

ABELIAN SURFACES WITH LEVEL $\sqrt{5}$ STRUCTURE*

J. MANOHARMAYUM†

In this article, we study abelian surfaces with real multiplication by the ring of integers of $\mathbb{Q}(\sqrt{5})$. The $\sqrt{5}$ division points on such an abelian surface will give a representation of the absolute Galois group into $\mathrm{GL}_2(\mathbb{F}_5)$.

Suppose \mathcal{W} is an \mathbb{F}_5 vector space scheme of dimension 2, defined over \mathbb{Q} , together with an alternating non-degenerate pairing $\mathcal{W} \times \mathcal{W} \rightarrow \mu_5$. This is just the same as saying that we are given a two dimensional Galois representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ into $\mathrm{GL}_2(\mathbb{F}_5)$ together with an alternating non-degenerate pairing on the underlying two dimensional vector space, and the determinant of the representation is equal to the cyclotomic character. We fix a splitting field of $x^2 - 5$ over \mathbb{Q} , a root δ of $x^2 - 5$ in our splitting field, and set $\mathcal{O} = \mathbb{Z}(\eta)$ where $\eta = (1 + \delta)/2$. For an abelian variety A , we denote its dual by A^\vee .

By an HB (short for Hilbert-Blumenthal) principally polarised abelian surface over a field K of characteristic 0, we shall mean a triple $(A, \lambda, i)_{/K}$ where

- A is an abelian surface defined over K ,
- $\lambda : A \rightarrow A^\vee$ is a principal polarisation defined over K , and
- $i : \mathcal{O} \rightarrow \mathrm{End}_K(A)$ is an injective homomorphism of rings such that the image is fixed under the Rosati involution. In other words, we have $i(x)^\vee \circ \lambda = \lambda \circ i(x)$ for any $x \in \mathcal{O}$.

Often, we shall simply abbreviate this to A has real multiplication.

From the general theory of abelian varieties and their duals, we have a non-degenerate pairing between $A[\delta]$ and $A^\vee[\delta^\vee]$ for any triple $(A, \lambda, i)_{/K}$ as above. We can thus define a Weil pairing on $A[\delta]$ by using λ and the condition i satisfies (see [SB-T]). Using this, we can define a ‘level $\sqrt{5}$ structure’ on such a triple.

More specifically, by an abelian surface with level \mathcal{W} structure, we shall mean a 4-tuple $(A, \lambda, i, \alpha)_{/K}$ where

- $(A, \lambda, i)_{/K}$ is an HB principally polarised abelian surface, and
- $\alpha : \mathcal{W} \rightarrow A[\delta]$ is an isomorphism of symplectic spaces. That is, under α , the pairing on \mathcal{W} goes to the Weil pairing on $A[\delta]$.

We shall be looking at the moduli space of such 4-tuples over fields of characteristic zero. Because the coarse moduli space exists, we need to check that our objects have no non trivial automorphisms. We can then complete the resulting fine moduli scheme by adding cusps to get a projective surface over \mathbb{Q} , which we denote by $X(\mathcal{W})$, or simply by X . The resulting surface has six singular points corresponding to the cusps. Resolving singularities over \mathbb{Q} (see [Chai]), we get a smooth projective surface which we denote by $\mathbb{X}(\mathcal{W})$, or simply by \mathbb{X} . We shall show the following:

THEOREM A. Let \mathcal{W} be a \mathbb{F}_5 vector space scheme of dimension two over \mathbb{Q} together with a non-degenerate alternating pairing to μ_5 . Then $\mathbb{X}(\mathcal{W})$ is birationally equivalent to the projective plane \mathbb{P}^2 over \mathbb{Q} .

Now let A be an abelian surface over K with real multiplication by \mathcal{O} . Let I be a non trivial ideal of \mathcal{O} . We write $A[I] = \{a \in A(\bar{K}) : i(x)(a) = 0 \text{ for all } x \in I\}$. Here,

*Received February 28, 1999; accepted for publication March 10, 1999.

†Department of Pure Mathematics and Mathematical Statistics, Cambridge University, 16, Mill Lane, Cambridge CB2 1SB, UK (J.Manoharmayum@dpmms.cam.ac.uk). Supported by an IGS, Trinity College, Cambridge.

$A(\bar{K})$ is the set of geometric points of A . $\text{Gal}(\bar{K}/K)$ acts on $A[I]$ thus giving rise to a representation of the Galois group with coefficients in some ring. Note that, as \mathcal{O} is a Principal Ideal Domain, $I = (a)$ for some $a \in \mathcal{O}$ and $A[I]$ is precisely the kernel of the ‘multiplication by a ’ map. When $a \in \mathbb{Z}$, we get a representation of $\text{Gal}(\bar{K}/K)$ into $GL_4(\mathbb{Z}/a\mathbb{Z})$. (We are of course assuming that the characteristic of K is zero). We write $\bar{\rho}_{A,I}$ for the representation we get from $A[I]$ for an ideal I of \mathcal{O} .

For a prime p , we write D_p for a decomposition group at p .

Using Theorem A, we shall show the following result:

THEOREM B. Let $\bar{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_5)$ be a representation of the absolute Galois group of \mathbb{Q} with determinant equal to the cyclotomic character. Let Σ be a finite set of finite primes. Assume that for each $p \in \Sigma$, we are given an HB principally polarised abelian surface (A_p, λ_p, i_p) defined over \mathbb{Q}_p such that $\bar{\rho}|_{D_p} \sim \bar{\rho}_{A_p, \sqrt{5}}$. Further, assume that $\bar{\rho}|_{D_p}$ is reducible and decomposable for all but at most one prime in Σ . Fix a non trivial ideal I of \mathcal{O} .

Then there are infinitely many HB principally polarised abelian surfaces (A, λ, i) over \mathbb{Q} such that

- a) $\bar{\rho}_{A, \sqrt{5}} \sim \bar{\rho}$
- b) $\bar{\rho}_{A,I}|_{D_p} \sim \bar{\rho}_{A_p,I}$ for all $p \in \Sigma$.

