{GL}_n^*(\mathbb{R})$-conjugate to γ_1. Then

$$\gamma = t\gamma_1 t^{-1} = h\gamma_1 h^{-1} \tag{8.2.2}$$

for some $t \in \mathrm{GL}_{2n}(\mathbb{Q})$ and some $h \in \mathrm{GL}_n^*(\mathbb{R})$. The set

$$L' := (tL_1) \cap (\tau_0 t L_1) \subset \mathbb{Q}^{2n}$$

is a lattice, so there exists an integer m such that ω_0 takes integer values on $L := mL'$. Then $(L = mL', \gamma, \omega_0, \tau_0)$ is a polarized Deligne module with real structure in the $\overline{\mathbb{Q}}$-isogeny class of $(L_1, \gamma_2, \omega_0, \tau_0)$. The lattice L is preserved by τ_0, by γ and by $q\gamma^{-1}$ from (8.2.2). The element γ is Φ_ε-viable by construction so the symplectic form ω_0 is a polarization on the Deligne module (L, γ).

For (3)$\leftrightarrow$(4), the set $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), I_1)$ indexes the $\mathrm{GL}_n^*(\mathbb{Q})$-conjugacy classes of elements γ within the $\mathrm{GL}_n^*(\overline{\mathbb{Q}})$-conjugacy class of γ_1. Such a class becomes trivial in $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), I_1)$ if γ is $\mathrm{GL}_n^*(\mathbb{R})$-conjugate to γ_1. The isomorphism of equation (8.2.1) follows immediately from equation (5.6.2). □

There may be infinitely many $\mathbb{Q}$-isogeny classes of polarized Deligne modules with real structure within a given $\overline{\mathbb{Q}}$-isogeny class. However, it follows from Theorem 7.1 that only finitely many of these $\mathbb{Q}$-isogeny classes contain principally polarized modules.

8.3. Let $Z(\gamma_1)$ denote the centralizer of γ_1 in GSp_{2n}. Removing the real structure from the proof of Proposition 8.2 gives a one to one correspondence between (a) the set of $\mathbb{Q}$-isogeny classes of Φ_ε-positively polarized Deligne modules within the $\overline{\mathbb{Q}}$-isogeny class of $(L_1, \gamma_1, \omega_0)$, (b) the set of $\mathrm{Sp}_{2n}(\mathbb{Q})$-conjugacy classes of elements $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ that are $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugate to γ_1, and (c) elements of

$$\ker(H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), Z(\gamma_1)) \to H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), Z(\gamma_1)).$$

9. Isomorphism classes within a $\mathbb{Q}$-isogeny class

9.1. The category $\mathcal{P}_N$. In this chapter and in all subsequent chapters we fix $N \geq 3$, not divisible by p. Fix $n \geq 1$. Throughout this chapter we fix a Φ_ε-positively polarized Deligne module (over $\mathbb{F}_q$, of rank $2n$) with real structure, which (by Lemma 6.3) we may assume to be of the form $(T_0, \gamma, \omega_0, \tau_0)$ where $T_0 \subset \mathbb{Q}^{2n}$ is a lattice, $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ is a semisimple element whose characteristic polynomial is an ordinary Weil q-polynomial, and where ω_0 is the standard symplectic form and τ_0 is the standard involution.

Following the method of [36] we consider the category $\mathcal{P}_N = \mathcal{P}_N(T_0, \gamma, \omega_0, \tau_0)$ (possibly empty) for which an object $(T, F, \omega, \beta, \tau, \phi)$ consists of a (Φ_ε positive) *principally* polarized Deligne module $(T, F, \omega, \beta, \tau)$ with real structure τ and principal level N structure β (see §4.1), and where $\phi : (T, F, \omega, \tau) \to (T_0, \gamma, \omega_0, \tau_0)$ is a $\mathbb{Q}$-isogeny of polarized Deligne modules with real structure, meaning that: $\phi : T \otimes \mathbb{Q} \xrightarrow{\sim} \mathbb{Q}^{2n}$, $\phi F = \gamma\phi$, $\phi^*(\omega_0) = c\omega$ for some $c \in \mathbb{Q}^\times$, and $\phi\tau = \tau_0\phi$. A morphism $\psi : (T, F, \omega, \beta, \tau, \phi) \to (T', F', \omega', \beta', \tau', \phi')$ is a group homomorphism $\psi : T \hookrightarrow T'$ such that $\phi = \phi'\psi$ (hence $\psi F = F'\psi$), $\omega = \psi^*(\omega')$, $\beta = \beta' \circ \psi$, and $\psi\tau = \tau'\psi$.

Let X denote the set of isomorphism classes in this category. We obtain a natural one to one correspondence between the set of isomorphism classes of principally polarized Deligne modules with level N structure and real structure within the $\mathbb{Q}$-isogeny class of $(T_0, \gamma, \omega_0, \tau_0)$, and the quotient

$$I_{\mathbb{Q}} \backslash X \tag{9.1.1}$$

where $I_{\mathbb{Q}} = I_{\mathbb{Q}}(T_0, \gamma, \omega_0, \tau_0)$ denotes the group of self $\mathbb{Q}$-isogenies of $(T_0, \gamma, \omega_0, \tau_0)$.

9.2. Category of lattices. See §1.8 for the notations $\mathbb{A}_f^p$, $\widehat{\mathbb{Z}}^p$, $\widehat{K}_N$, $\widehat{K}_N^0$, K_p. Denote by $\mathcal{L}_N = \mathcal{L}_N(\mathbb{Q}^{2n}, \gamma, \omega_0, \tau_0)$ the category for which an object is a pair (L, α) where $L \subset T_0 \otimes \mathbb{Q}$ is a lattice that is symplectic (up to homothety), is preserved by γ, by $q\gamma^{-1}$ and by τ_0, and $\alpha : L/NL \to (\mathbb{Z}/N\mathbb{Z})^{2n}$ is a compatible level structure, (that is: $\bar{\tau}_0\alpha = \alpha\bar{\tau}_0,\ \alpha\gamma = \alpha$), and there exists $c \in \mathbb{Q}^\times$ so that $L^\vee = cL$ and $\alpha_*(c\omega_0) = \overline{\omega}_0$.

A morphism $(L, \alpha) \to (L', \alpha')$ is an inclusion $L \subset L'$ such that $\alpha'|(L/NL) = \alpha$. (Since $L \to L'$ is an inclusion it also commutes with γ and τ_0, and it preserves the symplectic form ω_0.) In this category every isomorphism class contains a unique object.

9.3. Adèlic lattices. Given $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ as above, let $\widehat{\mathcal{L}}_N = \widehat{\mathcal{L}}_N(\mathbb{A}_f^{2n}, \gamma, \omega_0, \tau_0)$ be the category for which an object is a pair $(\widehat{L}, \alpha)$ consisting of a lattice $\widehat{L} \subset \mathbb{A}_f^{2n}$ (cf. Appendix D.3, D.4, D.5) that is symplectic (up to homothety) and is preserved by γ, by $q\gamma^{-1}$ and by τ_0, and a compatible level N structure α, that is:

$$\tau_0\widehat{L} = \widehat{L},\ \alpha\bar{\tau}_0 = \bar{\tau}_0\alpha, \tag{9.3.0}$$

$$\gamma\widehat{L} \subset \widehat{L},\ q\gamma^{-1}\widehat{L} \subset \widehat{L},\ \alpha \circ \gamma = \alpha \tag{9.3.1}$$

$$\widehat{L}^\vee = c\widehat{L} \ \text{ and } \ \alpha_*(c\omega_0) = \overline{\omega}_0 \quad (\exists c \in \mathbb{Q}^\times). \tag{9.3.2}$$

A morphism in $\widehat{\mathcal{L}}_N$ is an inclusion $\widehat{L} \subset \widehat{M}$ that is compatible with the level structures. As in [36] we have the following:

9.4. Proposition. *The association*

$$(T, F, \omega, \beta, \tau, \phi) \mapsto \left(L = \phi(T), \alpha = \beta \circ \phi^{-1}\right) \mapsto (\widehat{L} = \textstyle\prod_v L \otimes \mathbb{Z}_v, \alpha)$$

determines equivalences of categories $\mathcal{P}_N \xrightarrow{\sim} \mathcal{L}_N \xrightarrow{\sim} \widehat{\mathcal{L}}_N$.

Proof. Given $(T, F, \omega, \beta, \phi)$ let $L = \phi(T)$ and $\alpha = \beta\phi^{-1}$. Then $\gamma L = \gamma\phi(T) = \phi(FT) \subset \phi(T) = L$ and similarly $q\gamma^{-1}L \subset L$. Since ω is a principal polarization we obtain

$$T = T^\vee = \{u \in T \otimes \mathbb{Q} |\ \omega(u, v) \in \mathbb{Z} \ \text{ for all } \ v \in T\}.$$

Since ϕ is a $\mathbb{Q}$-isogeny with multiplier $c \in \mathbb{Q}^\times$ we have that $\omega_0(\phi(x), \phi(y)) = c\omega(x, y)$ for all $x, y \in T \otimes \mathbb{Q}$ so

$$\begin{aligned} L^\vee &= \{u \in L \otimes \mathbb{Q} |\ \omega_0(u, v) \in \mathbb{Z} \text{ for all } v \in L\} \\ &= (\phi(T))^\vee = c\phi(T^\vee) = c\phi(T) = cL. \end{aligned}$$

This implies that $c\omega_0$ is integral valued on L and hence

$$\alpha_*(c\omega_0) = \beta_*\phi^*(c\omega_0) = \beta_*(\omega) = \overline{\omega}_0.$$

Hence the pair (L, α) is an object in $\mathcal{L}_N(\mathbb{Q}^{2n}, \gamma, \omega_0, \tau_0)$. If $\psi : (T, F, \omega, \phi) \to (T', F', \omega', \phi')$ is a morphism in $\mathcal{P}_N(T_0, \gamma, \omega_0, \tau_0)$ then $\psi(T) \subset T'$ so $L = \phi(T) \subset L' = \phi(T')$ is a morphism in $\mathcal{L}_N(\mathbb{Q}^{2n}, \gamma, \omega_0, \tau_0)$.

Conversely, given an object (L,α) in $\mathcal{L}_N$, that is, a lattice $L\subset\mathbb{Q}^{2n}$ preserved by γ and $q\gamma^{-1}$ such that $L^\vee = cL$, and a principal level structure $\alpha: L/NL\to(\mathbb{Z}/N\mathbb{Z})^{2n}$ such that $\alpha_*(c\omega_0)=\overline{\omega}_0$, we obtain an object in $\mathcal{P}_N$,

$$(T=L,\ F=\gamma|L,\ \omega=c\omega_0,\ \beta=\alpha,\ \phi=id)$$

such that $T^\vee=\frac{1}{c}L^\vee=L=T$ and such that $\beta_*(\omega)=\alpha_*(c\omega_0)=\overline{\omega}_0$. It follows that $\mathcal{P}_N\to\mathcal{L}_N$ is an equivalence of categories. Finally, $\mathcal{L}_N\to\widehat{\mathcal{L}}_N$ is an equivalence of categories by Lemma D.5. □

9.5. Lattices at p. Let $\gamma\in\mathrm{GSp}_{2n}(\mathbb{Q})$ be a semisimple element whose characteristic polynomial is an ordinary Weil q-polynomial. It induces a decomposition $\mathbb{Q}_p^{2n}\cong W'\oplus W''$ that is preserved by γ but exchanged by τ_0, where the eigenvalues of $\gamma|W'$ are p-adic units and the eigenvalues of $\gamma|W''$ are non-units ([10]§7). Define

$$\alpha_q=\alpha_{\gamma,q}=I'\oplus qI'' \tag{9.5.1}$$

to be the identity on W' and multiplication by q on W''. The following lemma, which is implicit in [36] will be used in Proposition 9.8 to count the number of lattices in $\widehat{\mathcal{L}}_N$.

