Chapter XII. The endomorphism ring.

§ 1. *First basic results about the endomorphism algebra.*

Let X and Y be abelian varieties over a field k. If f and g are homomorphisms from X to Y then we have a homomorphism $(f+g)\colon X \to Y$ given on points by $x \mapsto f(x)+g(x)$. More formally,

$$(f+g) = m_Y \circ (f,g)\colon X \xrightarrow{(f,g)} Y \times_k Y \xrightarrow{m_Y} Y\,.$$

This gives the set $\mathrm{Hom}_k(X,Y)$ of homomorphisms $X \to Y$ (over the given field k) the structure of an abelian group. For $Y = X$ we find that $\mathrm{End}_k(X)$ has a natural ring structure, with composition of endomorphisms as the ring multiplication.

If $n \in \mathbb{Z}$ and $f \in \mathrm{Hom}_k(X,Y)$ then we have $n \cdot f = f \circ [n]_X = [n]_Y \circ f$. But for $n \neq 0$ we know that $[n]_X$ is an isogeny, in particular it is surjective; so we find that the group $\mathrm{Hom}_k(X,Y)$ is torsion-free. We write

$$\mathrm{Hom}^0_k(X,Y) := \mathrm{Hom}_k(X,Y) \otimes_{\mathbb{Z}} \mathbb{Q} \qquad \text{and} \qquad \mathrm{End}^0_k(X) := \mathrm{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q}\,.$$

By definition, $\mathrm{End}^0_k(X)$ is a $\mathbb{Q}$-algebra. If there is no risk of confusion one simply refers to $\mathrm{End}^0_k(X)$ as the endomorphism algebra of X. (The term *algebra* is supposed to distinguish it from the endomorphism *ring* $\mathrm{End}_k(X)$.) In the sequel we shall often suppress the subscript "k"; in such cases it shall be understood that we consider homomorphisms or endomorphisms over the given ground field.

(12.1) Remark. If $k \subset K$ is a field extension then we have a natural inclusion $\mathrm{Hom}_k(X,Y) \subset \mathrm{Hom}_K(X_K, Y_K)$, which in general is strict. Now $\mathrm{Hom}_K(X_K,Y_K)$ is the set of K-valued points of the k-group scheme $\mathit{Hom}(X,Y)$ which, as we have shown in Proposition (7.14), is étale. Hence if $k = k_s$ we have $\mathrm{Hom}_k(X,Y) = \mathrm{Hom}_K(X_K,Y_K)$ for any field extension $k \subset K$. We shall further sharpen this in Corollary (12.13) below.

(12.2) Theorem. (Poincaré Splitting Theorem) *Let X be an abelian variety over a field k. If $Y \subset X$ is an abelian subvariety then there exists an abelian subvariety $Z \subset X$ such that the homomorphism $f\colon Y \times Z \to X$ given by $(y,z) \mapsto y+z$ is an isogeny. (Thus $Y + Z = X$ and $Y \cap Z$ is finite.)*

Proof. Write $i\colon Y \hookrightarrow X$ for the inclusion. Choose a polarization $\lambda\colon X \to X^t$, and let

$$W := \mathrm{Ker}\big(X \xrightarrow{\lambda} X^t \xrightarrow{i^t} Y^t\big)\,.$$

We know from Exercise (11.1) that $\lambda_Y := i^t \circ \lambda \circ i\colon Y \to Y^t$ is again a polarization. In particular, $Y \cap W$ is finite.

Suppose we can find an abelian subvariety $Z \subset X$ of dimension $\dim(X) - \dim(Y)$ with $Z \subseteq W$. Then $(Y \cap Z)$ is finite, and because the kernel of $f\colon Y \times Z \to X$ is contained in $(Y \cap Z) \times (Y \cap Z)$ this implies that f is an isogeny, as desired.

Now take $Z := W^0_{\mathrm{red}}$. By Prop. (5.31) we know that Z is indeed an abelian subvariety of X, and Z has dimension $\dim(X) - \dim(Y)$. Further, $(Y \cap Z)$ is finite, and because the kernel of the natural homomorphism $f\colon Y \times Z \to X$ is contained in $(Y \cap Z) \times (Y \cap Z)$ this implies that f is an isogeny, as desired. □

(12.3) Remark. In the proof of the theorem we use the fact, proven in Prop. (5.31), that W^0_{red} is an abelian subvariety of X. The main difficulty is that *a priori* (i.e., without knowing this result) W^0_{red} might not even be a subgroup scheme of X; see Exercise (3.2). Instead of using Prop. (5.31) we can also prove the theorem by the following argument that uses the existence of the quotient abelian variety X/Y.