We give another formulation of the above theorem:

THEOREM C. Let $\bar{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_5)$ be a representation of the absolute Galois group of \mathbb{Q} with determinant equal to the cyclotomic character. Assume that \mathcal{W} is a given \mathbb{F}_5 vector space scheme of dimension two over \mathbb{Q} together with a non-degenerate alternating pairing to μ_5 which induces the representation $\bar{\rho}$. Let Σ be a finite set of finite primes, and assume that for each $p \in \Sigma$, we are given an HB principally polarised abelian surface (A_p, λ_p, i_p) defined over \mathbb{Q}_p such that $A_p[\sqrt{5}]$ is isomorphic, as symplectic spaces, to $\mathcal{W}_{\mathbb{Q}_p}$. Fix a non trivial ideal I of \mathcal{O} .

Then there are infinitely many HB principally polarised abelian surfaces (A, λ, i) over \mathbb{Q} such that

- a) $A[\sqrt{5}]$ is isomorphic to \mathcal{W} , and
- b) $\bar{\rho}_{A,I}|_{D_p} \sim \bar{\rho}_{A_p,I}$ for all $p \in \Sigma$.

I would like to thank F. Diamond, J. Nekovář and N. I. Shepherd-Barron for many helpful discussions.

Throughout this article, all fields, unless mentioned otherwise, are of characteristic zero. All schemes are assumed to be defined over \mathbb{Q} .

1. The associated moduli space. We fix \mathcal{W} , a two dimensional \mathbb{F}_5 vector space scheme over \mathbb{Q} together with a pairing $\mathcal{W} \times \mathcal{W} \rightarrow \mu_5$ where μ_5 is the kernel of multiplication by 5 on the multiplicative group scheme \mathbb{G}_m . Given such a pair, we shall denote, for $i \in (\mathbb{Z}/5\mathbb{Z})^\times$, the pair consisting of \mathcal{W} and pairing given by the composite $\mathcal{W} \times \mathcal{W} \rightarrow \mu_5 \rightarrow \mu_5$ where the last map is ‘raising to the i -th power’ by $\mathcal{W}(i)$.

We write $\sqrt{5}$ for δ in this section.

Strictly speaking, we need to look at abelian surfaces over a general scheme (defined over $\text{Spec}\mathbb{Q}$) with real multiplication in order to define our moduli space. For details, see [vdGeer] or [Falt-Ch]. But to check that such an object has no non trivial automorphism, we only need to check it for abelian surfaces over a field.

PROPOSITION 1.1. *Let $(A, \lambda, i, \alpha)_K$ be the 4-tuple over K where $(A, \lambda, i)_K$ is an abelian surface with real multiplication over K and $\alpha : \mathcal{W} \rightarrow A[\sqrt{5}]$ is an isomorphism which sends the given pairing on \mathcal{W} to the Weil pairing on $A[\sqrt{5}]$. Then $(A, \lambda, i, \alpha)_K$ has no non trivial automorphism.*

Proof. Let θ be an automorphism of $(A, \lambda, i, \alpha)_K$. We first show that θ^5 is the identity. To see this, note that we have the following exact sequence:

$$0 \rightarrow \ker(\sqrt{5}) \rightarrow A[5] \xrightarrow{\sqrt{5}} \ker(\sqrt{5}) \rightarrow 0 .$$

Thus with respect to a suitable choice of basis for the Tate module $T_5(A)$, we can write θ , modulo 5, as the matrix

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Thus θ^5 acts as the identity on $A[5]$, and hence from this, we conclude that θ^5 is the identity. (See, for example, [Mil].)

The Tate module $T_{(\sqrt{5})}(A) \stackrel{\text{defn}}{=} \varprojlim A[\sqrt{5}^n]$ comes with an action of $\varprojlim \mathcal{O}/(\sqrt{5})^n$. Since the Tate module is torsion free, $T_{(\sqrt{5})}(A)$ is a free $\mathbb{Z}_5(\sqrt{5})$ module of rank 2. Since θ commutes with $\sqrt{5}$, we can view, with respect to a choice of basis, θ as an element of $GL_2(\mathbb{Z}_5(\sqrt{5}))$ whose reduction modulo $\sqrt{5}$ is the identity. Further, recall that the map

$$\text{End}(A) \rightarrow \text{End}(T_p(A))$$

is injective for any prime p different from the characteristic of K .

We are thus led to the following: let $B \in GL_2(\mathbb{Z}_5(\sqrt{5}))$ be such that $B \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\sqrt{5}}$ and $B^5 = \text{Identity}$. Then B is the identity.

To see this, assume that B is not the identity. We can write $B = I + \sqrt{5}^n C$ where $n \geq 1$ and C is not divisible by $\sqrt{5}$. Then

$$B^5 = I + 5\sqrt{5}^n C + 10\sqrt{5}^{2n} C^2 + 10\sqrt{5}^{3n} C^3 + 5\sqrt{5}^{4n} C^4 + \sqrt{5}^{5n} C^5 .$$

We get a contradiction by taking valuations, thus showing the above statement. \square

We thus have the following

COROLLARY 1.2. *The fine moduli space of 4-tuples (A, λ, i, α) exists.*

NOTATION. We denote by $Y(\mathcal{W})$ the resulting fine moduli space.

$Y(\mathcal{W})$ is defined over \mathbb{Q} . As mentioned in the beginning, there is a natural completion of $Y(\mathcal{W})$ over \mathbb{Q} giving a projective surface $X(\mathcal{W})$ over \mathbb{Q} . The resolution of singularities is denoted by $\mathbb{X}(\mathcal{W})$. We note that $\mathbb{X}(\mathcal{W})$ is a smooth projective surface defined over \mathbb{Q} .