9.6. Lemma. *Let $\gamma\in\mathrm{GSp}_{2n}(\mathbb{Q})$ be a semisimple element with multiplier equal to q. Let $L_{0,p}=\mathbb{Z}_p^{2n}$ be the standard lattice in $\mathbb{Q}_p^{2n}$. Let $g\in\mathrm{GSp}_{2n}(\mathbb{Q}_p)$ and let c denote its multiplier. Let $L_p=g(L_{0,p})$. Then $L_p^\vee=c^{-1}L_p$ and the following statements are equivalent:*

(a) *The lattice L_p is preserved by γ and by $q\gamma^{-1}$.*
(b) *The lattice L_p satisfies $qL_p\subset\gamma L_p\subset L_p$.*
(c) *$g^{-1}\gamma g\in K_pA_qK_p$*

where $K_p=\mathrm{GSp}_{2n}(\mathbb{Z}_p)$ and $A_q=\left(\begin{smallmatrix}I & 0\\ 0 & qI\end{smallmatrix}\right)$. If the characteristic polynomial of γ is an ordinary Weil q-polynomial then conditions (a),(b),(c) above are also equivalent to:

(d) *$g^{-1}\alpha_q^{-1}\gamma g\in K_p$*

Proof. Clearly (a) and (b) are equivalent, and also to: $qL_p\subset q\gamma^{-1}L_p\subset L_p$. Hence

(b′) $L_p/\gamma L_p\cong\gamma^{-1}L_p/L_p\subset L_p/qL_p\cong(\mathbb{Z}/q\mathbb{Z})^{2n}$.

We now show that (b) $\Longrightarrow$ (c). Since $\det(\gamma)^2=q^{2n}$ we know that $|\det(\gamma)|=|L_p/\gamma L_p|=q^n$. Condition (b) implies that $L_p/\gamma L_p$ consists of elements that are killed by multiplication by q. Condition (b′) implies that $L_p/\gamma L_p$ is free over $\mathbb{Z}/q\mathbb{Z}$. Therefore

$$L_{0,p}/(g^{-1}\gamma g)L_{0,p}\cong L_p/\gamma L_p\cong(\mathbb{Z}/q\mathbb{Z})^n. \tag{9.6.1}$$

By the theory of Smith normal form for the symplectic group (see [57] or [3] Lemma 3.3.6) we may write $g^{-1}\gamma g=uDv$ where $u,v\in K_p$ and $D=\mathrm{diag}(p^{r_1},p^{r_2},\cdots,p^{r_{2n}})$ where $r_1\le r_2\le\cdots\le r_{2n}$. This, together with equation (9.6.1) implies that $r_1=\cdots=r_n=0$ and $r_{n+1}=\cdots=r_{2n}=a$, that is, $D=A_q$. This proves that (b) implies (c).

Now let us show that (c) implies (a). Since $K_pA_qK_p\subset M_{2n\times 2n}(\mathbb{Z}_p)$, condition (c) implies that $\gamma gL_{0,p}\subset gL_{0,p}$. Taking the inverse of condition (c) and multiplying by q gives

$$qg^{-1}\gamma^{-1}g\in K_pqA_q^{-1}K_p\subset M_{2n\times 2n}(\mathbb{Z}_p)$$

which implies that $q\gamma^{-1}L_p\subset L_p$.

Finally, if the characteristic polynomial of γ is an ordinary Weil q-polynomial then (by [10]) the lattice L_p decomposes into γ-invariant sublattices, $L_p = L'_p \oplus L''_p$ such that $\gamma|L'_p$ is invertible and $\gamma|L''_p$ is divisible by q, or $\gamma L'_p = L'_p$ and $\gamma L''_p \subset qL''_p$ which, in light of (d) implies that $\gamma L''_p = qL''_p$. In summary, $\alpha_q^{-1}\gamma L_p = L_p$, which is equivalent to (d). □

9.7. Counting real lattices. As explained in §9.1 we wish to count the number of isomorphism classes of (Φ_ε-positive) principally polarized Deligne modules with level N structure and with real structure that are $\mathbb{Q}$-isogenous to the polarized Deligne module $(T_0, \gamma, \omega_0, \tau_0)$ that was fixed in §9.1. By equation (9.1.1) and Proposition 9.4 this number is

$$|S(\mathbb{Q})\backslash X|$$

where X denotes the set of objects $(\widehat{L}, \alpha)$ in the category $\widehat{\mathcal{L}}_N(\mathbb{A}_f^{2n}, \gamma, \omega_0, \tau_0)$ of §9.3 and where $S(\mathbb{Q})$ denotes the group of (involution preserving) $\mathbb{Q}$-self isogenies of $(T_0, \gamma, \omega_0, \tau_0)$. It may be identified with the centralizer,

$$S_\gamma(\mathbb{Q}) = \{x \in \mathrm{GL}_n^*(\mathbb{Q}) \,|\gamma x = x\gamma\}\,.$$

(Note that $\gamma \notin \mathrm{GL}_n^*(\mathbb{Q})$.) Following Proposition D.7 the $\mathrm{GL}_n^*(\mathbb{A}_f)$-orbit containing a given object $(\widehat{L}, \alpha)$ is determined by its cohomology class $[\widehat{L}, \alpha] \in H^1 = H^1(\langle\tau_0\rangle, \widehat{K}_N^0)$ of equation (D.7.1). For simplicity, for the moment we assume that N is even: this implies that the contributions from different cohomology classes are independent of the cohomology class, as explained in the following paragraph.

Fix such a class $[t] \in H^1$, corresponding to some element $t \in \widehat{K}_N^0$ with $t\tilde{t} = 1$. Let

$$X_{[t]} = \left\{(\widehat{L}, \alpha) \in X \;\middle|\; [(\widehat{L}, \alpha)] = [t] \in H^1\right\}$$

denote the set of objects $(\widehat{L}, \alpha)$ whose associated cohomology class is $[t]$. We wish to count the number of elements in the set $S_\gamma(\mathbb{Q})\backslash X_t$. Since N is even, the cohomology class $[t]$ vanishes in the cohomology of $\mathrm{Sp}_{2n}(\widehat{\mathbb{Z}})$, by Proposition D.9. This means that $t = g^{-1}\widetilde{g}$ for some $g \in \mathrm{Sp}_{2n}(\widehat{\mathbb{Z}})$.

Let $\widehat{L}_0 = \widehat{Z}^{2n}$ and $\alpha_0 : \widehat{L}/N\widehat{L} \to (\mathbb{Z}/N\mathbb{Z})^{2n}$ denote the standard lattice and the standard level N structure. Then $(g\widehat{L}_0, \alpha_0 \circ g^{-1}) \in \mathcal{R}_N$ is a lattice with real structure and level N structure, whose cohomology class equals $[t] \in H^1$. Its isotropy group under the action of $\mathrm{GL}_n^*(\mathbb{A}_f)$ is the principal congruence subgroup

$$\widehat{\Gamma}_N = \mathrm{GL}_n^*(\mathbb{A}_f) \cap g\widehat{K}_N g^{-1} = \mathrm{GL}_n^*(\mathbb{A}_f) \cap \widehat{K}_N$$

(since $\widehat{K}_N$ is a normal subgroup of $\mathrm{Sp}_{2n}(\widehat{\mathbb{Z}})$) and is independent of the class $[t]$. Hence

$$X_{[t]} \cong \widehat{\Gamma}_N \backslash \mathrm{GL}_n^*(\mathbb{A}_f)$$

is a finite-adèlic analog of the space $X_\mathbb{C}$ described in §1.1. Choose the Haar measure on $\mathrm{GL}_n^*(\mathbb{A}_f)$ that gives measure one to the group $\widehat{\Gamma}_N$.

With $\widehat{K}_N = \widehat{K}_N^p K_p$ (cf. §1.8), define χ^p to be the characteristic function on $\mathrm{GSp}_{2n}(\mathbb{A}_f^p)$ of $\widehat{K}_N^p$ and define χ_p to be the characteristic function on $\mathrm{GSp}_{2n}(\mathbb{Q}_p)$ of K_p. Let $H = \mathrm{GL}_n^*$.

9.8. Proposition. *Suppose that $N \geq 3$ is even and $p \nmid N$. Then*

$$|S_\gamma(\mathbb{Q})\backslash X_t| = \mathrm{vol}(S_\gamma(\mathbb{Q})\backslash S_\gamma(\mathbb{A}_f)) \cdot I_\gamma^p \cdot I_{\gamma,p}$$

where

$$I_\gamma^p = \int_{S_\gamma(\mathbb{A}_f^p)\backslash H(\mathbb{A}_f^p)} \chi^p(x^{-1}\gamma x)dx \tag{9.8.1}$$

and

$$I_{\gamma,p} = \int_{S_\gamma(\mathbb{Q}_p)\backslash H(\mathbb{Q}_p)} \chi_p(x^{-1}\alpha_q^{-1}\gamma x)dx.$$

Here, $\alpha_q = \alpha_{\gamma,q}$ is defined in equation (9.5.1).

Proof. By Proposition D.7 each $(\widehat{L},\alpha) \in X_{[t]}$ has the form $xg.(\widehat{L}_0,\alpha_0)$ for some

$$x = (x^p, x_p) \in \mathrm{GL}_n^*(\mathbb{A}_f^p) \times \mathrm{GL}_n^*(\mathbb{Q}_p) = \mathrm{GL}_n^*(\mathbb{A}_f)$$

where $t = g^{-1}\tilde{g}$ as above, with $g \in \mathrm{Sp}_{2n}(\widehat{\mathbb{Z}})$. Write $\widehat{L} = L^p \times L_p$ for its component away from p and component at p respectively and similarly for $g = g^p g_p$. The conditions (9.3.1) give $\gamma x^p g^p L_0^p = x^p g^p L_0^p$. Hence

$$(g^p)^{-1}(x^p)^{-1}\gamma x^p g^p \in \widehat{K}_N^p$$

which is normal in K^p so equivalently, $\chi^p((x^p)^{-1}\gamma x^p) = 1$. Similarly, by Lemma 9.6,

$$g_p^{-1}x_p^{-1}\alpha_q^{-1}\gamma x_p g_p \in K_p \ \text{ or } \ \chi_p(x_p^{-1}\alpha_q^{-1}\gamma x_p) = 1.$$

In this way we have identified $\widehat{X}_{[t]}$ with the product $X_{[t]}^p \times X_p$ where

$$X_{[t]}^p = \left\{ x \in \mathrm{GL}_n^*(\mathbb{A}_f^p)/\widehat{\Gamma}_N^p \;\middle|\; x^{-1}\gamma x \in \widehat{K}_N^p \right\}$$
$$X_p = \left\{ x \in \mathrm{GL}_n^*(\mathbb{Q}_p)/\,\mathrm{GL}_n^*(\mathbb{Z}_p) \;\middle|\; x^{-1}\alpha_q^{-1}\gamma x \in K_p \right\}.$$

In summary,

$$\begin{aligned} |S_\gamma(\mathbb{Q})\backslash X_{[t]}| &= \int_{S_\gamma(\mathbb{Q})\backslash \mathrm{GL}_n^*(\mathbb{A}_f)} \chi^p(x^{-1}\gamma x)\chi_p(x^{-1}\alpha_q^{-1}\gamma x)dx \\ &= \mathrm{vol}(S_\gamma(\mathbb{Q})\backslash S_\gamma(\mathbb{A}_f)) \cdot I_\gamma^p \cdot I_{\gamma,p}. \end{aligned}$$

□

9.9. If N is odd (with $N \geq 3$ and $p \nmid N$) then the formula must be modified slightly. The pairs $(\widehat{L},\alpha)$ appear in $\mathrm{GL}_n^*(\mathbb{A}_f)$-orbits, $X_{[t]}$, corresponding to cohomology classes $[t] \in H^1(\langle\tau_0\rangle, \widehat{K}_N^0)$ as before. However the class $[t]$ vanishes in $H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\mathbb{A}_f))$ (rather than in $H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\widehat{\mathbb{Z}}))$. Then $t = g^{-1}\tilde{g}$ for some $g \in \mathrm{Sp}_{2n}(\mathbb{A}_f)$ so the orbit $X_{[t]}$ is isomorphic to $\widehat{J}_{[t]}\backslash \mathrm{GL}_n^*(\mathbb{A}_f)$ where $\widehat{J}_{[t]} = \mathrm{GL}_n^*(\mathbb{A}_f) \cap g\widehat{K}_N g^{-1}$. Haar measure on $\mathrm{GL}_n^*(\mathbb{A}_f)$ should be chosen to give measure one to the set $\widehat{J}_{[t]}$, and the function χ^p in equation (9.8.1) should be replaced by the characteristic function ${}^{[t]}\chi^p$ on $\mathrm{GSp}_{2n}(\mathbb{A}_f^p)$ of the set $g\widehat{K}_N^p g^{-1}$.