Let $Y \subset X$ be an abelian subvariety. By Thm. (4.38) there exists an fppf quotient group scheme $q\colon X \twoheadrightarrow Q := X/Y$. Since Q is also a geometric quotient of X by Y, it is in fact an abelian variety, of dimension $\dim(X) - \dim(Y)$. The homomorphism $q^t\colon Q^t \to X^t$ is injective (see Exercise 7.7), and we use it to identify Q^t with an abelian subvariety of X^t. Choose an isogeny $\mu\colon X^t \to X$ such that $\lambda \circ \mu = [n]_{X^t}$ for some positive integer n. Let $Z \subset X$ be the image of Q^t under μ; so $Z \cong Q^t/\big(Q^t \cap \mathrm{Ker}(\mu)\big)$ is an abelian subvariety of X, with $\dim(Z) = \dim(Q) = \dim(X) - \dim(Y)$. Now note that $\lambda(Z) \subseteq Q^t \subseteq \mathrm{Ker}(i^t)$; hence $Z \subseteq W$. In particular, $Z \cap Y$ is finite, and as in the above proof it follows that the natural homomorphism $Y \times Z \to X$ is an isogeny. □

(12.4) Definition. A non-zero abelian variety X over a field k is said to be *simple* if X has no abelian subvarieties other than 0 and X. We say that X is *elementary* if X is isogenous (over k) to a power of a simple abelian variety, i.e., $X \sim_k Y^m$ for some $m \geqslant 1$ and Y simple.

Note that an abelian variety that is simple over the ground field k need not be simple over an extension of k. To avoid confusion we sometimes uses the terminology "k-simple". If X is simple over a separably closed field k then it follows from Remark (12.1) that X_L is simple for every extension $k \subset L$.

(12.5) Corollary. *A non-zero abelian variety over k is isogenous to a product of k-simple abelian varieties. More precisely, there exists k-simple abelian varieties $Y_1, \ldots, Y_n$, no two of which are k-isogenous, and positive integers $m_1, \ldots, m_n$ such that*

$$X \sim_k Y_1^{m_1} \times \cdots \times Y_n^{m_n}\,. \tag{1}$$

Up to permutation of the factors the Y_i appearing in this decomposition are unique up to k-isogeny, and the corresponding "multiplicities" m_i are uniquely determined.

Proof. The existence of a decomposition (1) is immediate from the theorem. The unicity statement is an easy exercise—note that a homomorphism between two simple abelian varieties is either zero or an isogeny. □

(12.6) Definition. Let k be a field. We define *the category of abelian varieties over k up to isogeny*, notation $\mathbb{Q}\mathsf{AV}_{/k}$, to be the category with as objects abelian varieties over k and with $\mathrm{Hom}_{\mathbb{Q}\mathsf{AV}_{/k}}(X,Y) = \mathrm{Hom}^0_k(X,Y) := \mathrm{Hom}_{\mathsf{AV}_{/k}}(X,Y) \otimes_{\mathbb{Z}} \mathbb{Q}$.

If X and Y are abelian varieties over k then an element $f \in \mathrm{Hom}^0(X,Y)$ is called a *quasi-isogeny* if f is an isomorphism in the category $\mathbb{Q}\mathsf{AV}_{/k}$.

To explain the terminology, notice that a homomorphism of abelian varieties is an isomorphism in the category $\mathbb{Q}\mathsf{AV}_{/k}$ if and only if it is an isogeny. In particular, two abelian varieties

give isomorphic objects of $\mathbb{Q}\mathsf{AV}_{/k}$ if and only if they are k-isogenous. More precisely, an element $f \in \mathrm{Hom}^0(X,Y)$ is a quasi-isogeny if and only if there is a non-zero integer n such that nf is an isogeny from X to Y.