Since we have a fine moduli space, there is a universal abelian surface with real multiplication and level structure given by \mathcal{W} . We write $\mathcal{A}(\mathcal{W})_{\text{univ}}$ for the universal abelian surface. Thus given a \mathbb{Q} scheme S and an abelian surface $A_{/S}$ with real

multiplication and level structure given by \mathcal{W} , there are unique morphisms $S \rightarrow Y(\mathcal{W})$, $A \rightarrow \mathcal{A}(\mathcal{W})_{\text{univ}}$ such that the following diagram is cartesian:

$$\begin{array}{ccc} A & \longrightarrow & \mathcal{A}(\mathcal{W})_{\text{univ}} \\ \downarrow & & \downarrow \\ S & \longrightarrow & Y(\mathcal{W}) \end{array}$$

2. Complex points of the moduli space and a Galois involution. We refer to [vdGeer-Hi] for details.

In this and the next section, we let K be the fixed splitting field of $x^2 - 5$ over \mathbb{Q} , and denote by \mathcal{O} its ring of integers. Recall that δ is a fixed root of $x^2 - 5$ in K . Recall that \mathcal{O} is a Principal Ideal Domain (in fact a Euclidean Domain).

Set $\mathfrak{H} = \{z \in \mathbb{C} \text{ such that } \text{Im}(z) > 0\}$, the complex upper half plane. We denote by $\Gamma(\delta)$ the principal congruence subgroup of level δ . That is

$$\Gamma(\delta) = \{A \in SL_2(\mathcal{O}) : A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\delta}\}.$$

Often, we shall just write Γ in place of $\Gamma(\delta)$.

We denote the Galois involution of \mathcal{O} by $'$. This gives us an involution on $GL_2(K)$. We will write $'$ for the involution on $GL_2(K)$ as well. An element of $GL_2(K)$ is said to be totally positive if the determinant of the element is positive for any embedding of K in to \mathbb{R} . We write $GL_2^+(K)$ for the subgroup of totally positive elements.

If we fix an embedding of K into \mathbb{R} , and hence an identification of K with $\mathbb{Q}(\sqrt{5})$, the totally positive elements of $GL_2(K)$ act on the complex upper half plane \mathfrak{H} as linear fractional transformations. We write the action as $A\tau$ for $A \in GL_2^+(\mathbb{Q}(\sqrt{5}))$, $\tau \in \mathfrak{H}$. We have the standard extension of this action to the product of two copies of the upper half plane:

$$A(\tau_1, \tau_2) = (A\tau_1, A'\tau_2) \text{ for } A \in GL_2^+(\mathbb{Q}(\sqrt{5})), (\tau_1, \tau_2) \in \mathfrak{H} \times \mathfrak{H}.$$

We now describe how we can think of $\Gamma \backslash \mathfrak{H} \times \mathfrak{H}$ as the complex points of our moduli space. We have to produce, for each $(\tau_1, \tau_2) \in \mathfrak{H} \times \mathfrak{H}$, a principally polarised abelian variety with real multiplication and distinguished basis for the vector space of $\sqrt{5}$ division points.

We first define an alternating, non-degenerate integral form on $\mathcal{O} \oplus \mathcal{O}$ as follows:

$$E : \mathcal{O} \oplus \mathcal{O} \times \mathcal{O} \oplus \mathcal{O} \longrightarrow \mathbb{Z} \text{ by } E((\alpha_1, \beta_1), (\alpha_2, \beta_2)) = \text{trace}_{K/\mathbb{Q}}(\alpha_1\beta_2 - \alpha_2\beta_1)/\delta.$$

We fix the basis $(\frac{1}{\delta}, 0), (0, \frac{1}{\delta})$ for $\frac{1}{\delta}(\mathcal{O} \oplus \mathcal{O})/\mathcal{O} \oplus \mathcal{O}$.

Now fix, once and for all, an embedding of K which sends δ to the positive square root of 5 in \mathbb{R} .

To each $(\tau_1, \tau_2) \in \mathfrak{H} \times \mathfrak{H}$, we associate the lattice

$$\Lambda(\tau_1, \tau_2) = \{(\alpha\tau_1 + \beta, \alpha'\tau_2 + \beta') : (\alpha, \beta) \in \mathcal{O} \oplus \mathcal{O}\}.$$

We write $E(\tau_1, \tau_2)$ for the pairing on $\Lambda(\tau_1, \tau_2)$ gotten from E by transport of structure. Set

$$\mathcal{A}(\tau_1, \tau_2) \stackrel{\text{defn}}{=} \mathbb{C}^2/\Lambda(\tau_1, \tau_2).$$

The pairing $E(\tau_1, \tau_2)$ extends to give the complex torus $\mathcal{A}(\tau_1, \tau_2)$ the structure of an abelian surface with principal polarisation gotten from $E(\tau_1, \tau_2)$. The embedding of \mathcal{O} into $\text{End}(\mathcal{A}(\tau_1, \tau_2))$ is then given by multiplication component wise along with Galois conjugation: $\alpha(z_1, z_2) = (\alpha z_1, \alpha' z_2)$ for $\alpha \in \mathcal{O}$. Finally a $\sqrt{5}$ level structure is given by the basis for $\sqrt{5}$ -division points

$$\left\{ \left(\frac{1}{\delta}, -\frac{1}{\delta} \right), \left(\frac{\tau_1}{\delta}, -\frac{\tau_2}{\delta} \right) \right\},$$

where now we have identified δ with $\sqrt{5}$.

With this description, the complex points of $Y(\mathcal{W})$ are identified with $\Gamma \backslash \mathfrak{H} \times \mathfrak{H}$.

The complex points of the compactification also can be interpreted as obtained by adding cusps to $\Gamma \backslash \mathfrak{H} \times \mathfrak{H}$. This comes from consideration of the action of Γ on $\mathbb{P}^1(\mathbb{Q}(\sqrt{5}))$. There are six cusps in our case. All of these can be found in [vdGeer] and [vdGeer-Hi].

On $\Gamma \backslash \mathfrak{H} \times \mathfrak{H}$, there is an involution defined by switching the two factors of $\mathfrak{H} \times \mathfrak{H}$. (See [vdGeer].) Our aim is to define, over \mathbb{Q} , an involution on $Y(\mathcal{W})$ which, on complex points, corresponds to the involution given by transposition of the two factors of $\mathfrak{H} \times \mathfrak{H}$.