9.10. Kottwitz integral. If we drop the involutions and real structures in the preceding sections then the same procedure as Proposition 9.4 identifies the number of isomorphisms classes of Φ_ε-positive principally polarized Deligne modules with level N structure ($N \geq 3$ and $p \nmid N$) that are $\mathbb{Q}$-isogenous to (T_0, γ, ω_0) with the set $Z_\gamma(\mathbb{Q})\backslash Y$ where Y denotes the set of pairs $(\widehat{L}, \alpha)$ consisting of a lattice $\widehat{L} \subset \mathbb{A}_f^{2n}$, symplectic up to homothety and preserved by γ and by $q\gamma^{-1}$, and a level N structure α. As in [36] this gives:

$$|Z_\gamma(\mathbb{Q})\backslash Y| = \mathrm{vol}(Z_\gamma(\mathbb{Q})\backslash Z_\gamma(\mathbb{A}_f)) \cdot \mathcal{O}_\gamma^p \cdot \mathcal{O}_{\gamma,p}$$

where

$$\mathcal{O}_\gamma^p = \int_{Z_\gamma(\mathbb{A}_f^p)\backslash G(\mathbb{A}_f^p)} f^p(g^{-1}\gamma g)dg \tag{9.10.1}$$

and

$$\mathcal{O}_{\gamma,p} = \int_{Z_\gamma(\mathbb{Q}_p)\backslash G(\mathbb{Q}_p)} f_p(g^{-1}\gamma g)dg = \int_{Z_\gamma(\mathbb{Q}_p)\backslash G(\mathbb{Q}_p)} \chi_p(g^{-1}\alpha_q^{-1}\gamma g)dg \tag{9.10.2}$$

where f^p is the characteristic function on $G(\mathbb{A}_f^p)$ of $\widehat{K}_N^p$, and f_p is the characteristic function on $G(\mathbb{Q}_p)$ of $K_p \left(\begin{smallmatrix} I & 0 \\ 0 & qI \end{smallmatrix}\right) K_p$, see Lemma 9.6 and §9.10.

10. The counting formula

10.1. Fix a finite field $k = \mathbb{F}_q$ with q elements, and characteristic $p > 0$. Let $N \geq 3$ be a positive integer relatively prime to p. The theorem of R. Kottwitz ([36, 37]) specializes to:

10.2. Theorem. [36, 37] *The number $A(q)$ of principally polarized ordinary Abelian varieties with principal level N structure, over the field $k = \mathbb{F}_q$, is finite and is equal to*

$$\sum_{\gamma_0} \sum_{\gamma \in \mathcal{C}(\gamma_0)} \mathrm{vol}\left(Z_\gamma(\mathbb{Q})\backslash Z_\gamma(\mathbb{A}_f)\right) \cdot \mathcal{O}_\gamma^p \cdot \mathcal{O}_{\gamma,p} \tag{10.2.1}$$

where $\mathcal{O}_\gamma^p$, $\mathcal{O}_{\gamma,p}$ are defined in (9.10.1), (9.10.2).

10.3. Explanation and proof. Rather than start with the general formula of [36] and figure out what it says in the case of ordinary Abelian varieties, we will follow the proof in [36], but apply it to Deligne modules; see also [1, 7]. As discussed in the Introduction the result differs from the formula in [36] in two ways: (1) the invariant $\alpha(\gamma_0; \gamma, \delta)$ does not appear in our formula and (2) the twisted orbital integral in [36] (at p) is replaced by an ordinary orbital integral.

Recall Deligne's embedding $\varepsilon : W(\overline{k}) \to \mathbb{C}$. It determines a CM type Φ_ε on the CM algebra $\mathbb{Q}[F]$ for every Deligne module (T, F). As described in §3 Deligne constructs an equivalence of categories between the category of Φ_ε-positively polarized Deligne modules and the category of polarized ordinary Abelian varieties over k, so we may count Deligne modules (that are Φ_ε-positively polarized) rather than Abelian varieties.

The proof of equation (10.2.1) now follows five remarkable pages (pp. 203-207) in [36]. Roughly speaking the first sum indexes the $\overline{\mathbb{Q}}$-isogeny classes, the second sum indexes the $\mathbb{Q}$-isogeny classes within a given $\overline{\mathbb{Q}}$-isogeny class, and the orbital integrals count the number of isomorphism classes within a given $\mathbb{Q}$-isogeny class.

10.4. The first sum is over rational representatives $\gamma_0 \in \mathrm{GSp}_{2n}(\mathbb{Q})$, one from each $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$-conjugacy class of semisimple elements such that the characteristic polynomial of γ_0 is an ordinary Weil q-polynomial (see Appendix A). Let $\mathcal{C} \subset \mathrm{GSp}_{2n}(\mathbb{Q})$ denote the $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$-conjugacy class of γ_0 within $\mathrm{GSp}_{2n}(\mathbb{Q})$. The first sum could equally well be considered as a sum over such conjugacy classes.

By Proposition 3.12, the set $\mathcal{C} \subset \mathrm{GSp}_{2n}(\mathbb{Q})$ contains elements that are *viable* with respect to the CM type Φ_ε (cf. §3.11), and the set of such Φ_ε-viable elements constitute the intersection of $\mathcal{C}$ with a unique $\mathrm{Sp}_{2n}(\mathbb{R})$ conjugacy class. Therefore we may (and do) choose the representative $\gamma_0 \in \mathcal{C}$ to be Φ_ε-viable.

By Proposition 6.2, the choice of conjugacy class $\mathcal{C}$ corresponds to a $\overline{\mathbb{Q}}$-isogeny classes of polarized Deligne modules. In fact, according to Lemma 6.3, since $\gamma_0 \in \mathcal{C}$ is Φ_ε-viable, there exists a polarized Deligne module of the form $(L_1, \gamma_0, \omega_0)$ where $L_1 \subset \mathbb{Q}^{2n}$ is a lattice such that

(a) L_1 is preserved by γ_0 and by $q\gamma_0^{-1}$ and
(b) the standard symplectic form ω_0 takes integral values on L_1.

The next step is to decompose the set of Φ_ε-viable elements in $\mathcal{C}$ into $\mathrm{GSp}_{2n}(\mathbb{Q})$ conjugacy classes. Thus, the second sum is over representatives $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$, one from each $\mathrm{GSp}_{2n}(\mathbb{Q})$-conjugacy class of elements such that

(1) γ, γ_0 are $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$-conjugate (i.e., $\gamma \in \mathcal{C}$) and
(2) γ, γ_0 are $\mathrm{Sp}_{2n}(\mathbb{R})$-conjugate (i.e., γ is Φ_ε-viable).

Fix such an element γ. As explained in §8.3 (and Proposition 8.2) this choice of γ for the second sum corresponds to the choice of a $\mathbb{Q}$-isogeny class of Φ_ε-positively polarized Deligne modules within the $\overline{\mathbb{Q}}$-isogeny class of $(L_1, \gamma_0, \omega_0)$. The chosen element γ arises from some (not necessarily principally) Φ_ε-positively polarized Deligne module, say, (T_0, γ, ω_0) where $T_0 \subset \mathbb{Q}^{2n}$ is a lattice that also satisfies (a) and (b) above.

The set of isomorphism classes of Φ_ε-positive principally polarized Deligne modules within the $\mathbb{Q}$-isogeny class of (T_0, γ, ω_0) is identified, using Proposition 9.4 (cf. §9.10), with the quotient $Z_\gamma(\mathbb{Q})\backslash Y$, where $Z_\gamma(\mathbb{Q})$ is the centralizer of γ in $\mathrm{GSp}_{2n}(\mathbb{Q})$ and where Y denotes the set of pairs $(\widehat{L}, \alpha)$ consisting of a lattice $\widehat{L} \subset \mathbb{A}_f^{2n}$ and a level N structure α, satisfying (9.3.1) and (9.3.2), that is, $\widehat{L}$ is a lattice that is *symplectic up to homothety* (see §D.4) and is preserved by γ and by $q\gamma^{-1}$, and the level structure is compatible with γ and with the symplectic structure. Decomposing the lattice $\widehat{L}$ into its adèlic components gives a product decomposition $Y \cong Y^p \times Y_p$ as described in Proposition 9.8 and §9.10. This in turn leads to the product of orbital integrals in equation (10.2.1).

Although the second sum in (10.2.1) may have infinitely many terms, only finitely many of the orbital integrals are non-zero. This is a consequence of Theorem 7.1, or of the more general result in [35] Prop. 8.2. This completes the proof of Theorem 10.2. □

10.5. Counting real structures. Let τ_0 be the standard involution on $\mathbb{Q}^n \oplus \mathbb{Q}^n$ (see Appendix B). For $g \in \mathrm{GSp}_{2n}$ let $\tilde{g} = \tau_0 g \tau_0^{-1}$. Define $H = \mathrm{GL}_n^* \cong \mathrm{GL}_1 \times \mathrm{GL}_n$ to be the fixed point subgroup of this action, as in §5.4. If $\gamma \in \mathrm{GSp}_{2n}$ denote its H-centralizer by

$$S_\gamma = \{x \in \mathrm{GL}_n^* \mid x\gamma = \gamma x\}\,.$$

Assume the level $N \geq 3$ is even (cf. §9.9) and not divisible by p. Let χ^p denote the characteristic function of $\widehat{K}_N^p$ and let χ_p denote the characteristic function of $K_p = \mathrm{GSp}_{2n}(\mathbb{Z}_p)$.

10.6. Theorem. *The number of isomorphism classes of principally polarized ordinary Abelian varieties with real structure is finite and is equal to:*

$$\sum_{A_0} \sum_{C} \left|\widehat{H}^1\right| \mathrm{vol}\left(S_\gamma(\mathbb{Q})\backslash S_\gamma(\mathbb{A}_f)\right) \int_{S_\gamma(\mathbb{A}_f)\backslash H(\mathbb{A}_f)} \chi^p(x^{-1}\gamma x)\chi_p(x^{-1}\alpha_q^{-1}\gamma x)dx. \tag{10.6.1}$$

10.7. Explanation and proof. As in Theorem 10.2 the first sum indexes the $\overline{\mathbb{Q}}$-isogeny classes, the second sum indexes $\mathbb{Q}$-isogeny classes within a given $\overline{\mathbb{Q}}$-isogeny class, and the orbital integrals count the number of isomorphism classes within a $\mathbb{Q}$-isogeny class.

The first sum is over representatives, one from each $\mathrm{GL}_n(\mathbb{Q})$-conjugacy class (which is the same as the $\mathrm{GL}_n(\overline{\mathbb{Q}})$ conjugacy class) of semisimple elements $A_0 \in \mathrm{GL}_n(\mathbb{Q})$ whose characteristic polynomial $h(x) = b_0 + b_1 x + \cdots + x^n \in \mathbb{Z}[x]$ satisfies (see Appendix A)

(h1) $b_0 \neq 0$ and $p \nmid b_0$

(h2) the roots $\beta_1, \beta_2, \cdots, \beta_n$ of h are totally real and $|\beta_i| < \sqrt{q}$ for $1 \leq i \leq n$.