(12.7) Corollary. *If X is k-simple then $\mathrm{End}_k^0(X)$ is a division algebra. For X as in* (1) *we have, writing $D_i := \mathrm{End}_k^0(Y_i)$,*

$$\mathrm{End}_k^0(X) \cong M_{m_1}(D_1) \times \cdots \times M_{m_n}(D_n)\,.$$

(Recall that $M_m(R)$ denotes the ring of $m \times m$ matrices with coefficients in R.)

Proof. Let us (again) remark that any homomorphism between two k-simple abelian varieties is either zero or an isogeny. But the isogenies from X to itself are invertible elements of $\mathrm{End}_k^0(X)$. So if X is k-simple then $\mathrm{End}_k^0(X)$ is indeed a division algebra. For the second statement, note that $\mathrm{Hom}_k(Y_i, Y_j) = 0$ if $i \neq j$, as it was assumed that Y_i and Y_j are simple and non-isogenous. □

In categorical language, we have shown that $\mathbb{Q}\mathsf{AV}_{/k}$ is a semi-simple category.

To obtain further results, we shall investigate homomorphisms $f\colon X \to Y$ via the induced maps $T_\ell f$ on Tate-ℓ-modules, or the maps $f[p^\infty]$ on p-divisible groups. We shall usually state results in both settings. If $p \neq \mathrm{char}(k)$ then statements about $f[p^\infty]$ can also be phrased in terms of Tate modules, and it is this formulation that is most often used. (This is based on the sentiment that ordinary groups with Galois action are conceptually easier than étale group schemes.) Hence our main interest in results about $f[p^\infty]$ is in the case that $\mathrm{char}(k) = p > 0$, even though this is often irrelevant in the proofs.

(12.8) Lemma. *Let X and Y be abelian varieties over a field k, and let $f \in \mathrm{Hom}(X,Y)$.*

(i) *Let ℓ be a prime number, $\ell \neq \mathrm{char}(k)$. If $T_\ell(f)$ is divisible by ℓ^m in $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$ then f is divisible by ℓ^m in $\mathrm{Hom}(X,Y)$.*

(ii) *Let p be a prime number. If $f[p^\infty]$ is divisible by p^m in $\mathrm{Hom}\big(X[p^\infty], Y[p^\infty]\big)$ then f is divisible by p^m in $\mathrm{Hom}(X,Y)$.*

Proof. The divisibility of $T_\ell(f)$ means that f vanishes on $X[\ell^m](k_s)$. But $X[\ell^m]$ is an étale group scheme ($\ell \neq \mathrm{char}(k)$), hence f vanishes on $X[\ell^m]$. This means that f factors through $[\ell^m]_X$.

The argument for (ii) is essentially the same: If $f[p^\infty]$ is divisible by p^m then f vanishes on $X[p^m]$; hence it factors through $[p^m]_X$. □

If $T_\ell(f) = \ell^m \cdot \varphi$ for some $\varphi \in \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$ then the element $g \in \mathrm{Hom}(X,Y)$ such that $\ell^m \cdot g = f$ is unique (as $\mathrm{Hom}(X,Y)$ is torsion-free), and it follows from Theorem (12.10) below that $T_\ell(g) = \varphi$. Similarly, if $f[p^\infty] = p^m \cdot \varphi$ then there is a unique $g \in \mathrm{Hom}(X,Y)$ with $p^m \cdot g = f$, and $g[p^\infty] = \varphi$.

(12.9) Lemma. *Let X be an abelian variety, and let L be an ample line bundle on X. Then the form $B_L\colon \mathrm{End}(X) \times \mathrm{End}(X) \to \mathbb{Z}$ given by*

$$B_L(f,g) = c_1(L)^{g-1} \cdot c_1\big((f+g)^*L \otimes f^*L^{-1} \otimes g^*L^{-1}\big)$$

is bilinear and positive definite.

Note that by slight abuse of notation we write $c_1(L)^{g-1} \cdot c_1(M)$ for $\deg\big(c_1(L)^{g-1} \cdot c_1(M)\big) = \int_X c_1(L)^{g-1} \cdot c_1(M)$; cf. the remark following Thm. (9.11).