If we change the embedding of \mathcal{O} in to the endomorphism ring by the Galois involution on \mathcal{O} , then this corresponds to making an identification of δ with $-\sqrt{5}$. Thus the basis for $\sqrt{5}$ division points becomes $\left\{ \left(-\frac{1}{\sqrt{5}}, \frac{1}{\sqrt{5}} \right), \left(-\frac{\tau_1}{\sqrt{5}}, \frac{\tau_2}{\sqrt{5}} \right) \right\}$.

There is an isomorphism $\mathcal{A}(\tau_1, \tau_2) \xrightarrow{\sim} \mathcal{A}(\tau_2, \tau_1)$ gotten from transposing the two factors of $\mathbb{C} \times \mathbb{C}$. We denote this map by \dagger . Thus on the lattices $\Lambda(\tau_1, \tau_2)$, $\Lambda(\tau_2, \tau_1)$, we have $(\alpha\tau_1 + \beta, \alpha'\tau_2 + \beta') \xrightarrow{\dagger} (\alpha'\tau_2 + \beta', \alpha\tau_1 + \beta)$. To ease notation, we shall identify (α, β) with $(\alpha\tau_1 + \beta, \alpha'\tau_2 + \beta')$. Then our map is just $(\alpha, \beta)^\dagger = (\alpha', \beta')$.

We now look at how the embedding of \mathcal{O} into $\text{End}\mathcal{A}$ changes. Let $\alpha \in \mathcal{O}$ and let $(z_1, z_2) \in \mathcal{A}(\tau_1, \tau_2)$. We continue writing \dagger for the resulting isomorphism $\text{End}\mathcal{A}(\tau_1, \tau_2) \longrightarrow \text{End}\mathcal{A}(\tau_2, \tau_1)$. It follows easily that $\alpha^\dagger(z_1, z_2) = (\alpha'z_1, \alpha z_2)$.

Thus as principally polarised abelian surfaces with real multiplication, $\mathcal{A}(\tau_2, \tau_1)$ (with real multiplication as constructed) is the same as the principally polarised abelian surface $\mathcal{A}(\tau_1, \tau_2)$ but with real multiplication given by Galois conjugation of the standard one.

Finally, we need to see how the level structure changes under \dagger . Under \dagger , we have

$$\begin{aligned} \left(\frac{1}{\sqrt{5}}, -\frac{1}{\sqrt{5}} \right) &\longrightarrow \left(-\frac{1}{\sqrt{5}}, \frac{1}{\sqrt{5}} \right), \\ \left(-\frac{\tau_1}{\sqrt{5}}, \frac{\tau_2}{\sqrt{5}} \right) &\longrightarrow \left(\frac{\tau_2}{\sqrt{5}}, -\frac{\tau_1}{\sqrt{5}} \right). \end{aligned}$$

We are now ready to define our involution.

DEFINITION 2.1. For a morphism $\phi : \mathcal{O} \longrightarrow R$ with R a ring (with unit), we define ϕ' to be the composite

$$\mathcal{O} \xrightarrow{\prime} \mathcal{O} \xrightarrow{\phi} R,$$

where \prime is the Galois involution on \mathcal{O} .

DEFINITION 2.2. We define the involution \dagger on $Y(\mathcal{W})$ by its action on 4-tuples:

$$(A, \lambda, i, \alpha)^\dagger \stackrel{\text{defn}}{=} (A, \lambda, i', \alpha).$$

We observe \dagger is defined over \mathbb{Q} . It further extends to an involution, again defined over \mathbb{Q} on $X(\mathcal{W})$ and $\mathbb{X}(\mathcal{W})$.

And, of course, we have already checked

PROPOSITION 2.3. *On $\Gamma(\sqrt{5}) \backslash \mathfrak{H} \times \mathfrak{H}$ the involution \dagger is the one we have been using. That is, we have $\Gamma(\sqrt{5})(\tau_1, \tau_2)^\dagger = \Gamma(\sqrt{5})(\tau_2, \tau_1)$. \square*

REMARK. We could have equally well defined \dagger by

$$(A, \lambda, i, \alpha) \longrightarrow (A, \lambda, i', -\alpha).$$

To see that they give the same involution, simply apply multiplication by -1 on A .

We have the following result:

PROPOSITION 2.4. *The fixed points of \dagger on $X(\mathcal{W})$ lie on a geometrically rational and geometrically irreducible curve.*

The proof is a direct consequence of the above Proposition and the description of fixed points over \mathbb{C} (see [vdGeer] or [Hirz]). \square

DEFINITION 2.5. *We define the diagonal of $\mathbb{X}(\mathcal{W})$ to be the fixed points of the involution \dagger on $\mathbb{X}(\mathcal{W})$. We shall denote it by $D(\mathcal{W})$, or by D if the context is clear.*

3. Rationality of the diagonal. As usual, \mathcal{W} is our fixed vector space scheme over \mathbb{Q} with a fixed alternating, non-degenerate pairing in to μ_5 , and δ is a fixed root of $x^2 - 5$. The Galois involution is defined by

$$(A, \lambda, i, \alpha) \longrightarrow (A, \lambda, i', \alpha).$$

D is the diagonal in $\mathbb{X}(\mathcal{W})$. Our aim is to show the following result:

THEOREM 3.1. *The diagonal D is rational over \mathbb{Q} . That is, D is isomorphic to \mathbb{P}^1 over \mathbb{Q} .*

We know (from [Hirz] for example) that D is indeed isomorphic to \mathbb{P}^1 if we go up to an algebraic closure of \mathbb{Q} .

First we show the following lemma:

LEMMA 3.2. *(A, λ, i, α) is fixed by \dagger if and only if there exists an endomorphism $u : A \longrightarrow A$ with the following properties:*

- a) $u^t = u$ where t is the Rosati involution given by λ ,
- b) u^2 is the identity,
- c) $u \circ \delta = -\delta \circ u$, and
- d) u restricted to $A[\delta]$ is the identity.

Such an endomorphism is unique.