By Proposition 6.2 the terms in this sum correspond to $\overline{\mathbb{Q}}$-isogeny classes of Φ_ε-positively polarized Deligne modules with real structure.

Fix such an element $A_0 \in \mathrm{GL}_n(\mathbb{Q})$. By Proposition 5.8 there exist C_0 so that the element

$$\gamma_0 = \begin{pmatrix} A_0 & B_0 \\ C_0 & {}^tA_0 \end{pmatrix} \in \mathrm{GSp}_{2n}(\mathbb{Q})$$

(where $B_0 = (qI - A_0^2)C_0^{-1}$) is q-inversive (§5) and viable (§3.11) with respect to the CM type Φ_ε. (Viability corresponds to an appropriate choice of signature $\mathrm{sig}(A_0; C_0)$, cf. §5.8.) Then γ_0 corresponds to some Φ_ε-positively polarized Deligne module with real structure which (by Lemma 6.3) may be taken to be of the form $(L_1, \gamma_0, \omega_0, \tau_0)$ where $L_1 \subset \mathbb{Q}^{2n}$ is a lattice that is preserved by τ_0 and by γ_0 and $q\gamma_0^{-1}$.

The second sum in (10.6.1) is over representatives $C \in \mathrm{GL}_n(\mathbb{Q})$, one from each $Z_{\mathrm{GL_n}(\mathbb{Q})}(A_0)$-congruence class (§5.4) of matrices such that

(1) C is symmetric and nonsingular

(2) $A_0 C = C\,{}^tA_0$

(3) $\mathrm{sig}(A_0; C) = \mathrm{sig}(A_0; C_0)$ (cf. §5.4).

According to Proposition 8.2, the elements in this sum correspond to $\mathbb{Q}$-isogeny classes of Φ_ε-positively polarized Deligne modules with real structure that are in the same $\overline{\mathbb{Q}}$-isogeny class as $(L_1, \gamma_0, \omega_0, \tau_0)$. Let us fix such an element C and let $\gamma = \begin{pmatrix} A_0 & B \\ C & {}^tA \end{pmatrix}$ be the corresponding element from Proposition 8.2 (where $B = (A_0^2 - qI)C^{-1}$). Then γ is q-inversive and viable and it corresponds to some Φ_ε-positively polarized Deligne module with real structure, say $(T_0, \gamma, \omega_0, \tau_0)$ which we will use as a "basepoint" in the $\mathbb{Q}$-isogeny class determined by A_0, B.

(In fact, the first two sums may be replaced by a single sum over $\mathrm{GL}_n(\mathbb{Q})$-conjugacy classes of semisimple elements $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ that are q-inversive, whose characteristic polynomial is an ordinary Weil q-polynomial, and that are Φ_ε-viable.)

According to Proposition 9.4 the isomorphism classes of Φ_ε-positive principally polarized Deligne modules with real structure and level N structure that are $\mathbb{Q}$-isogenous to $(T_0, \gamma, \omega_0, \tau_0)$ correspond

to isomorphism classes of pairs $(\widehat{L}, \alpha)$ (consisting of a lattice $\widehat{L} \subset \mathbb{A}_f^{2n}$ and a level structure) that satisfy (9.3.0), (9.3.1) and (9.3.2). In Proposition D.7 these lattices are divided into cohomology classes $[t] \in \widehat{H}^1 = H^1(\langle\tau_0\rangle, \widehat{K}_N^0)$. Each cohomology class provides the same contribution, which accounts for the factor of $|\widehat{H}^1|$. The number of isomorphism classes of pairs $(\widehat{L}, \alpha)$ corresponding to each cohomology class is proven, in Proposition 9.8, to equal the value of the orbital integral in equation (10.6.1). This completes the proof of equation (10.6.1).

The second sum in equation (10.6.1) (that is, the sum over C) may have infinitely many terms. However it follows from Theorem 7.1 that only finitely many of those terms give a non-zero contribution to the sum. This completes the proof of equation (10.6.1).

11. Totally real lattice modules

11.1. Suppose (T, F, τ) is a Deligne module of rank $2n$ over $\mathbb{F}_q$ with a real structure. The fixed point set or "real sublattice" $L = T^\tau$ has an interesting endomorphism[10] $A = (F + V)|L$, in which case the characteristic polynomial of A is $h(2x)$ where $h(x)$ is the real counterpart to the characteristic polynomial of F, cf. §5.1. Although it is not required for the rest of this paper it is interesting to examine these structures in more detail.

If $\alpha : T/NT \to (\mathbb{Z}/N\mathbb{Z})^{2n}$ is a level N structure that is compatible with τ then its restriction to the fixed point set $\beta : L/NL \to (\mathbb{Z}/N\mathbb{Z})^n$ is a level N structure on (L, A). Thus, the category of Deligne modules (resp. with level N structure) fibers over a "totally real" category of lattices and endomorphisms (resp. with level N structure):

11.2. Definition. A totally real lattice module (of rank n and Norm q) is a pair (L, A) where L is a free Abelian group of rank n and $A : L \to L$ is a semisimple endomorphism whose eigenvalues α are totally real algebraic integers with $|\rho(\alpha)| \leq \sqrt{q}$ for every embedding $\rho : \mathbb{Q}[\alpha] \to \mathbb{R}$. The module (L, A) is *ordinary* if $|\rho(\alpha)| < \sqrt{q}$ (for all eigenvalues α and all embeddings ρ) and $\det(A)$ is not divisible by p (cf. Proposition A.3). A level N structure on (L, A) is an isomorphism $\beta : L/NL \to (\mathbb{Z}/N\mathbb{Z})^n$ such that $\beta \circ \overline{A} = \beta$ where $\overline{A} = A \pmod N$. A polarization (resp. principal polarization) of (L, A) is a symmetric bilinear form $R : L \times L \to \mathbb{Z}$ that is nonsingular over $\mathbb{Q}$ (resp. over $\mathbb{Z}$) such that $\mathbb{Q}[A]$ acts as an algebra of self adjoint operators on $L \otimes \mathbb{Q}$.

If $h(x)$ is the characteristic polynomial of an ordinary totally real lattice module then $h(2x)$ is an ordinary real Weil q-polynomial (cf. Appendix A).

11.3. Proposition. *The association $(T, F, \tau) \mapsto (L = T^\tau, A = F + V)$ defines a functor from the category of Deligne modules with real structure to the category of ordinary totally real lattice modules. It becomes an equivalence on the corresponding categories up to $\mathbb{Q}$-isogeny.*

Proof. In both cases the $\mathbb{Q}$-isogeny class is determined by the characteristic polynomial of A (cf. Proposition 6.2 below), so the result follows from Proposition A.3. □

(Similarly, if (T, F, ω, τ) is a Φ_ε-positively polarized Deligne module with real structure then a choice of totally positive imaginary algebraic integer $\iota \in \mathbb{Q}[F]$ determines a positive definite

[10] In this section, our use of the letter A differs by a factor of 2 from our previous use in §5.1 in the matrix representation for F as $\gamma = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right) \in \mathrm{GSp}_{2n}(\mathbb{Q})$ to guarantee that the action of A preserves the lattice $L = T^\tau$.

symmetric bilinear form $R(x,y) = \omega(x, \iota y)$ that takes integer values on $L = T^\tau$ such that $\mathbb{Q}[A]$ acts as an algebra of self adjoint operators on $L \otimes \mathbb{Q}$, thereby determining a polarized totally real lattice module $(L = T^\tau, A = F + V, R(x,y))$. However this procedure does not give an equivalence between the category of polarized Deligne modules and the category of polarized totally real lattice modules.)

11.4. Let $q = p^r$ and fix $n \geq 1$. Let $A \in \mathrm{GL}_n(\mathbb{Q})$ be a semisimple endomorphism whose determinant $\det(A)$ is not divisible by p, whose characteristic polynomial is integral, with roots α that are totally real such that $|\rho(\alpha)| < \sqrt{q}$ for every embedding $\rho : \mathbb{Q}[\alpha] \to \mathbb{R}$. Fix $N \geq 3$ not divisible by p. Let f be the characteristic function of the principal congruence subgroup of level N in $\mathrm{GL}_n(\mathbb{A}_f)$. Using arguments that are similar (but simpler) than those in §10, we find that *the number of isomorphism classes of (ordinary) totally real lattice modules of rank n, Norm q and level N within the $\mathbb{Q}$-isogeny class determined by A is equal to the orbital integral*

$$\int_{Z_A(\mathbb{A}_f)\backslash GL_n(\mathbb{A}_f)} f(x^{-1}Ax)dx.$$

12. Further questions

12.1. We do not know whether the count of the number of "real" polarized Deligne modules has a rational zeta-function interpretation.

12.2. We do not know of a scheme-theoretic interpretation of anti-holomorphic involution that applies to Abelian varieties, rather than to Deligne modules. Consequently we do not know whether the notion of an anti-holomorphic involution makes sense for general Abelian varieties over $\mathbb{F}_q$. It would even be interesting to understand the case of supersingular elliptic curves.

12.3. In [17] the authors showed that certain arithmetic hyperbolic 3-manifolds (and more generally, certain arithmetic quotients of quaternionic Siegel space) can be viewed as parametrizing Abelian varieties with anti-holomorphic multiplication by the integers $\mathcal{O}_d$ in a quadratic imaginary number field. It should be possible to mimic these constructions using Deligne modules. Define an anti-holomorphic multiplication on a Deligne module (T, F) by an order $\mathcal{O}$ in a CM field E to be a homomorphism $\mathcal{O} \to \mathrm{End}(T)$ such that each purely imaginary element $u \in \mathcal{O}$ acts in an anti-holomorphic manner, that is, $uF = Vu$. One could probably count the number of isomorphism classes of principally polarized Deligne modules with level structure and with anti-holomorphic multiplication by $\mathcal{O}$.

Appendix A. Weil polynomials and a real counterpart

A.1. Let π be an algebraic integer. It is *totally real* if $\rho(\pi) \in \mathbb{R}$ for every embedding $\rho : \mathbb{Q}(\pi) \to \mathbb{C}$. It is a *Weil q-integer* if $|\rho(\pi)|^2 = q$ for every embedding $\rho : \mathbb{Q}(\pi) \to \mathbb{C}$. (In this case the field $\mathbb{Q}(\pi)$ is either a CM field, which is the usual case, or it is $\mathbb{Q}(\sqrt{q})$, the latter case occurring iff $\pi = \pm\sqrt{q}$.) A *Weil q-polynomial* is a monic polynomial $p(x) \in \mathbb{Z}[x]$ of even degree, all of whose roots are Weil q-integers. Let us say that a Weil q-polynomial $p(x) = \sum_{i=0}^{2n} a_i x^i$ is *ordinary* if the middle coefficient a_n is nonzero and is coprime to q. This implies that half of its roots in $\overline{\mathbb{Q}}_p$ are p-adic

units and half of its roots are divisible by p; also that $x^2 \pm q$ is not a factor of $p(x)$, hence $p(x)$ has no roots in the set $\{\pm\sqrt{q}, \pm\sqrt{-q}\}$.

The characteristic polynomial of Frobenius associated to an Abelian variety B of dimension n defined over the field $\mathbb{F}_q$ is a Weil q-polynomial. It is ordinary if and only if the variety B is ordinary, cf. §3.

A monic polynomial $p(x) \in \mathbb{Z}[x]$ is *totally real* if all of its roots are totally real algebraic integers. A *real* (resp. *real ordinary*) Weil q-polynomial of degree n is a monic polynomial $h(x) \in \mathbb{Z}[x]$ such that the polynomial $p(x) = x^n h(x + q/x)$ is a Weil q-polynomial (resp. an ordinary Weil q-polynomial). (see also [25, 26]).