Proof. Consider the map $q\colon \mathrm{End}(X) \to \mathrm{CH}^1(X)$ given by $f \mapsto c_1(f^*L)$. It follows from the Theorem of the Cube, Cor. (2.8), together with Exercise (2.5) that the map $b_L\colon \mathrm{End}(X) \times \mathrm{End}(X) \to \mathrm{CH}^1(X)$ given by

$$b_L(f,g) = q(f+g) - q(f) - q(g) = c_1\big((f+g)^*L \otimes f^*L^{-1} \otimes g^*L^{-1}\big)$$

is bilinear. But if $h\colon \mathrm{CH}^1(X) \to \mathbb{Z}$ is the linear map given by $\xi \mapsto c_1(L)^{g-1} \cdot \xi$ then $B_L = h \circ b_L$; hence B_L is bilinear too.

It remains to be shown that $B_L(f,f) > 0$ for all non-zero $f \in \mathrm{End}(X)$. Note that $(2f)^*L \otimes (f^*L)^{-2} = f^*\big([2]^*L\big) \otimes f^*L^{-2}$ is algebraically equivalent to $f^*L^4 \otimes f^*L^{-2} = f^*L^2$. Hence $B_L(f,f) = 2 \cdot c_1(L)^{g-1} \cdot c_1(f^*L)$. Because L is ample, it suffices to show that $c_1(f^*L)$ is an effective class if $f \neq 0$. Further, as $B_{L^n}(f,f) = n^g \cdot B_L(f,f)$ we may assume that L is very ample. If $f \neq 0$ then $Y := f(X) \subset X$ is an abelian subvariety of X of positive dimension, and there is an effective divisor $D = \sum n_i D_i$ on Y such that $L_{|Y} = O_Y(D)$. But $f\colon X \to Y$ is flat (see Exercise (5.1)), so f^*L is represented by the divisor $\sum n_i [f^{-1}D_i]$, where $[f^{-1}D_i]$ is the divisor class associated to the scheme-theoretic inverse image of D_i. In particular, $c_1(f^*L)$ is an effective class, and the positivity of B_L follows. □

(12.10) Theorem. *Let X and Y be abelian varieties over a field k.*

(i) *If ℓ is a prime number, $\ell \neq \mathrm{char}(k)$ then the $\mathbb{Z}_\ell$-linear map*

$$T_\ell\colon \mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$$

given by $f \otimes c \mapsto c \cdot T_\ell(f)$ is injective and has a torsion-free cokernel.

(ii) *If p is a prime number, the $\mathbb{Z}_p$-linear map*

$$\Phi\colon \mathrm{Hom}(X,Y) \otimes \mathbb{Z}_p \longrightarrow \mathrm{Hom}\big(X[p^\infty], Y[p^\infty]\big)$$

given by $f \otimes c \mapsto c \cdot f[p^\infty]$ is injective and has a torsion-free cokernel.

Proof. (i) We first prove that T_ℓ has a torsion-free cokernel. Notice that $\mathrm{Coker}(T_\ell)$ is a $\mathbb{Z}_\ell$-module, so it can only have ℓ-power torsion. Suppose we have $\varphi \in \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$ and $\sum f_i \otimes c_i \in \mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell$ such that $\ell^m \cdot \varphi = \sum c_i \cdot T_\ell(f_i)$. Choose integers n_i with $n_i \equiv c_i \bmod \ell^m$, and write $c_i = n_i + \ell^m \cdot d_i$ with $d_i \in \mathbb{Z}_\ell$. Then $f := \sum n_i f_i$ is an element of $\mathrm{Hom}(X,Y)$, and $T_\ell(f) = \ell^m \cdot \big(\varphi - \sum d_i T_\ell(f_i)\big)$ is divisible by ℓ^m. By Lemma (12.8) there exists an element $g \in \mathrm{Hom}(X,Y)$ with $T_\ell(g) = \varphi - \sum d_i T_\ell(f_i)$. Hence φ is in the image of the map T_ℓ, which is what we had to prove.

Now we prove that T_ℓ is injective. We first reduce to the case that $Y = X$. For this, put $Z := X \times Y$. Then we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(X,Y) & \xrightarrow{T_\ell} & \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y) \\ \downarrow & & \downarrow \\ \mathrm{End}(Z) & \xrightarrow{T_\ell} & \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell Z) \end{array}$$

where the left vertical map sends $f\colon X \to Y$ to the endomorphism $(x,y) \mapsto \big(0, f(x)\big)$ of Z, and where the right vertical map is defined similarly. As the left vertical map is clearly injective, this reduces the problem to the case $X = Y$.