Proof. Note that a morphism $\theta : A \longrightarrow A$ is a morphism of polarised abelian varieties if and only if $\lambda = \theta^\vee \circ \lambda \circ \theta$.

Suppose now that (A, λ, i, α) is fixed by \dagger . Then, by definition, there is an endomorphism u satisfying (c). As it is a morphism of polarised abelian varieties, we must have $u^t \circ u$ equal to the identity morphism. Note that u^2 is an automorphism of (A, λ, i, α) . So (b) holds, and then (a) follows from this.

For the reverse implication, simply note that (a) and (b) implies that u is indeed a morphism of polarised abelian varieties.

To prove uniqueness, let u_1 and u_2 be two endomorphisms having the four properties. We then have $(u_1 \circ u_2) \circ (u_1 \circ u_2)^t = u_1 \circ u_2 \circ u_2^t \circ u_1^t$ – which is the identity. Further, we have $(u_1 \circ u_2) \circ \delta = -u_1 \circ \delta \circ u_2 = \delta \circ (u_1 \circ u_2)$. Hence $u_1 \circ u_2$ is an automorphism of (A, λ, i, α) , and hence it is the identity. Thus we have $u_1 = u_2$. \square

We can thus think of the diagonal as the moduli space for 5-tuples $(A, \lambda, i, \alpha, u)$ where u is an endomorphism satisfying the four conditions of the lemma above.

LEMMA 3.3. *For $(A, \lambda, i, \alpha, u)$, the morphism*

$$A \longrightarrow \text{Image}(1 + u) \times \text{Image}(1 - u)$$

is an isogeny with kernel contained in $A[2]$. Each factor of the product on the right hand side is an elliptic curve.

Proof. We work over \mathbb{C} . Take the abelian surface corresponding to the point $(\tau, \tau) \in \mathfrak{H} \times \mathfrak{H}$. u , as an endomorphism of $\mathbb{C} \times \mathbb{C}$, is simply the matrix $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

The morphism $1 + u$ then corresponds to the map

$$\begin{aligned} \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ (z_1, z_2) &\longrightarrow z_1 - z_2 \end{aligned}$$

Under this, $\Lambda(\tau, \tau)$ goes to the lattice $\mathbb{Z}\sqrt{5}\tau + \mathbb{Z}\sqrt{5}$.

The morphism $1 - u$ corresponds to the map

$$\begin{aligned} \mathbb{C} \times \mathbb{C} &\longrightarrow \mathbb{C} \\ (z_1, z_2) &\longrightarrow z_1 + z_2 \end{aligned}$$

Under this, $\Lambda(\tau, \tau)$ goes to the lattice $\mathbb{Z}\tau + \mathbb{Z}$.

The lemma then follows. \square

LEMMA 3.4. *Under $1 + u$, $A[\delta]$ goes to the subgroup scheme of 5 division points of the elliptic curve $\text{Image}(1 + u)$.*

Proof. Follows again from looking at the corresponding problem over \mathbb{C} . \square

Proof of Theorem. The previous lemma will give us a morphism if we know a bit more about the pairing on the images. Applying the lemma to the pull back of the universal abelian surface over D , we see that we get a rational map, defined over \mathbb{Q} , from D to the modular elliptic curve $X(\mathcal{W}(i))$ for some i . Since both the curves are smooth, the rational map extends to a morphism. On complex points, this morphism is clearly injective. Hence it is an isomorphism. The result then follows from the fact that the modular elliptic curve $X(\mathcal{W}(i))$ is isomorphic over \mathbb{Q} to \mathbb{P}^1 (this can be shown in exactly the same way as Theorem 1.2 of [SB-T]). \square

4. Geometrically rational surfaces over fields of characteristic zero. Let k be a field of characteristic zero. By a surface S over k , we shall mean an integral, geometrically irreducible projective scheme of dimension 2 over k . We denote the canonical sheaf of S by ω_S , or simply by ω . We write K_S for a divisor in the class of the canonical sheaf of a smooth surface S . Again we simply write K for such a divisor

when the context is clear. A divisor D on S gives rise to an invertible sheaf (see [Hart]), which we denote by $\mathcal{L}(D)$. We have, for example, an isomorphism between $\mathcal{L}(D)^{-1}$ and $\mathcal{L}(-D)$. Following the notation of [Hart], we write

$$l(D) = \dim_k H^0(S, \mathcal{L}(D)), \quad s(D) = \dim_k H^1(S, \mathcal{L}(D)).$$

DEFINITION 4.1. *We say that a surface S defined over k is rational, or birationally trivial if there exists a birational map*

$$\phi : S \dashrightarrow \mathbb{P}^2$$

defined over k . We say that S is geometrically rational if $S_{/\bar{k}}$ is rational.

We shall be using the following classical result of Noether and Enriques:

(Enriques-Noether) Assume that k is algebraically closed. Let S be a surface, $p : S \rightarrow C$ a morphism from S to a smooth curve C . Suppose we are given a point $x \in C$ such that p is smooth at x and the fibre at x is isomorphic to \mathbb{P}^1 . Then there exists a Zariski open $U \subset C$ with $x \in U$ such that $p^{-1}U$ is isomorphic to $U \times \mathbb{P}^1$ over U . In other words, there is an isomorphism $p^{-1}U \xrightarrow{\psi} U \times \mathbb{P}^1$ such that $\psi \circ \pi = p|_U$ where $\pi : U \times \mathbb{P}^1 \rightarrow U$ is the projection.

For a proof, see Chapter III of [Beau].

We now prove a result for checking birational triviality of geometrically rational surfaces.

THEOREM 4.2. *Let S be a smooth, projective, geometrically rational surface over k . Let C be a curve in S which is isomorphic to \mathbb{P}^1 over k . Assume that $C^2 = 0$ and that there exists a smooth curve H in S , defined over k , with $C.H = 1$. Then S is birationally trivial.*

Proof. First note, using birational invariance of the geometric and arithmetic genus, that we have $p_a(S) = p_g(S) = 0$. We claim that $l(C) = \dim_k H^0(S, \mathcal{L}(C)) \geq 2$.