A.2. Real counterpart. Let $q \in \mathbb{Q}$. Let us say that a monic polynomial $p(x) = x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_0 \in \mathbb{C}[x]$ is *q-palindromic* if it has even degree and if $a_{n-r} = q^r a_{n+r}$ for $1 \leq r \leq n$, or equivalently if

$$q^{-n}x^{2n}p\left(\frac{q}{x}\right) = p(x).$$

Thus $p(x)$ is q-palindromic iff the following holds: for every root π of $p(x)$ the number $q\pi^{-1}$ is also a root of $p(x)$. It is easy to see that every Weil q-polynomial is q-palindromic but the converse is not generally true. Let

$$p(x) = \prod_{j=1}^{n}(x - \alpha_j)\left(x - \frac{q}{\alpha_j}\right) = \sum_{i=0}^{2n} a_i x^i$$

be a q-palindromic polynomial with no real roots. Define the *associated real counterpart*

$$h(x) = \prod_{j=1}^{n}\left(x - \left(\alpha_j + \frac{q}{\alpha_j}\right)\right) = \sum_{i=0}^{n} b_i x^i$$

or equivalently, $p(x) = x^n h(x + q/x)$.

A.3. Proposition. *Fix $n, q \in \mathbb{Z}$ with $n > 0$ and $q > 0$.*

1. *Let $p(x) = \sum_{i=0}^{2n} a_i x^i \in \mathbb{C}[x]$ be q-palindromic with no real roots and let $h(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{C}[x]$ be its real counterpart. Then $p(x) \in \mathbb{Z}[x]$ if and only if $h(x) \in \mathbb{Z}[x]$.*
2. *A q-palindromic polynomial $p(x) \in \mathbb{Z}[x]$ of even degree is a Weil q-polynomial if and only if the corresponding polynomial $h(x)$ is totally real.*
3. *A totally real polynomial $h(x) \in \mathbb{Z}[x]$ is the real counterpart to a Weil q-polynomial $p(x)$ with no real roots if and only if the roots $\beta_1, \beta_2, \cdots, \beta_n \in \mathbb{R}$ of $h(x)$ satisfy $|\beta_i| < 2\sqrt{q}$ for $i = 1, 2, \cdots, n$.*
4. *A Weil q-polynomial $p(x) \in \mathbb{Z}[x]$ is ordinary if and only if the constant coefficient $h(0) = b_0$ of the real counterpart is nonzero and is coprime to q. In this case, $p(x)$ is irreducible over $\mathbb{Q}$ if and only if $h(x)$ is irreducible over $\mathbb{Q}$.*

Proof. It is clear that $h \in \mathbb{Z}[x]$ implies $p \in \mathbb{Z}[x]$. Let $p(x) = \sum_{k=0}^{2n} a_k x^k \in \mathbb{C}[x]$ be a q-palindromic polynomial with roots $\alpha_i, q/\alpha_i$ for $1 \leq i \leq n$. The real counterpart is $h(x) = \sum_{j=0}^{n} b_j x^j =$

$\prod_{i=1}^n (x-\beta_i)$ where $\beta_i = \alpha_i + q/\alpha_i$, hence

$$p(x) = x^n h\left(x + \frac{q}{x}\right) = \sum_{j=0}^{n} b_j \sum_{t=0}^{j} \binom{j}{t} q^{j-t} x^{n-j+2t}.$$

Set $r = n - j + 2t$. Then $n - j \le r \le n + j$ and $r - (n - j)$ is even, hence

$$p(x) = \sum_{r=0}^{2n} a_r x^r = \sum_{j=0}^{n} \sum_{r=n-j}^{n+j} A_{rj} b_j x^r$$

where

$$A_{rj} = \binom{j}{\frac{r+j-n}{2}} q^{\frac{n-r+j}{2}}$$

provided that $r+j-n$ is even and that $n-j \le r \le n+j$, and $A_{rj} = 0$ otherwise. Then $A_{n+s,s} = 1$ for all $1 \le s \le n$, so the lower half $A_{n+*,*}$ of the matrix A is nonsingular with determinant equal to 1. Let B to be the inverse of the lower half of A. It is an integral matrix and for all $1 \le k \le n$,

$$b_k = \sum_{s=0}^{n} B_{ks} a_{n+s} \in \mathbb{Z}$$

which proves the first part of the Proposition.

To verify statement (2) let $p(x)$ be a Weil q-polynomial. If it has any real roots then they must be of the form $\alpha = \pm\sqrt{q}$ so $\alpha + q/\alpha = \pm 2\sqrt{q}$ which is real. Every pair $\{\alpha, q/\alpha\}$ of complex roots are necessarily complex conjugate hence $\beta = \alpha + q/\alpha$ is real. Since $h(x)$ has integer coefficients this implies that every Galois conjugate of β is also real, hence $h(x)$ is a totally real polynomial. Conversely, given $p(x)$, if the associated polynomial $h(x)$ is totally real then for each root $\beta = \alpha + q/\alpha$ of $h(x)$, the corresponding pair of roots $\{\alpha, q/\alpha\}$ are both real or else they are complex conjugate, and if they are real then they are both equal to $\pm\sqrt{q}$. This implies that $p(x)$ is a Weil q-polynomial.

For part (3) of the proposition, each root $\beta_i \in \mathbb{R}$ of $h(x)$ is a sum $\beta_i = \alpha_i + q/\alpha_i$ of complex conjugate roots of $p(x)$. Hence α_i and q/α_i are the two roots of the quadratic equation

$$x^2 - \beta_i x + q = 0$$

which has real solutions if and only if $\beta_i^2 - 4q \ge 0$. Thus, $p(x)$ has no real roots if and only if $|\beta_i| < 2\sqrt{q}$ for $i = 1, 2, \cdots, n$.

For part (4), the polynomial $p(x)$ is ordinary if and only if exactly one of each pair of roots $\alpha_i, q/\alpha_i$ is a p-adic unit, from which it follows that each $\beta_i = \alpha_i + q/\alpha_i$ is a p-adic unit, hence the product $b_0 = \prod_{i=1}^n \beta_i$ is a p-adic unit (and it is nonzero). Conversely, if b_0 is a p-adic unit then so is each β_i so at least one of the elements in each pair $\alpha_i, q/\alpha_i$ is a unit. But in [24, 10] it is shown that this implies that exactly one of each pair of roots is a p-adic unit, so $p(x)$ is ordinary. The irreducibility statement follows from the formula $p(x) = x^n h(x + q/x)$. □

A.4. Lemma. *Let $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ with multiplier $q \in \mathbb{Q}$. Then the characteristic polynomial $p(x)$ of γ is q-palindromic.*

Using the Jordan decomposition $\gamma = \gamma_s\gamma_u$ into semisimple and unipotent factors, it suffices to consider the case that γ is semisimple, so it can be diagonalized over $\overline{\mathbb{Q}}$, $\gamma = \left(\begin{smallmatrix} D & 0 \\ 0 & D' \end{smallmatrix}\right)$ where D and D') are diagonal matrices with $DD' = qI$ and entries $d_i' = q/d_i$. So $p(x) = \prod_{i=1}^n (x^2 - 2\alpha_i x + q)$ (where $\alpha_i = \frac{1}{2}(d_i + q/d_i)$) is a product of q-palindromic polynomials. □

A.5. Proposition. *Let $p(x) = \sum_{i=0}^{2n} a_i x^i \in \mathbb{Q}[x]$ be a q-palindromic polynomial of degree $2n$ with no roots in the set $\{\pm\sqrt{q}, \pm\sqrt{-q}\}$. Then there exists a q-inversive element $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$ with multiplier q, whose characteristic polynomial is $p(x)$. Moreover, γ may be chosen to be semisimple, in which case it is uniquely determined up to conjugacy in $\mathrm{GSp}_{2n}(\overline{\mathbb{Q}})$ by its characteristic polynomial $p(x)$.*

Proof. Let $\lambda_1, \cdots, \lambda_n, \frac{q}{\lambda_1}, \cdots, \frac{q}{\lambda_n}$ denote the roots of $p(x)$. By assumption λ_j and $\frac{q}{\lambda_j}$ are distinct and their sum is nonzero. Factor the polynomial

$$p(x) = \prod_{i=1}^n (x - \lambda_i)\left(x - \frac{q}{\lambda_i}\right) = \prod_{i=1}^n \left(x^2 - (\lambda_i + \frac{q}{\lambda_i})x + q\right),$$

set $\alpha_i = \frac{1}{2}(\lambda_i + q/\lambda_i)$ and define

$$h(x) = \prod_{i=1}^n (x - \alpha_i) = -h_0 - h_1 x - \cdots - h_{n-1}x^{n-1} + x^n.$$

(For convenience in this section, the signs of the coefficients of $h(x)$ have been modified from that of the preceding section.) The desired element is $\gamma = \left(\begin{smallmatrix} A & B \\ C & {}^tA \end{smallmatrix}\right)$ where the matrices A, B, C are defined as follows. The matrix A is the companion matrix for the polynomial $h(x)$, that is,

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & h_0 \\ 1 & 0 & 0 & \cdots & 0 & h_1 \\ 0 & 1 & 0 & \cdots & 0 & h_2 \\ 0 & 0 & 1 & \cdots & 0 & h_3 \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 & h_{n-1} \end{pmatrix}.$$

It is nonsingular (but not necessarily semisimple unless the roots of $h(x)$ are distinct). Now define

$$B = \begin{pmatrix} & & & & h_0 & 0 \\ & & & h_0 & h_1 & 0 \\ & & h_0 & h_1 & h_2 & 0 \\ & & & \cdots & & \\ h_0 & h_1 & h_2 & \cdots & h_{n-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Then B is symmetric and nonsingular, and one checks directly that $AB = B\,{}^tA$. Define $C = B^{-1}\left(A^2 - qI\right)$ so that $A^2 - BC = qI$. These conditions guarantee that $\gamma \in \mathrm{GSp}_{2n}(\mathbb{Q})$, its multiplier is q, and it is q-inversive. Since the characteristic polynomial of A is $h(x)$, Lemma 5.2 implies that the characteristic polynomial of γ is $p(x)$.

If the roots of $p(x)$ are distinct then this element γ is semisimple. However if $p(x)$ has repeated roots it is necessary to proceed as follows. Factor $h(x) = \prod_{j=1}^r h_j^{m_j}(x)$ into its irreducible factors over $\mathbb{Q}$. This corresponds to a factorization $p(x) = \prod_{j=1}^r p_j^{m_j}(x)$ into q-palindromic factors. Take $A = \mathrm{diag}(A_1^{\times m_1}, \cdots, A_r^{\times m_r})$ to be a block-diagonal matrix with m_j copies of the matrix A_j. Then B, C will also be block-diagonal matrices, and γ will be the corresponding product of q-inversive symplectic matrices γ_j. It suffices to show that each nonzero γ_j is semisimple. Since $h_j(x)$ is irreducible over $\mathbb{Q}$, its roots are distinct, and the roots of $p_j(x)$ are the solutions to $x^2 - 2\alpha x + q = 0$ where $h_j(\alpha) = 0$. If $\pm\sqrt{q}$ is not a root of $h_j(x)$ then the roots of $p_j(x)$ are distinct, hence γ_j is semisimple. If $\pm\sqrt{q}$ is a root of $h_j(x)$ then $p(x) = (x - \sqrt{q})^2$ or $p(x) = (x^2 - q)^2$ depending on whether or not $\sqrt{q} \in \mathbb{Q}$. In the first case we may take $A_j = \sqrt{q}$; $B_j = C_j = 0$ and in the second case we may take $A_j = \left(\begin{smallmatrix} 0 & 1 \\ q & 0 \end{smallmatrix}\right)$; $B_j = C_j = 0$. □