Suppose there exist linearly independent elements $f_1, \ldots, f_r \in \mathrm{End}(X)$ and non-zero ℓ-adic integers $c_1, \ldots, c_r$ such that

$$c_1 T_\ell(f_1) + \cdots + c_r T_\ell(f_r) = 0\,. \tag{2}$$

We may assume that r is minimal, i.e., that there is no such relation with fewer terms. Choose an ample bundle L and let $B = B_L\colon \mathrm{End}(X) \times \mathrm{End}(X) \to \mathbb{Z}$ be the form as in the lemma. In (2) we may assume that $B(f_1, f_j) = 0$ for all $j \in \{2, \ldots, r\}$; to achieve this, replace c_1 by $\sum_{k=1}^{r} B(f_k, f_1) \cdot c_k$, and for $j \geqslant 2$ replace f_j by $B(f_1, f_1) \cdot f_j - B(f_j, f_1) \cdot f_1$. (Note that the new elements f_j are again linearly independent.)

Let m be a positive integer. Choose integers n_i with $n_i \equiv c_i \bmod \ell^m$. Then $g := n_1 f_1 + \cdots + n_r f_r$ is an endomorphism of X such that $T_\ell(g)$ divisible by ℓ^n. By Lemma (12.8) there is an $h \in \mathrm{End}(X)$ such that $g = \ell^n \cdot h$. Hence $n_1 \cdot B(f_1, f_1) = B(g, f_1)$ is divisible by ℓ^m, and by our choice of n_1 it follows that $c_1 \cdot B(f_1, f_1)$ is divisible by ℓ^m. But m was arbitrary, and $B(f_1, f_1)$ is a fixed positive integer. Hence $c_1 = 0$, contradicting the minimality assumption on r.

The proof of (ii) is essentially the same; we leave it to the reader. □

(12.11) Corollary. *If X and Y are abelian varieties over k then $\mathrm{Hom}(X, Y)$ is a free $\mathbb{Z}$-module of rank at most $4 \dim(X) \dim(Y)$. In particular, $\mathrm{End}^0(X)$ is a finite dimensional semi-simple $\mathbb{Q}$-algebra, of dimension at most $4 \dim(X)^2$.*

Proof. We already know that $\mathrm{Hom}(X, Y)$ is torsion-free. The upper bound for the rank is immediate from the theorem, as $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$ is a free $\mathbb{Z}_\ell$-module of rank $4 \dim(X) \dim(Y)$. □

(12.12) Corollary. *If X is a g-dimensional abelian variety over a field k then its Néron-Severi group $\mathrm{NS}(X)$ is a free $\mathbb{Z}$-module of rank at most $4g^2$.*

Proof. By Corollary (7.26) we have $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{symm}}(X, X^t)$. □

(12.13) Corollary. *Let X and Y be abelian varieties over a field k. Fix a separable algebraic closure $k \subset k_s$. Then there is a finite field extension $k \subset K$ inside k_s which is "the smallest field extension over which all homomorphisms from X to Y are defined", meaning that K has the following two properties:*

(a) *for any field extension $K \subset L$ we have $\mathrm{Hom}_K(X_K, Y_K) \xrightarrow{\sim} \mathrm{Hom}_L(X_L, Y_L)$;*

(b) *if Ω is a field containing k_s and $F \subset \Omega$ is a subfield with $k \subseteq F$ and $\mathrm{Hom}_F(X_F, Y_F) \xrightarrow{\sim} \mathrm{Hom}_\Omega(X_\Omega, Y_\Omega)$, then $K \subseteq F$.*

Proof. As $\mathit{Hom}(X, Y)$ is an étale group scheme, this assertion is just a matter of Galois theory. Choose generators $f_1, \ldots, f_r$ of $\mathrm{Hom}_{k_s}(X_{k_s}, Y_{k_s})$ as an additive group. Let $\Gamma_i \subset \mathrm{Gal}(k_s/k)$ be the stabilizer of f_i under the natural continuous action of $\mathrm{Gal}(k_s/k)$ on $\mathrm{Hom}_{k_s}(X_{k_s}, Y_{k_s})$. Each Γ_i is an open subgroup of $\mathrm{Gal}(k_s/k)$. Now let $K \subset k_s$ be the fixed field of $\Gamma_1 \cap \cdots \cap \Gamma_r$; it is the smallest subfield of k_s over which the f_i are all defined. Because the f_i generate $\mathrm{Hom}_{k_s}(X_{k_s}, Y_{k_s})$ the group scheme $\mathit{Hom}(X, Y)$ becomes constant over K; hence (a) holds. If F is as in (b) then the f_i are all defined over $K \cap F$ (intersection inside Ω), and by definition of K it follows that $K \subseteq (K \cap F)$, i.e., $K \subseteq F$. □