To prove the claim, we note, by the adjunction formula, $C.K_S = -2$. Thus by Riemann-Roch, we have $l(C) - s(C) + l(K - C) = 2$. Obviously, for a function f on S , $(f) + K - C \geq 0$ implies $(f) + K \geq 0$. Since $p_g = 0$, we get $l(K - C) = 0$. Finally, since $s(C) \geq 0$, we get $l(C) \geq 2$.

Hence we can find a non constant function g on S , defined over k , such that $(g) + C \geq 0$. In other words, $(g) = D - C$ with D effective. The linear system given by D, C has no base points. For if it did, then we would have, by invariance of intersection numbers under rational equivalence, $0 = C.C = C.D > 0$. Hence g defines a non constant morphism, over k , from S to \mathbb{P}^1 . We write π for this morphism $\pi : S \rightarrow \mathbb{P}^1_k$. Without loss of generality, we may assume that the fibre at $(0 : 1)$ is C .

By generic smoothness (see corollary 10.7, Chapter III of [Hart]), there is a non empty open subset U of \mathbb{P}^1 , defined over k , such that the restriction $\pi|_{\pi^{-1}U} : \pi^{-1}U \rightarrow U$ is smooth. (The result in [Hart] is over an algebraically closed field, but we can then take intersection of the Galois conjugates as there are only finitely many of them.)

We claim that we can assume $(0 : 1) \in U$.

To see this, let $V = U \cup \{(0 : 1)\}$. Consider $\pi|_{\pi^{-1}V} : \pi^{-1}V \rightarrow V$. The restriction is certainly a proper morphism. The restriction $\pi|_{\pi^{-1}V}$ is seen to be flat by checking dimension on each closed fibre. (See corollary to Theorem 23.1 of [Mats]). This further implies that $\pi|_{\pi^{-1}V}$ is smooth (Theorem 10.2, Chapter III in [Hart]).

By the theorem of Enriques-Noether, we can assume $\pi^{-1}V_{/\bar{k}}$ is isomorphic to $V_{\bar{k}} \times \mathbb{P}_{\bar{k}}^1$ over $V_{\bar{k}}$.

Hence we can conclude that the generic fibre of π is a smooth projective curve of genus 0. We need to show that this is in fact \mathbb{P}^1 , and for this we need to produce a section for π . We now show that H gives rise to a section.

For this, we show that $\pi|_H : H \rightarrow \mathbb{P}^1$ is an isomorphism. This morphism is non constant as $C.H = 1$. Now let z be a geometric point in V . Since intersection numbers are unchanged under algebraic equivalence, we see that $\pi^{-1}z.H = C.H = 1$. Hence H intersects such a geometric fibre at exactly one point. Thus $\pi|_H$ is of degree 1, and so an isomorphism. \square

COROLLARY 4.3. *Let S be a smooth, projective, geometrically rational surface over k , and let C be a smooth curve in S such that C is isomorphic to \mathbb{P}^1 over k . Suppose $C^2 \geq 1$. Then S is birationally trivial.*

Proof. We first do the case $C^2 = 1$. Let P be a k -rational point of S lying in C . Let \tilde{S} be the blow up of S at P . We write σ_P for the corresponding birational morphism $\sigma_P : \tilde{S} \rightarrow S$. Denote by \tilde{C} the strict transform of C .

Then \tilde{C} is isomorphic to \mathbb{P}^1 over k as C is smooth at P . Writing E for the corresponding exceptional curve (i.e. $\sigma_P^{-1}(P)$), we have $E \xrightarrow{\sim}_{/k} \mathbb{P}^1$, $E^2 = -1$, $E.\tilde{C} = 1$ (as C is smooth at P). Further, $\sigma_P^*(C) = \tilde{C} + E$. Hence we have

$$\begin{aligned} 1 &= C^2 \\ &= \sigma_P^*(C).\sigma_P^*(C) \\ &= (\tilde{C} + E)(\tilde{C} + E) \\ &= \tilde{C}^2 + 2 - 1. \end{aligned}$$

Thus $\tilde{C}^2 = 0$, and the result in this case follows by applying the above theorem to \tilde{S} .

In the general case, we note that the strict transform of C under blowing up at a k -rational point on the curve has self intersection $C^2 - 1$, and is still isomorphic to \mathbb{P}^1 over k . The result then follows by induction. \square

5. Proof of Theorem A. We now write \mathbb{X} in place of $\mathbb{X}(\mathcal{W})$, X in place of $X(\mathcal{W})$ and Y in place of $Y(\mathcal{W})$. Recall that we have the diagonal D on \mathbb{X} . By Theorem 3.1, we know that D is isomorphic to \mathbb{P}^1 over \mathbb{Q} .

Write K for a divisor in the class of the canonical sheaf $\omega_{\mathbb{X}}$. It is shown in [Hirz] (see the statement numerated as (12) and the paragraph preceding that in [Hirz]) that $-K.D = 4$. By the Adjunction Formula, we have $-2 = D(K + D) = -4 + D^2$, and hence $D^2 = 2$.

From the classification of Hilbert modular surfaces (see [vdGeer]), we know that \mathbb{X} is geometrically rational. **Theorem A** then follows directly from Corollary 4.3. \square

6. Analogue of a result of Hirzebruch. We now describe the structure of our surfaces $X(\mathcal{W})$ and \mathbb{X} over \mathbb{Q} as a double cover of \mathbb{P}^2 ramified along a rational curve with prescribed singularities. All of this is done in [Hirz]. Our result follows from observing that most of the arguments there are valid over \mathbb{Q} as well.

PROPOSITION 6.1. *Let K be a divisor in the class of the canonical sheaf $\omega_{\mathbb{X}}$. Then we have $K^2 = -4$.*

Proof. This is already contained in [Hirz]. The volume of $\Gamma(\sqrt{5}) \backslash \mathfrak{H} \times \mathfrak{H}$ is shown to be 4. The six singularities of X are resolved by cycles of type $(-3, -3)$. The value of K^2 then follows from the formula in chapter 4 of [vdGeer]. \square

The surface X has singularities at geometric points corresponding to the six cusps of $\Gamma(\sqrt{5})$. We have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{X}(\mathcal{W}) & \longrightarrow & X(\mathcal{W}) \\ \downarrow & & \downarrow \\ \mathbb{X}(\mathcal{W})/\dagger & \longrightarrow & X(\mathcal{W})/\dagger \end{array},$$

where \dagger is the Galois involution defined in section 2.