Appendix B. The symplectic group and its involutions

B.1. Let R be a commutative ring (with 1) and let T be a free, finite dimensional R module. Let us say that an alternating form $\omega : T \times T \to R$ is *strongly non-degenerate*, if the induced mapping $\omega^\sharp : T \to \mathrm{Hom}_R(T, R)$ is an isomorphism[11]. Denote by $\mathrm{GSp}(T, \omega)$ the set of $g \in \mathrm{GL}(T)$ such that $\omega(gx, gy) = \lambda\omega(x, y)$ for some $\lambda = \lambda(g) \in R^\times$. Then λ is a character of $\mathrm{GSp}(T, \omega)$ and we say that $g \in \mathrm{GSp}(T, \omega)$ has *multiplier* $\lambda(g)$. The *standard symplectic form* on $T = R^{2n}$ is

$$\omega_0(x, y) = {}^t x J y \quad \text{where} \quad J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}. \tag{B.1.1}$$

If $\omega : T \times T \to R$ is a symplectic form then a *symplectic basis* of T is an isomorphism $\Phi : T \to R^{2n}$ which takes ω to the standard symplectic form ω_0. By abuse of notation we will write

$$\mathrm{GSp}_{2n}(R) = \mathrm{GSp}(R^{2n}, \omega_0) = \mathrm{GSp}(R^{2n}, J)$$

for the group of automorphisms of R^{2n} that preserve the standard symplectic form. If $\gamma \in \mathrm{GSp}_{2n}(R)$ then so is ${}^t\gamma^{-1}$, hence ${}^t\gamma$ is also. In this case, expressing γ as a block matrix, $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ the symplectic condition ${}^t\gamma J \gamma = qJ$ is equivalent to either of the following:

$${}^tAC,\ {}^tBD \ \text{ are symmetric, and } {}^tAD - {}^tCB = qI \tag{B.1.2}$$

$$A\,{}^tB, C\,{}^tD \ \text{ are symmetric, and } A\,{}^tD - B\,{}^tC = qI. \tag{B.1.3}$$

B.2. Lemma. *Let R be a principal ideal domain and let $\omega : T \times T \longrightarrow R$ be a strongly non-degenerate symplectic form. Then T admits a symplectic basis. If $L', L'' \subset T$ are Lagrangian submodules such that $T = L' \oplus L''$ then the basis may be chosen so that L' and L'' are spanned by basis elements.*

Proof. Since ω is strongly non-degenerate there exist $x_1, y_1 \in T$ so that $\omega(x_1, y_1) = 1$. Let T_1 denote the span of x_1, y_1. Then $T = T_1 \oplus T_1^\perp$ because $T_1 \cap (T_1)^\perp = 0$ and for $v \in T$ we have that $u = v - \omega(v, y_1)x_1 - \omega(v, x_1)y_1 \in (T_1)^\perp$. So, T_1 and $T_1^\perp$ are projective, hence free, and ω is strongly non-degenerate on T_1. If $\dim(T) = 2$ we are done, otherwise strong nondegeneracy implies that ω

[11] If R is an integral domain then an alternating form $B : T \times T \to R$ is *weakly non-degenerate* if $\omega^\sharp \otimes K$ is an isomorphism, where K is the fraction field of R.

induces an isomorphism

$$T_1 \oplus T_1^\perp \cong \mathrm{Hom}(T,R) \cong \mathrm{Hom}(T_1,R) \oplus \mathrm{Hom}(T_1^\perp, R).$$

Then $\omega|T_1$ is also strongly nondegenerate so it has a symplectic basis by induction.

If $T = L' \oplus L''$ is a decomposition into Lagrangian submodules, then the symplectic form induces an isomorphism $L'' \cong \mathrm{Hom}_R(L', R)$. Therefore an arbitrary basis of L' together with the dual basis of L'' will constitute a symplectic basis for T. □

B.3. Let R be a commutative ring. The *standard involution* $\tau_0 : R^{2n} \to R^{2n}$ is $\tau_0 = \left(\begin{smallmatrix} -I_n & 0 \\ 0 & I_n \end{smallmatrix}\right)$. If $g \in \mathrm{GSp}_{2n}(R)$ let $\tilde{g} = \tau_0^{-1} g \tau_0$, cf. §5.4.

B.4. Proposition. *Let R be a principal ideal domain containing 2^{-1}. Let $\tau \in \mathrm{GSp}_{2n}(R)$ be an involution ($\tau^2 = I$) with multiplier -1. Then τ is $\mathrm{Sp}_{2n}(R)$-conjugate to τ_0.*

Proof. Write $T = R^{2n}$. The (standard) symplectic form ω_0 induces an isomorphism

$$T \cong \mathrm{Hom}(T,R) \quad \text{say,} \quad x \mapsto x^\sharp. \tag{B.4.1}$$

Let T_+, T_- be the ± 1 eigenspaces of τ. Since $2^{-1} \in R$, any $x \in T$ may be written

$$x = \frac{x - \tau(x)}{2} + \frac{x + \tau(x)}{2} \in T_- + T_+$$

so $T = T_- \oplus T_+$. Therefore T_-, T_+ are projective, hence free. Apply this splitting to equation (B.4.1) to find

$$\Phi : T_- \oplus T_+ \longrightarrow \mathrm{Hom}(T_-, R) \oplus \mathrm{Hom}(T_+, R). \tag{B.4.2}$$

Since $\omega_0(\tau x, \tau y) = -\omega_0(x,y)$ it follows that $\Phi(x,y) = (y^\sharp, x^\sharp)$, hence $\dim(T_-) = \dim(T_+) = n$ and we obtain an isomorphism $T_+ \cong \mathrm{Hom}(T_-, R)$. With respect to a basis of T_1 and the corresponding dual basis of T_+ the matrix of τ is $\left(\begin{smallmatrix} -I & 0 \\ 0 & I \end{smallmatrix}\right)$. □

The proposition fails if the ring R does not contain $\frac{1}{2}$, in fact we have:

B.5. Lemma. *Let R be a Euclidean domain and let ω_0 be the standard symplectic form on R^{2n}. Let $\tau \in \mathrm{GSp}_{2n}(R)$ be an involution with multiplier equal to -1. Then τ is $\mathrm{Sp}_{2n}(R)$ conjugate to an element*

$$\begin{pmatrix} I & S \\ 0 & -I \end{pmatrix}$$

where S is a symmetric matrix consisting of zeroes and ones which may be taken to be one of the following: if $\mathrm{rank}(S) = r$ is odd then $S = \left(\begin{smallmatrix} I_r & 0 \\ 0 & 0 \end{smallmatrix}\right) = I_r \oplus 0_{n-r}$; if r is even then either $S = I_r \oplus 0_{n-r}$ or $S = H \oplus H \cdots \oplus H \oplus 0_{n-r}$ where $H = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ appears $r/2$ times in the sum.

Proof. There exists a vector $v \in \mathbb{Z}^{2n}$ that is primitive and has $\tau(v) = v$. By a lemma of Siegel (see [14] Satz A5.4) there exists $g \in \mathrm{Sp}_{2n}(R)$ so that $gv = e_1 = (1, 0, \cdots, 0)$.

It follows that τ is $\mathrm{Sp}_{2n}(R)$ conjugate to a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ where

$$A = \begin{pmatrix} 1 & * \\ 0 & A_1 \end{pmatrix}, \quad B = \begin{pmatrix} * & * \\ * & B_1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 \\ 0 & C_1 \end{pmatrix}, \quad D = \begin{pmatrix} -1 & 0 \\ * & D_1 \end{pmatrix}$$

and where $\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in \mathrm{GSp}_{2n-2}(R)$ is an involution with multiplier equal to -1. By induction, the involution τ is therefore conjugate to such an element where $A_1 = I$, B_1 is symmetric, $C_1 = 0$ and $D_1 = -I$. The condition $\tau^2 = I$ then implies that $A = I$, $D = -I$, $C = 0$ and B is symmetric. Conjugating τ by any element $\left(\begin{smallmatrix} I & T \\ 0 & I \end{smallmatrix}\right) \in \mathrm{Sp}_{2n}(R)$ (where T is symmetric) we see that B can be modified by the addition of an even number to any symmetric pair (b_{ij}, b_{ji}) of its entries. Therefore, we may take B to consist of zeroes and ones.

The problem may then be reduced to describing the list of possible symmetric bilinear forms on a $\mathbb{Z}/(2)$ vector space V, which are described in [40] §6.2. □

Appendix C. Positivity and $\mathbb{R}$-isogeny

C.1. Lemma. *Let (T, F) be a Deligne module and let Φ be a CM type on $\mathbb{Q}[F]$ (cf. §3.7). Let ω be a Φ-positive polarization of (T, F). Suppose $\beta \in \mathrm{End}_{\mathbb{Q}}(T, F)$ is a self isogeny that is fixed under the Rosati involution, that is, $\beta' = \beta$ where $\omega(\beta' x, y) = \omega(x, \beta y)$ for all $x, y \in T \otimes \mathbb{Q}$. Then there exists $\alpha \in \mathrm{End}_{\mathbb{Q}}(T, F) \otimes \overline{\mathbb{Q}}$ such that $\beta = \alpha'\alpha$. If $\beta' = \beta$ and β is positive definite then the element α may be chosen to lie in $\mathrm{End}_{\mathbb{Q}}(T, F) \otimes \mathbb{R}$. If ω_1, ω_2 are two Φ-positive polarizations of the same Deligne module (T, F) then there exists an $\mathbb{R}$-isogeny $(T, F, \omega_1) \to (T, F, \omega_2)$ with multiplier equal to 1.*

Proof. (See also [36] p. 206.) As indicated in [45] p. 220, the algebra $\mathrm{End}_{\mathbb{Q}}(T, F) \otimes \mathbb{R}$ is isomorphic to a product of matrix algebras $M_{d\times d}(\mathbb{C})$ such that $\beta' = {}^t\bar{\beta}$. Then $\beta' = \beta$ implies that β is Hermitian so there exists a unitary matrix $U \in M_{d\times d}(\mathbb{C})$ with $\beta = {}^t\bar{U}DU$ where D is a diagonal matrix of real numbers. Choose a square root $\sqrt{D} \in M_{d\times d}(\overline{\mathbb{Q}})$ and set $\alpha = \sqrt{D}U \in \mathrm{End}_{\mathbb{Q}}(T, F) \otimes \overline{\mathbb{Q}}$. Then $\alpha'\alpha = {}^t\bar{U}DU = \beta$ as claimed. Moreover, if β is positive definite then the entries of D are positive real numbers so we may arrange that $\sqrt{D} \in M_{d\times d}(\mathbb{R})$, so $\alpha \in \mathrm{End}_{\mathbb{Q}}(T, F) \times \mathbb{R}$ as claimed.

For the last sentence in the lemma, let $\beta \in \mathrm{End}_{\mathbb{Q}}(T, F)$ be the unique endomorphism so that $\omega_2(x, y) = \omega_1(\beta x, y)$. Then β is fixed under the Rosati involution for the polarization ω_1 because

$$\omega_1(\beta' x, y) = \omega_1(x, \beta y) = -\omega_1(\beta y, x) = -\omega_2(y, x) = \omega_2(x, y) = \omega_1(\beta x, y).$$

Moreover, β is positive definite: if $x \in T \otimes \mathbb{R}$ is an eigenvector of β with eigenvalue t then

$$tR_1(x, x) = R_1(\beta x, x) = \omega_1(\beta x, \iota x) = \omega_2(x, \iota x) = R_2(x, x) > 0$$

in the notation of §3.7. According to the first part of this lemma, there exists $\alpha \in \mathrm{End}_{\mathbb{Q}}(T, F) \otimes \mathbb{R}$ so that $\beta = \alpha'\alpha$, or

$$\omega_2(x, y) = \omega_1(\alpha'\alpha x, y) = \omega_1(\alpha x, \alpha y)$$

which says that α is an $\mathbb{R}$-isogeny which takes ω_1 to ω_2 with multiplier equal to 1. □

Appendix D. Symplectic cohomology

D.1. Nonabelian cohomology. Let R be a commutative ring with 1. As in Appendix B the involution τ_0 of $R^n \times R^n$ is defined by $\tau_0(x, y) = (-x, y)$. Let $\langle\tau_0\rangle = \{1, \tau_0\} \cong \mathbb{Z}/(2)$ denote the group generated by the involution τ_0. For $g \in \mathrm{Sp}(2n, R)$ let $\tilde{g} = \tau_0 g \tau_0^{-1}$. This defines an action of the group $\langle\tau_0\rangle$ on $\mathrm{Sp}(2n, R)$. Let $\Gamma \subset \mathrm{Sp}_{2n}(R)$ be a subgroup that is preserved by this action (that is, $\widetilde{\Gamma} = \Gamma$). Recall that a 1-cocycle for this action is a mapping $f : \langle\tau_0\rangle \to \Gamma$ such that $f(1) = I$

and $f(\tau_0) = g$ where $g\tilde{g} = I$. We may write $f = f_g$ since the mapping f is determined by the element g. Then two cocycles $f_g, f_{g'}$ are cohomologous if there exists $h \in \Gamma$ such that $g' = h^{-1}g\tilde{h}$ or equivalently, such that $g' = \tilde{h}gh^{-1}$. The set of cohomology classes is denoted

$$H^1(\langle\tau_0\rangle, \Gamma).$$

If $\tau \in \mathrm{GSp}_{2n}(R)$ is another involution (meaning that $\tau^2 = I$) with multiplier equal to -1 then $g = \tau\tau_0$ defines a cocycle since $g\tilde{g} = 1$. One easily checks the following.

