Chapter 5

The endomorphism algebra

5.1 Endomorphisms of elliptic curves

A *homomorphism* between abelian varieties $f : V/L \to W/M$ is given by a $\mathbb{C}$-linear map $F : V \to W$ such that $F(L) \subseteq M$. This is called an endomorphism if the abelian varieties are the same. Our goal is to study the ring of endomorphisms $End(A)$, of an abelian variety. We start with elliptic curves.

Theorem 5.1.1. *Let $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$, then either*

1. *$End(E) = \mathbb{Z}$ or*
2. *$\mathbb{Q}(\tau)$ is an imaginary quadratic field, and $End(E)$ is an order in $\mathbb{Q}(\tau)$ i.e. a finitely generated subring such that $End(E) \otimes \mathbb{Q} = \mathbb{Q}(\tau)$.*

Proof. Let $L = \mathbb{Z} + \mathbb{Z}\tau$. Then $End(E)$ can be identified with $R = \{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$. For $\alpha \in R$, there are integers ab, c, d such that

$$\alpha = a + b\tau,\ \alpha\tau = c + d\tau$$

By Cayley-Hamilton, or direct calculation, we see that

$$\alpha^2 - (a + d)\tau + ad - bc = 0$$

Therefore R is an integral extension of $\mathbb{Z}$.

Suppose that $R \neq \mathbb{Z}$, and choose $\alpha \in R$ but $\alpha \notin \mathbb{Z}$. Then eliminating α from the previous equations yields

$$b\tau^2 - (a - d)\tau - c = 0$$

Therefore $\mathbb{Q}(\tau)$ is quadratic imaginary and $R \subset \mathbb{Q}(\tau)$ is an order. □

5.2 Poincaré reducibility

A homomorphism between abelian varieties $f : V/L \to W/M$ f is called an *isogeny* if F is an *isomorphism*, and an isomorphism if in addition $F(L) = M$. Isomorphisms are always bijections, while isogenies a finite to one surjections. For example, multiplication by a nonzero integer $n : V \to V$ induces an isogeny, which is not an isomorphism unless $n = \pm 1$. Two abelian varieties X and Y are called isogenous if there exists an isogeny from X to Y. Recall

Lemma 5.2.1. *Isogeny is an equivalence relation.*

We gave a direct proof earlier. We can give another proof, by interpreting isogeny in a fancier way. The collection of abelian varieties and homomorphisms forms an additive category $AbVar$. We can form a new category $AbVar_{\mathbb{Q}}$ with the same objects but with morphisms given by $Hom_{\mathbb{Q}}(X, Y) = Hom(X, Y) \otimes \mathbb{Q}$. We also set $End(X) = Hom(X, X)$ and $End_{\mathbb{Q}}(X) = End(X) \otimes \mathbb{Q}$. These are both not necessarily commutative rings. The previous lemma is now an immediate consequence of the observation:

Lemma 5.2.2. *Two abelian varieties are isogenous if and only if they are isomorphic in $AbVar_{\mathbb{Q}}$.*

Corollary 5.2.3. *$End_{\mathbb{Q}}(X)$ depends only on the isogeny class of X.*

Theorem 5.2.4 (Poincaré)**.** *If $X \subset Y$ is an injective homomorphism of abelian varieties, then Y is isogenous to a product X with another abelian variety.*

Proof. Suppose that $Y = V/L$ then $X = W/L \cap W$ for some subspace $W \subset V$ Let $W^\perp$ be the orthogonal complement with respect to a polarization H. Then this is also the orthogonal complement with respect to $E = \operatorname{Im} H$ by lemma 4.1.3. Equivalently, $W^\perp$ is the kernel of the map $v \mapsto E(v, -)$. Since this transformation can be represented by a rational matrix with respect to a basis of L, this implies that $\dim_{\mathbb{Q}} L_{\mathbb{Q}} \cap W^\perp = \dim_{\mathbb{R}} W^\perp$. Therefore $L \cap W^\perp$ is a lattice in $W^\perp$, so we can form torus $Z = W^\perp / L \cap W^\perp$. This is an abelian variety polarized by the restriction of H. The identity map $W \oplus W^\perp = V$ defines an isogeny $X \times Z \to Y$. □

An abelian variety is *simple* if it contains no nontrivial abelian subvarieties.

Corollary 5.2.5. *An abelian variety is isogenous to a product of simple abelian varieties.*

We turn now to the structure of the endomorphism ring $End_{\mathbb{Q}}(X)$. In general, it is noncommutative. The following is a standard argument in representation theory.

Theorem 5.2.6. *If X is simple, then $End_{\mathbb{Q}}(X)$ is a finite dimensional division algebra over $\mathbb{Q}$. In general, $End_{\mathbb{Q}}(X)$ is a product of matrix algebras over finite division algebras over $\mathbb{Q}$.*

Proof. The finite dimensionality is clear from construction, since $End_{\mathbb{Q}}(X) \subset End(L \otimes \mathbb{Q})$ where L is the lattice. Suppose that X is simple and that $f \in End_{\mathbb{Q}}(X)$ is nonzero. We have to show that f has an inverse. After replacing f by nf, we can assume that it is a homomorphism $f : X \to X$. It is enough to show that it is an isogeny. Since $f(X) \subset X$ is nonzero abelian subvariety, it follows that $f(X) = X$. Consider $\ker(f) \subset X$. It must be finite, since otherwise the connected component of the identity would give a nonzero abelian subvariety. It follows that f is an isogeny.