The action of \dagger on the cycles given by resolution of singularities is described in [Hirz]. Hirzebruch shows that the image of each cycle in $\mathbb{X}(\sqrt{5}, \mathcal{W})/\dagger$ is an exceptional curve of the first kind, i.e. a smooth rational curve with self intersection -1 . Further, each of the resulting exceptional curves meets the image of the diagonal D tangentially at two distinct points. Let us call the six exceptional curves E_i . The divisor

$$E = H_1 + H_2 + H_3 + H_4 + H_5 + H_6$$

is defined over \mathbb{Q} , and we have $H_i.H_j = -\delta_{i,j}$. Thus we can blow down the divisor E . The blow down is naturally identified with X/\dagger . From [Hirz], we see that X/\dagger is a smooth surface whose canonical divisor has self intersection 9, and hence it is a Severi-Brauer variety, i.e. a surface which is isomorphic to \mathbb{P}^2 over the algebraic closure. Since the image of $D(\mathcal{W})$ is rational over \mathbb{Q} , X/\dagger contains a geometric point defined over \mathbb{Q} and hence it is isomorphic to \mathbb{P}^2 over \mathbb{Q} .

The images of H_i , $i = 1, \dots, 6$, give us six points in \mathbb{P}^2 which correspond to the images of the six singular points of X . The collection of these six points is defined over \mathbb{Q} . The image of D in \mathbb{P}^2 is a rational curve passing through these six points. From [Hirz], we see that the degree of the image is 10.

Write C for the image of $D(\mathcal{W})$ in \mathbb{P}^2 . Using the fact that \mathbb{P}^2 is the blow down along H_i , or from [Hirz] directly, we see that C is smooth except at the points corresponding to the singular points of X and it has double cusps as singularities there.

Hence we have the following rational analogue of Hirzebruch’s theorem:

THEOREM 6.2. *The quotient $X(\sqrt{5}, \mathcal{W})/\dagger$ of $X(\sqrt{5}, \mathcal{W})$ under the involution \dagger is isomorphic, over \mathbb{Q} , to \mathbb{P}^2 . Under this isomorphism, the singular points of X give a collection of six points defined over \mathbb{Q} . There is a rational curve C over \mathbb{Q} of degree 10 whose singularities are at the six points and which has double cusps as singularities there. C corresponds to the image of the diagonal $D(\mathcal{W})$. Under these identifications, X is a double cover of \mathbb{P}^2 ramified along C .*

7. Proof of Theorem B and and Theorem C. Recall that for \mathcal{W} , we have defined, in section 1, its twists $\mathcal{W}(i)$ where $i \in (\mathbb{Z}/5\mathbb{Z})^\times$. For each twist, we have a fine moduli space $Y(\mathcal{W}(i))$ which we shall shorten to $Y(i)$. We shall write Y instead of $Y(1) = Y(\mathcal{W})$. For each $Y(i)$, we have a universal abelian surface $\mathcal{A}(i)_{\text{univ}}$ with real multiplication together with the right level structure.

LEMMA 7.1. *Let $(A, \lambda, i)_k$ be an abelian surface with real multiplication. Suppose $\bar{\rho}_{A, \sqrt{5}} : \text{Gal}(\bar{k}/k) \longrightarrow \text{Gl}_2(\mathbb{F}_5)$ is reducible and decomposable. Write \mathcal{W} for the vector*

space scheme given by $\sqrt{5}$ division points together with the Weil pairing induced by λ . Then for each $i \in (\mathbb{Z}/5\mathbb{Z})^\times$, there are isomorphisms $\alpha(i) : \mathbb{W}(i) \rightarrow A[\sqrt{5}]$ such that the diagram

$$\begin{array}{ccc} (A, \lambda, i, \alpha(i)) & \longrightarrow & \mathcal{A}(i)_{\text{univ}} \\ \downarrow & & \downarrow \\ \text{Spec}(k) & \longrightarrow & Y(i)_{/k} \end{array}$$

is cartesian.

In other words, there are k -rational points x_i on $Y(i)_{/k}$ such that $(A, \lambda, i, \alpha(i))$ is the fibre at x_i of $\mathcal{A}(i)_{\text{univ}} \rightarrow Y(i)_{/k}$.

Proof. We only need to note that in this case, we can write

$$\mathcal{W} \xrightarrow{\sim} \mathcal{V}_1 \oplus \mathcal{V}_2$$

where \mathcal{V}_1 and \mathcal{V}_2 are one dimensional \mathbb{F}_5 vector space schemes over k . We can thus change the embedding by multiplying, say, on the second factor. \square

LEMMA 7.2. *Let k be a finite extension of \mathbb{Q}_p , and let X be a geometrically irreducible scheme of finite type over k . Suppose Z is a Zariski closed subscheme (with reduced induced structure) such that $X - Z$ is dense. Let \mathcal{U} be a non-empty open admissible set in X^{an} . Then $\mathcal{U} - Z^{\text{an}}$ is non-empty. (Here X^{an} is the rigid analytic space associated to X .)*

Proof. Without loss of generality, we can assume $k = \mathbb{C}_p$, and that X is affine. We need to show the following statement: let $z \in Z^{\text{an}}$ and let \mathcal{U} be an open neighbourhood of z . Then $\mathcal{U} \cap (X - Z)^{\text{an}}$ is non-empty.

This follows because the dimension of z in X^{an} is equal to the Krull dimension of X as X is reduced (see chapter 7 of [BGR]). If $\mathcal{U} \subset Z^{\text{an}}$, this dimension would also be the Krull dimension of Z giving a contradiction. \square

We shall use the following result. The result is Theorem 5.1 of [Kis1] (see also [Kis2]), and we use the same notations as in [Kis1] in our statement.