D.2. Proposition. *Let $\Gamma \subseteq \mathrm{Sp}_{2n}(R)$ be a subgroup that is normalized by τ_0. The mapping $\tau \mapsto \tau\tau_0$ determines a one to one correspondence between the set of Γ-conjugacy classes of involutions (i.e. elements of order 2), $\tau \in \Gamma.\tau_0$ and the cohomology set $H^1(\langle\tau_0\rangle, \Gamma)$.*

D.3. Lattices and level structures. If $L \subset \mathbb{Q}^{2n}$ is a lattice its *symplectic dual* is the lattice

$$L^\vee = \left\{ x \in \mathbb{Q}^{2n} \,|\omega_0(x, y) \in \mathbb{Z} \text{ for all } y \in L \right\}$$

where ω_0 is the standard symplectic form. A lattice $L \subset \mathbb{Q}^{2n}$ is *symplectic* if $L^\vee = L$. A lattice $L \subset \mathbb{Q}^{2n}$ is *symplectic up to homothety* if there exists $c \in \mathbb{Q}^\times$ so that $L^\vee = cL$. In this case the symplectic form $b = c\omega_0$ is integer valued and strongly nondegenerate on L. A lattice $L \subset \mathbb{Q}^{2n}$ is *real* if it is preserved by the standard involution τ_0, in which case write $\tau_L = \tau_0|L$.

Fix $N \geq 1$ and let $\bar{L} = L/NL$. A level N structure on a lattice L is an isomorphism $\alpha : \bar{L} \to (\mathbb{Z}/N\mathbb{Z})^{2n}$. A level N structure α is compatible with an integer valued symplectic form $b : L \times L \to \mathbb{Z}$ if $\alpha_*(b) = \bar{\omega}_0$ is the reduction modulo N of the standard symplectic form ω_0. A level N structure $\alpha : \bar{L} \to \bar{L}_0$ is *real* if it is compatible with the standard involution, that is, if $\bar{\tau}_0\alpha = \alpha\bar{\tau}_L : \bar{L} \to \bar{L}_0$.

D.4. Adèlic lattices. Let $\mathbb{A}_f = \prod'_{v<\infty} \mathbb{Q}_v$ (restricted direct product) denote the finite adèles of $\mathbb{Q}$ and let $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. A $\widehat{Z}$-lattice $\widehat{M} \subset \mathbb{A}_f^{2n}$ is a product $\widehat{M} = \prod_{v<\infty} M_v$ of $\mathbb{Z}_v$-lattices $M_v \subset \mathbb{Q}_v^{2n}$ with $M_v = (\mathbb{Z}_v)^{2n}$ for almost all finite places v. If $\widehat{M} = \prod_{v<\infty} M_v$ is a lattice, its symplectic dual is $\widehat{M}^\vee = \prod_{v<\infty} M_v^\vee$ where

$$(M_v)^\vee = \left\{ x \in \mathbb{Q}_v^{2n} |\ \omega_0(x, y) \in \mathbb{Z}_v \ \text{ for all } y \in M_v \right\}.$$

The lattice $\widehat{M}$ is *symplectic up to homothety* if there exists $\mathfrak{c} \in \mathbb{A}_f^\times$ so that $\widehat{M}^\vee = \mathfrak{c}\widehat{M}$. In this case, there exists $c \in \mathbb{Q}^\times$ (unique, up to multiplication by ± 1) so that $\widehat{M}^\vee = c\widehat{M}$, and the alternating form $b = c\omega_0$ takes $\widehat{Z}$ values on $\widehat{M}$. A lattice $\widehat{M}$ is *real* if it is preserved by the standard involution τ_0.

A level N structure on an adèlic lattice $\widehat{M}$ is an isomorphism $\beta : \widehat{M}/N\widehat{M} \to (\mathbb{Z}/N\mathbb{Z})^{2n}$. It is compatible with a $\widehat{Z}$-valued symplectic form $b : \widehat{M} \times \widehat{M} \to \widehat{Z}$ if $\beta_*(b) = \bar{\omega}_0$ is the reduction modulo N of the standard symplectic form. It is *real* if it commutes with the standard involution τ_0. The following statement is standard, see for example [49] Theorem 1.15:

D.5. Lemma. *Let $L \subset \mathbb{Q}^{2n}$ be a $\mathbb{Z}$-lattice and let $L_v = L \otimes \mathbb{Z}_v$ for each finite place v. Then*

- *$L_v = \mathbb{Z}_v^{2n}$ for almost all $v < \infty$.*
- *$L = \bigcap_{v<\infty}(\mathbb{Q}^{2n} \cap L_v)$.*

- *Given any collection of lattices $M_v \subset \mathbb{Q}_v^{2n}$ such that $M_v = \mathbb{Z}_v^{2n}$ for almost all $v < \infty$, there exists a unique $\mathbb{Z}$-lattice $M \subset \mathbb{Q}^{2n}$ such that $M_v = M \otimes \mathbb{Z}_v$ for all $v < \infty$.*

This correspondence is clearly compatible with symplectic structures, real structures and level structures.

D.6. The cohomology class of a symplectic lattice with "real" structure. Let $L \subset \mathbb{Q}^{2n}$ be a lattice, symplectic up to homothety (say, $L^\vee = cL$ where $c \in \mathbb{Q}$), and suppose that L is preserved by the standard involution $\tau_0 : \mathbb{Q}^{2n} \to \mathbb{Q}^{2n}$, in which case we refer to L as a "real" lattice. Let $\alpha : L/NL \to (\mathbb{Z}/N\mathbb{Z})^{2n}$ be a level N structure that is compatible with the involution (meaning that $\alpha_*(\bar{\tau}) = \bar{\tau}_0$ is the standard involution, where $\tau = \tau_0|L$, and where the bar denotes reduction modulo N) and with the nondegenerate symplectic form $b = c\omega_0$ on L (meaning that $\alpha_*(b) = \bar{\omega}_0$ is the standard symplectic form on $(\mathbb{Z}/N\mathbb{Z})^{2n}$). By the strong approximation theorem, the mapping

$$\mathrm{Sp}_{2n}(\mathbb{Z}) \to \mathrm{Sp}_{2n}(\mathbb{Z}/N\mathbb{Z})$$

is surjective. Together with the symplectic basis theorem (Lemma B.2) (and the fact that α is compatible with $b = c\omega_0$) this implies that there exists $g \in \mathrm{GSp}_{2n}(\mathbb{Q})$ so that $(L, \alpha) = g.(L_0, \alpha_0)$, where $L_0 = \mathbb{Z}^{2n}$ is the standard lattice with its standard level N structure $\alpha_0 : L_0/NL_0 \to (\mathbb{Z}/N\mathbb{Z})^{2n}$. Both the lattice L and the level structure α are compatible with the involution which implies that $(L, \alpha) = g.(L_0, \alpha_0) = \tilde{g}.(L_0, \alpha_0)$ (where $\tilde{g} = \tau_0 g \tau_0^{-1}$). Therefore

$$t = g^{-1}\tilde{g} \in K_N^0 \subset \mathrm{Sp}_{2n}(\mathbb{Q})$$

is a cocycle (with multiplier equal to 1) which lies in the principal congruence subgroup

$$K_N^0 = \ker\left(\mathrm{Sp}_{2n}(\mathbb{Z}) \to \mathrm{Sp}_{2n}(\mathbb{Z}/N\mathbb{Z})\right).$$

Let $[(L, \alpha)] \in H^1(\langle\tau_0\rangle, K_N^0)$ denote the resulting cohomology class.

Similarly, an adèlic lattice $\widehat{L}$, symplectic up to homothety, and preserved by the involution τ_0, together with a level N structure β, (compatible with the involution and with the corresponding symplectic form) determine a cohomology class $[(\widehat{L}, \beta)] \in H^1(\langle\tau_0\rangle, \widehat{K}_N^0)$ where

$$\widehat{K}_N^0 = \ker(\mathrm{Sp}_{2n}(\widehat{\mathbb{Z}}) \to \mathrm{Sp}_{2n}(\mathbb{Z}/N\mathbb{Z})).$$

The following proposition is essentially the same as in [50].

D.7. Proposition. *The resulting cohomology classes $[(L, \alpha)]$ and $[(\widehat{L}, \beta)]$ are well defined. The mapping $L \mapsto \widehat{L} = \prod_v (L \otimes \mathbb{Z}_v))$ determines a one to one correspondence between*

(1) $GL_n^*(\mathbb{Q})$-orbits in the set of such pairs (L, α) that are symplectic up to homothety and compatible with the involution (as above),

(2) $\mathrm{GL}_n^*(\mathbb{A}_f)$-orbits in the set of such pairs $(\widehat{L}, \beta)$ that are symplectic up to homothety and compatible with the involution (as above),

(3) elements of the cohomology set

$$H^1 := H^1(\langle\tau_0\rangle, K_N^0) \cong H^1(\langle\tau_0\rangle, \widehat{K}_N^0). \tag{D.7.1}$$

Proof. The cohomology class $[(L,\alpha)]$ is well defined for, suppose that $(L,\alpha) = h.(L_0,\alpha_0)$ for some $h \in \mathrm{GSp}_{2n}(\mathbb{Q})$. Since L is symplectic up to homothety, the elements g, h have the same multiplier hence $u = g^{-1}h \in K_N^0$. Therefore the cocycle $h^{-1}\tilde{h} = u^{-1}(g^{-1}\tilde{g})\tilde{u}$ is cohomologous to $g^{-1}\tilde{g}$.

Suppose $(L',\alpha') = g'.(L_0,\alpha_0)$ is another lattice with level N structure, with the same cohomology class. Then $(g')^{-1}\tilde{g}' = u^{-1}(g^{-1}\tilde{g})\tilde{u}$ for some $u \in K_N^0$ which implies that the element $h = g'u^{-1}g^{-1}$ is fixed under the involution. Hence $(L',\alpha') = h.(L,\alpha)$ is in the same $\mathrm{GL}_n^*(\mathbb{Q})$ orbit[12] as (L,α).

Similar remarks apply to adèlic lattices. Finally, Lemma D.5 implies that the cohomology sets (D.7.1) may be canonically identified. □

D.8. There is a simple relation between Propositions D.2 and D.7 which identifies the cohomology class of a lattice with a conjugacy class of involutions, as follows. Suppose (L,α) is a "real" symplectic (up to homothety) lattice with a level N structure. Express $(L,\alpha) = g.(L_0,\alpha_0)$ for some $g \in \mathrm{GSp}_{2n}(\mathbb{Q})$. Set $\tau = g^{-1}\tau_0 g = h^{-1}\tau_0 h$ where $h \in \mathrm{Sp}_{2n}(\mathbb{Q})$. Then τ is an involution in $K_N^0.\tau_0$ because $\tau\tau_0$ preserves (L_0,α_0), and the cohomology class of (L,α) coincides with the cohomology class of τ. We remark, moreover, if the cohomology class $[(L,\alpha)] \in H^1(\langle\tau_0\rangle, K_N^0)$ is trivial then the lattice L splits as a direct sum $L = L^+ \oplus L^-$ of ± 1 eigenspaces of τ and α determines a principal level N structure on each of the factors.