For the second statement, there is no loss in assuming that $X = \prod X_i'$ where X_i' simple. We can arrange this as $X = \prod X_i^{n_i}$ where X_i and X_j are nonisogenous when $i \neq j$. Given $\phi : X \to X$, we can decompose it as a product of morphisms $\phi_{ij} : X_i' \to X_j'$. Since both X_i' and X_j' are simple, ϕ_{ij} is either 0 or an isogeny. Thus we can decompose ϕ as product of matrices with values in $D_i = End_{\mathbb{Q}}(X_i)$. In other words, we have an inclusion

$$End_{\mathbb{Q}}(X) \hookrightarrow \prod Hom_{\mathbb{Q}}(X_i', X_j') = \prod Mat_{n_i \times n_i}(D_i)$$

This is clearly surjective as as well. □

An algebra of the above type is called semisimple.

5.3 The Rosati involution

There is an extra bit of structure which will be play a very important role. Given an algebra R over a field. An involution is a map $r \mapsto r^*$ which is linear over the field, such that $(rs)^* = s^* r^*$. For example, transpose gives an involution of on the algebra of matrices.

Let $X = V/L$ be an abelian variety with polarization H. The adjoint with respect to H:

$$H(Ax, y) = H(x, A^* y)$$

defines an involution on $End(V)$. The algebra $End_{\mathbb{Q}}(X)$ sits naturally inside this. It can be identified with the endomorphisms which preserve the rational lattice $L_{\mathbb{Q}} = L \otimes \mathbb{Q}$.

Theorem 5.3.1. *The subring $End_{\mathbb{Q}}(X) \subset End(V)$ is stable under the involution $*$.*

Proof. If $A \in End(L_{\mathbb{Q}})$ define $A^\dagger \in End(L_{\mathbb{Q}})$ to be the adjoint with respect to $E = \operatorname{Im} H$ i.e. $E(Ax, y) = E(x, A^\dagger y)$. This is defined because E is nonsingular. Given $A \in End_{\mathbb{Q}}(X)$, it preserves $L_{\mathbb{Q}}$, so we can form $A^\dagger \in End(L_{\mathbb{Q}})$. This coincides with the usual adjoint $A^* \in End(V)$ because $\operatorname{Im} H(Ax, y) = \operatorname{Im} H(x, A^* y)$. Therefore A^* preserves the rational lattice $L_{\mathbb{Q}}$, and thus defines an element of $End_{\mathbb{Q}}(X)$. □

The restriction of $*$ to $End_{\mathbb{Q}}(X)$ is called the *Rosati involution*. Although the construction would seem to be based on a linear algebra trick, there is a

way to make it more geometric. Let V^* be the space of complex *antilinear* maps $V \to \mathbb{C}$. This means that $f(av_1 + a_2v_2) = \bar{a}_1 f(v_1) + \bar{a}_2 f(v_2)$. This is can be understood as complex conjugate of the usual dual. Let $L^* \subset V^*$ denote the subset of those maps which are integer valued on L. The quotient $\hat{X} = V^*/L^*$ is a torus, which is in fact an abelian variety. The map $v \mapsto H(v, -)$ induces an isogeny ϕ_H between X and its dual $\hat{X} = V^*/L^*$. Thus we have an isomorphism $\Phi : End_{\mathbb{Q}}(X) \cong End_{\mathbb{Q}}(\hat{X})$. An endomorphism $A : X \to X$ induces a dual endomorphism $\hat{A} : \hat{X} \to \hat{X}$. Then $A^* \in End_{\mathbb{Q}}(X)$ is $\Phi^{-1}(\hat{A})$. All of this can be described geometrically as follows:

Theorem 5.3.2. *There is an isomorphism $Pic^0(X) \cong \hat{X}$ under which $\hat{A}$ corresponds to the homomorphism $Pic^0(X) \to Pic^0(X)$ given by $L \mapsto A^*L$. If M is an ample line bundle on X with the H the first Chern class (as discussed in section 4.1), then there is an isogeny $\phi_H : X \to \hat{X}$ is given by $\phi_H(x) = T_x^* M \otimes M^{-1} \in \hat{X}$. The Rosatti involution is given by*

$$A^* = \phi_H^{-1} \hat{A} \phi_H$$

Proof. [BL, MAV]. □

Given any finite dimensional $\mathbb{Q}$-algebra R, and element r defines a vector space endomorphism of R by left multiplication. This is the so called regular representation. Thus we have a well defined trace $Tr(r) \in \mathbb{Q}$. An involution $*$ on R is called *positive* if $Tr(r^*r) > 0$ when $r \neq 0$. Transpose on the algebra of matrices has this property.