LOCAL CONSTANCY. Let F be a field of characteristic zero, complete with respect to a non-archimedean valuation and residue characteristic positive. Suppose \mathcal{X} is a rigid space over F , and let L be a local system on \mathcal{X} which is given by a locally constant finite etale sheaf on \mathcal{X} .

For a rational point z of \mathcal{X} , write ρ_z for the corresponding representation of $\text{Gal}(\bar{F}/F)$.

Then for any rational point x of \mathcal{X} , there is a neighbourhood \mathcal{U} of x such that for any rational point y in \mathcal{U} the representations ρ_x and ρ_y are equivalent. \square

By Theorem A, we know that there are Zariski open subsets of $Y(i)$ which are isomorphic to Zariski open, dense subsets of \mathbb{A}^2 . Throughout this section, we fix such an open subset for each $Y(i)$, which we denote by $\mathbb{U}(i)$. We shall write \mathbb{U} in place of $\mathbb{U}(1)$ when \mathcal{W} is understood. We write the pull back of the universal abelian surface $\mathcal{A}(i)_{\text{univ}}$ as $\mathcal{A}(i)_{\mathbb{U}(i)}$. And, of course, $\mathcal{A}_{\mathbb{U}}$ is understood to be the case of $i = 1$.

We now turn to the proof of Theorem B.

Recall that we are given

- A representation $\bar{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_5)$ with determinant the cyclotomic character.

- Σ a finite set of finite primes such that for each $p \in \Sigma$, we have:
 - a) an abelian surface with real multiplication (A_p, λ_p, i_p) defined over \mathbb{Q}_p
 - b) an equivalence of Galois representations $\bar{\rho}|_{D_p} \sim \bar{\rho}_{A_p, \sqrt{5}}$
 - c) $\bar{\rho}|_{D_p}$ is reducible and decomposable for all but one prime p in Σ .

By lemma 7.1 above, we can thus assume that there is a symplectic \mathbb{F}_5 vector space scheme \mathcal{W} of dimension 2 over \mathbb{Q} such that each abelian surface (A_p, λ_p, i_p) lies on Y/\mathbb{Q}_p .

We are interested in the mod I representations $\bar{\rho}_{A_p, I}$. The mod I representations arise from the étale covering of $\mathcal{A}_{\text{univ}}$ obtained by taking kernel of I . By Local constancy and lemma 7.2, we can therefore assume that the (A_p, λ_p, i_p) 's are from \mathbb{Q}_p -rational points of \mathbb{U}/\mathbb{Q}_p . Identifying \mathbb{U} with the Zariski dense, open subset of $\mathbb{A}_{\mathbb{Q}}^2$, we get

- points (a_p, b_p) in $\mathbb{U}_{\mathbb{Q}_p}$ corresponding to (A_p, λ_p, i_p)
- an $\epsilon_p > 0$ such that for each (x_p, y_p) in \mathbb{Q}_p^2 with $\max\{|x_p - a_p|_p, |y_p - b_p|_p\} \leq \epsilon_p$, $(x_p, y_p) \in \mathbb{U}_{\mathbb{Q}_p}(\mathbb{Q}_p)$ and the abelian surface given by the fibre at (x_p, y_p) has the same (equivalent) mod I representation as $\bar{\rho}_{A_p, I}$.

By the weak approximation theorem, we can find infinitely many $(x, y) \in \mathbb{U}(\mathbb{Q})$ such that $\max\{|x - a_p|_p, |y - b_p|_p\} \leq \epsilon_p$ for all $p \in \Sigma$. Taking fibres at such points (x, y) then completes the proof of Theorem B.

Note that the same argument works for Theorem C: in fact, under the hypotheses of Theorem C, all the given abelian surfaces are points on one single component (determined by \mathcal{W}). \square

REFERENCES

- [Beau] A. BEAUVILLE, *Complex Algebraic Surfaces*, LMSLNS 68, Cambridge University Press, Cambridge, 1983.
- [BGR] S. BOSCH, U. GÜNTZER, AND R. REMMERT, *Non-Archimedean Analysis*, Springer-Verlag, Berlin, Heidelberg, 1984.
- [Chai] C.-L. CHAI, *Arithmetic minimal compactification of the Hilbert - Blumenthal moduli spaces*, Annals of Math., 131:3 (1990), pp. 541–554.
- [Fal-Ch] G. FALTINGS AND C.-L. CHAI, *Degeneration of Abelian Varieties*, Springer-Verlag, Berlin, Heidelberg, 1990.
- [vdGeer-Hi] G. V.D. GEER AND F. HIRZEBRUCH, *Lectures on Hilbert Modular Surfaces*, Montreal University Press, Montreal, 1981.
- [vdGeer] G. V.D. GEER, *Hilbert Modular Surfaces*, Springer-Verlag, Berlin, Heidelberg, 1988.
- [Hart] R. HARTSHORNE, *Algebraic Geometry*, GTM 52, Springer-Verlag, New York, 1977.
- [Hirz] F. HIRZEBRUCH, *The ring of Hilbert modular forms for real quadratic fields of small discriminant*, in Modular Functions of One Variable VI, J.-P. Serre and D. B. Zagier, ed., Springer-Verlag, Berlin, Heidelberg, 1977, pp. 287–323.
- [Kis1] M. KISIN, *Local constancy in p -adic families of Galois representations*, Preprint.
- [Kis2] M. KISIN, *Local Constancy in p -adic Families of Galois Representations*, Princeton University Ph.D. thesis.
- [Mats] H. MATSUMURA, *Commutative Ring Theory*, Cambridge studies in advanced mathematics 8, Cambridge University Press, Cambridge, 1986.
- [Mil] J. S. MILNE, *Abelian varieties*, in Arithmetic Geometry, G. Cornell and J. H. Silverman, ed., Springer-Verlag, New York, 1986, pp. 103–150.
- [SB-T] N. I. SHEPHERD-BARRON AND R. TAYLOR, *Mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc., 10 (1997), pp. 283–298.