D.9. Proposition. *Let R be an integral domain containing $\frac{1}{2}$. Then $H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(R))$ is trivial. If $2|N$ the mapping $H^1(\langle\tau_0\rangle, K_N^0) \to H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\mathbb{Z}))$ is trivial. The cohomology sets*

$$H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\mathbb{Z})) \cong H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\widehat{\mathbb{Z}})) \cong H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\mathbb{Z}_2)) \tag{D.9.1}$$

are isomorphic and have order $(3n+1)/2$ if n is odd, or $(3n+2)/2$ if n is even.

Proof. By Proposition D.2 cohomology classes in $\mathrm{Sp}_{2n}(R)$ correspond to conjugacy classes of involutions with multiplier -1. If $\frac{1}{2} \in R$ then Proposition B.4 says there is a unique such, hence the cohomology is trivial. For the second statement suppose $N \geq 2$ is even. Suppose $\alpha \in \mathrm{Sp}_{2n}(\langle\tau_0\rangle, K_N^0)$ is a cocycle. Then $\alpha\tau_0$ is an involution which, by Lemma B.5 implies that there exists $h \in \mathrm{Sp}_{2n}(\mathbb{Z})$ so that $h^{-1}\alpha\tilde{h} = \left(\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right)$ where B is a symmetric matrix of zeroes and ones. It now suffices to show that $B = 0$ which follows from the fact that $\alpha \equiv I \pmod 2$ and that $h^{-1}\tilde{h} \equiv I \pmod 2$, so $B \equiv 0 \pmod 2$.

The cohomology set $H^1(\langle\tau_0\rangle, \mathrm{Sp}_{2n}(\mathbb{Z}))$ is finite because it may be identified with $\mathrm{Sp}_{2n}(\mathbb{Z})$-conjugacy classes of involutions with multiplier -1 which, by Lemma B.5 corresponds to $\mathrm{GL}_n(\mathbb{Z})$-congruence classes of symmetric $n \times n$ matrices B consisting of zeroes and ones. Summing over the possible ranks $0 \leq r \leq n$ for the matrix B, with two possibilities when r is even and only one possibility when r is odd gives $(3n+1)/2$ for n odd and $(3n+2)/2$ for n even, cf.[40]. Equation (D.9.1) holds since $\frac{1}{2} \in \mathbb{Z}_p$ for p odd. □

References

[1] J. Achter and J. Gordon, Elliptic curves, random matrices and orbital integrals, Pacific J. Math. **287** (2017), 1-24.

[2] A. Adler, Antiholomorphic involutions of analytic families of Abelian varieties, Trans. Amer. Math. Soc. **254** (1979), 69-94

[12] so the orbit of (L,α) is isomorphic to $\Gamma_{(L,\alpha)} \backslash \mathrm{GL}_n^*(\mathbb{Q})$ where $\Gamma_{(L,\alpha)}$ is the stabilizer of (L,α).

[3] A. Andrianov, **Quadratic Forms and Hecke Operators**, Grundlehren der math. **286**, Springer Verlag, Berlin, 1987.

[4] T. Barnet-Lamb, T. Gee, D. Geraghty and R. Taylor, Potential automorphy and change of weight. Ann. Math. **179** (2014), 501-609.

[5] A. Borel, **Introduction aux Groupes Arithmetiques**, Hermann Paris, 1969.

[6] C.-L. Chai, B. Conrad and F. Oort, **Complex Multiplication and Lifting Problems**, Mathematical Surveys and Monographs **195**, American Mathematical Society, Providence R.I., 2013.

[7] L. Clozel, Nombre de points de variétés de Shimura sur un corps fini, Sém. Bourbaki 1992-93 exp. **736**, 121-149.

[8] H. Comessatti, Sulla varietà abeliane reali I & II. Ann. Math. Pura Appl. **2**, 67-106, (1924) and **4**, 27-71 (1926)

[9] M. Demazure, **Lectures on p-Divisible Groups**, Lecture Notes in Mathematics **302**, Springer Verlag, 1972.

[10] P. Deligne, Variétés abéliennes ordinaires sur un corps fini, Inv. Math. **8** (1969), 238-243.

[11] P. Deligne, Letter to Piatetski-Shapiro, March 25, 1973

[12] J. Dieudonné, On the automorphisms of the classical groups. With a supplement by Loo-Keng Hua. Mem. Amer. Math. Soc., **2** (1951).

[13] V.G. Drinfel'd, Coverings of p-adic symmetric domains (Russian). Funkcional. Anal. i. Prilozen. **10** (1976), 29-40.

[14] E. Freitag, **Siegelsche Modulfunktionen**, Grundlehren der Math. **254**, Springer Verlag, Berlin, 1983

[15] E. Goren, **Lectures on Hilbert Modular Varieties and Modular Forms** CRM Monograph Series **14**, American Mathematical Society, Providence R.I., 2002.

[16] M. Goresky and Y.-S. Tai, The moduli space of real Abelian varieties with level structure, Comp. Math. **139** (2003), 1-27.

[17] M. Goresky and Y. S. Tai, Anti holomorphic multiplication and a real algebraic modular variety, J. Diff. Geom. **65** (2003), 513-560.

[18] M. Goresky and Y. S. Tai, Real structures on ordinary Abelian varieties, arXiv:1701.07742

[19] M. Goresky and Y. S. Tai, Real structures on Dieudonné modules, to appear.

[20] B. Gross and J. Harris, Real algebraic curves. Ann. Sci. École Norm. Super, **14**, 157-182 (1981)

[21] M. Harris, K. -W. Lan, R. Taylor and J. Thorne, On the Rigid Cohomology of Certain Shimura Varieties, arXiv:1411.6717.

[22] M. Harris and R. Taylor, **The geometry and cohomology of some simple Shimura varieties**, Annals of Math. Studies 151, Princeton University Press, Princeton N.J., 2001.

[23] C. Hooley, On the representation of a number as a sum of a square and a product, Math. Zeit. **69** (1958), 211–227.

[24] E. Howe, Principally polarized ordinary Abelian varieties over finite fields, Trans. Amer. Math. Soc. **347** (1995), 2361-2401.

[25] E. Howe and K. Lauter, Improved upper bounds for the number of points on curves over finite fields, Annales de l'Institut Fourier (2003) **53**, 1677-1737.

[26] E. Howe and K. Lauter, New methods for bounding the number of points on curves over finite fields, in **Geometry and Arithmetic**, C. Faber, G. Farkas, and R. de Jong, eds., European Mathematical Society, 2012. pp. 173–212. Also: arxiv:1202.6308

[27] L.-K. Hua, On the automorphisms of the symplectic group over any field, Ann. Math. **49** (1948), 739-759.

[28] J. Humphreys, **Conjugacy Classes in Semisimple Algebraic Groups**, Mathematical Surveys and Monographs **43**, American Mathematical Society, Providence RI 1995

[29] J. Humphreys, **Linear Algebraic Groups**, Springer Verlag NY, 1995.

[30] B. Huppert, Isometrien von Vektorraumen I, Archiv Math. (Basel) **35** (1980), 164-176.

[31] A. E. Ingham, Some asymptotic formulae in the theory of numbers, J. London Math. Soc. **2** (1927), 202–208.

[32] N. Katz, Serre-Tate local moduli, in **Algebraic Surfaces, Orsay 1976-78**, Lecture Notes in Mathematics **868**, Springer Verlag 1981, pp. 138-202.

[33] D. Kirby, Integer matrices of finite order, Rend. Mat. 2 (1969) 403-408.

[34] A. Knapp, **Basic Algebra**, **Advanced Algebra**, Birkhauser, Boston MA, 2006, 2007.

[35] R. Kottwitz, Stable trace formula: elliptic singular terms, Math. Ann. **275** (1986), 365-399.

[36] R. Kottwitz, Shimura varieties and λ-adic representations, in **Automorphic Forms, Shimura Varieties, and L-functions**, L. Clozel and J. S. Milne, ed., Academic Press, Boston, 1990, vol 1, p.161-210.
[37] R. Kottwitz, Points on some Shimura varieties over finite fields, Jour. Amer. Math. Soc. **5** (1992), 373-444.
[38] R. Langlands and M. Rapoport, Shimuravarietäten und Gerben, J. Reine Angew. Math. **378** (1987), 113-220.
[39] H. W. Lenstra, A normal basis theorem for infinite Galois extensions, Indag. Math. **47** (1985), 221-228.
[40] R. Lidl and H. Niederreiter, **Encyclopedia of Finite Fields**, Cambridge University Press, New York, 1984.
[41] P. Lundström, Normal bases for infinite Galois ring extensions, Colloq. Math. **79** (1999), 235-240.
[42] W. Messing, **The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes**, Lecture Notes in Mathematics **264**, Springer Verlag, 1972.
[43] J. Milne, Introduction to Shimura varieties, in **Harmonic Analysis, the Trace Formula, and Shimura Varieties**, Clay Math. Proc. **4** (2005), Amer. Math. Soc., Providence R.I.
[44] J. Milne and K.-Y. Shih, The action of complex conjugation on a Shimura variety, Ann. Math. **113** (1981), 569-599.
[45] D. Mumford, **Abelian Varieties**, TATA Institute, 1970, reprinted by American Mathematical Society, Providence R.I., 2012.
[46] N. Nygaard, Construction of some classes in the cohomology of Siegel modular threefolds, Comp. Math. **97** (1995) 173-186
[47] S. Patrikis and R. Taylor, Automorphy and irreducibility of some l-adic representations, Comp. Math. **151** (2015) 207- 229.
[48] R. Pink, **Finite Group Schemes** Lecture Notes, E.T.H. Zurich., 2005.
[49] V. Platonov and A. Rapinchuk, **Algebraic Groups and Number Theory**, Academic Press, San Diego, 1994.
[50] Y. Rohlfs, Arithmetisch definierte Gruppen mit Galoisoperation, Inv. Math. **48** (1978), 185-205.
[51] P. Scholze, On torsion in the cohomology of locally symmetric varieties, Ann. Math. **182** (2015), 945-1066.
[52] G. Shimura, **Abelian Varieties with Complex Multiplication and Modular Functions**, Princeton University Press, Princeton NJ 1998.
[53] G. Shimura and Y. Taniyama, **Complex multiplication of Abelian Varieties and its Applications to Number Theory**, Mathematical Society of Japan, Tokyo, 1961.
[54] G. Shimura, On the real points of an arithmetic quotient of a bounded symmetric domain, Math Ann. **215** (1975), 135-164.
[55] R. Silhol, Real Abelian varieties and the theory of Comessatti. Math. Z. **181**, 345-364 (1982)
[56] M. Seppälä and R. Silhol, Moduli Spaces for Real Algebraic Curves and Real Abelian Varieties, Math. Zeit. **201**, 151-165 (1989)
[57] E. Spence, m-Symplectic Matrices, Trans. Amer. Math. Soc. **170** (1972), pp. 447-457.
[58] V. Srinivas and M. Nori, Appendix to: Varieties in positive characteristic with trivial tangent bundle." by Mehta and Srinivas; Comp. Math. **64** (1987), 191-212.
[59] J. Tate, Classes d'isogénie des varieétés abéliennes sur un corps fini (d'aprex T. Honda), Séminaire Bourbaki **352** (1968/69).
[60] R. Taylor, Automorphy for some l-adic lifts of automorphic mod ℓ representations II, Pub. Math. IHES **108** (2008), 183-239.

Institute for Advanced Study, Princeton NJ

Haverford College, Haverford PA