Theorem 5.3.3. *The Rosati involution is positive.*

5.4 Division rings with involution

In the first section, we showed that $End_{\mathbb{Q}}$ of an elliptic curve was either $\mathbb{Q}$ or an imaginary quadratic field. In higher dimensions, things are more complicated, but that they can be understood. Given a simple abelian variety X, $End_{\mathbb{Q}}(X)$ is a finite dimensional division algebra with a positive involution. Our goal is to describe all such rings with involution. Over $\mathbb{R}$, things are much are easier. There are only two (finite dimensional) division algebras over it, the complex numbers $\mathbb{C}$ and the quaternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ with $i^2 = j^2 = -1$ and $ij = -ji = k$. Both of these algebras have a positive involution given by ordinary complex conjugation and quaternionic conjugation $(x+yi+zj+wk)^* = x-yi-zj-wk$. The construction of quaternions can be generalized to an algebra given by replacing $\mathbb{R}$ by an arbitrary field F, and by modifying the relations to $i^2 = a$, $j^2 = b$ and $ij = -ji = k$ for $a, b \in F^*$. This algebra is usually denoted by the Hilbert symbol $\left(\frac{a,b}{F}\right)$. This carries an involution defined as above. There are two possibilities, either $\left(\frac{a,b}{F}\right)$ is a division algebra, or it is the algebra of 2×2 matrices, in which case, we say that it splits. The algebra splits precisely

when the quadratic form $ax^2 + by^2 = 1$ has a solution over F. Therefore, when $F = \mathbb{R}$, $\left(\frac{a,b}{F}\right)$ is nonsplit, and thus $\mathbb{H}$, if and only if $a, b < 0$.

Over $\mathbb{Q}$, there is a classification of division algebras with positive involution.

Theorem 5.4.1 (Albert)**.** *The set of finite dimensional division algebras $(D, *)$ over $\mathbb{Q}$ with a positive involution are exactly the ones described below (written out of the traditional order).*

Type I. *$D = F$ is a totally real number field F (this means that all complex embeddings lie in $\mathbb{R}$) We give this the trivial involution $x^* = x$.*

Type III. *D is a quaternion algebra $\left(\frac{a,b}{F}\right)$ over a totally real number field F with $a, b \in F$ totally negative. The involution is the standard one.*

Type II. *D is a quaternion algebra over a totally real number field F which splits when extended to $\mathbb{R}$ under any embedding $F \hookrightarrow \mathbb{R}$ The involution becomes conjugate to the transpose on the matrix algebra under each isomorphism $D \otimes_F \mathbb{R} \cong M_2(\mathbb{R})$.*

Type IV. *D is a division algebra whose centre is a CM field F, i.e. a quadratic extension $F = K(\sqrt{-D})$ of a totally real field K with D totally positive. The involution restricts to $x + y\sqrt{-D} \mapsto x - y\sqrt{-D}$ on F.*

Proof. We refer to [MAV, pp 193-202] for the proof, and for a more detailed description in case IV. □

Quaternion algebras as in II (resp. III) are also said to be totally indefinite (resp. definite).

Corollary 5.4.2. *The endomorphism algebra of a simple abelian variety must be one of the above 4 types; the abelian variety is labelled accordingly.*

The statement in the corollary can be sharpened somewhat.

Theorem 5.4.3. *Suppose that A is a simple abelian variety of dimension g. Let $D = End_{\mathbb{Q}}(A)$, K the centre, and $e = [K : \mathbb{Q}]$. Then*

1. *$e|g$ (type I)*
2. *$2e|g$ (types II and III)*
3. *$e_0 d|g$ (type IV, where $e_0 = [F : \mathbb{Q}]$ and $d^2 = \dim_{\mathbb{Q}} D$ – it's always a square).*

Proof. The space of holomorphic 1-forms is a g dimensional $\mathbb{C}$-vector space. The $End(X)$-action makes $H^0(A, \Omega^1_A)$ into a K-vector space. This implies 1. See [BL, §5.5] for the remaining cases. □

We will see later that all of the categories I-IV occur for abelian varieties, and almost all of the subcases. The idea is easy to explain for elliptic curves.. In theorem 5.1.1, we saw that an elliptic curve $E = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$ has either $End_{\mathbb{Q}}(E) = \mathbb{Q}$ (special case of type I) or $End_{\mathbb{Q}}(E)$ imaginary quadratic (special case of type IV). Furthermore, in the second case, $End_{\mathbb{Q}}(E) = \mathbb{Q}(\tau)$. The converse is simple.

Lemma 5.4.4. *Given $\mathbb{Q}$ or an imaginary quadratic field, it arises as above.*

Proof. To build an elliptic curve with E with $End_{\mathbb{Q}}(E) = \mathbb{Q}(\sqrt{-d})$ we can use $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\sqrt{-d}$. For $End_{\mathbb{Q}}(E) = \mathbb{Q}$, suffices to take $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ with $\mathbb{Q}(\tau)$ not imaginary quadratic. For example, we can take τ transcendental. □

It is clear that "most" E have $End_{\mathbb{Q}}(E) = \mathbb{Q}$. Making this idea work in higher dimensions will require some understanding of moduli spaces.