§ 2. *The characteristic polynomial of an endomorphism.*

(12.14) Let X be an abelian variety of dimension g over a field k. If W is a $\mathbb{Q}$-vector space then a map $\gamma\colon \mathrm{End}(X) \to W$ is said to be homogeneous of degree m if $\gamma(n \cdot f) = n^m \cdot \gamma(f)$ for all $f \in \mathrm{End}(X)$ and all $n \in \mathbb{Z}$. Any homogeneous map γ naturally extends to a map $\gamma\colon \mathrm{End}^0(X) \to W$: write $g \in \mathrm{End}^0(X)$ as $g = q \cdot f$ for some $q \in \mathbb{Q}$ and $f \in \mathrm{End}(X)$, and then set $\gamma(g) = q^m \cdot \gamma(f)$.

We appply this to the map $\deg\colon \mathrm{End}(X) \to \mathbb{Q}$, which is homogeneous of degree $2g$. Note that, by convention, $\deg(f) = 0$ if $f \in \mathrm{End}(X)$ is not finite. By the procedure that we have just explained, this degree map extends to a map $\deg\colon \mathrm{End}^0(X) \to \mathbb{Q}$, with $\deg(q \cdot f) = q^{2g} \cdot \deg(f)$ for $q \in \mathbb{Q}$ and $f \in \mathrm{End}(X)$.

(12.15) Proposition. *The map* $\deg\colon \mathrm{End}^0(X) \to \mathbb{Q}$ *is a homogeneous polynomial map of degree* $2g$. *This means that if* $e_1, \ldots, e_u$ *is a basis for* $\mathrm{End}^0(X)$ *as a* $\mathbb{Q}$*-vector space, then there is a homogeneous polynomial* $D \in \mathbb{Q}[t_1, \ldots, t_u]$ *of degree* $2g$ *such that*

$$\deg(c_1 e_1 + \cdots + c_u e_u) = D(c_1, \ldots, c_u)$$

for all $c_i \in \mathbb{Q}$.

Proof. Let L be a symmetric ample bundle on X. Then the map $\gamma\colon \mathrm{End}(X) \to \mathrm{CH}^1_{\mathbb{Q}}(X)$ given by $f \mapsto c_1(f^*L)$ is homogeneous of degree 2, so by what was explained in (12.14) it naturally extends to a map $\gamma\colon \mathrm{End}^0(X) \to \mathrm{CH}^1_{\mathbb{Q}}(X)$. By Cor. (9.12), $\deg(f) = c_1(f^*L)^g / c_1(L)^g$ for all $f \in \mathrm{End}(X)$; note that this also holds if $f\colon X \to X$ is not an isogeny, for in that case the Riemann-Roch Theorem (9.11) gives $\chi(f^*L)^2 = \deg(\varphi_{f^*L}) = 0$. Hence it suffices to show that the map γ is a homogeneous polynomial map of degree 2.

As we have seen in the proof of Lemma (12.9), the map $b\colon \mathrm{End}(X) \times \mathrm{End}(X) \to \mathrm{CH}^1(X)$ given by $b(f,g) = c_1\big((f+g)^*L \otimes f^*L^{-1} \otimes g^*L^{-1}\big)$ is bilinear. Also, b is clearly symmetric. But, again using the assumption that L is symmetric, $\gamma(f) = (1/2) \cdot b(f,f)$. From this it readily follows that γ is polynomial of degree 2. □

(12.16) Definition. Let X be an abelian variety over k. If $f \in \mathrm{End}^0(X)$ then, by the proposition, there is a monic polynomial $P = P_f \in \mathbb{Q}[t]$ of degree $2g$ such that $P(n) = \deg\big([n]_X - f\big)$ for all $n \in \mathbb{Z}$. We call P the *characteristic polynomial of* f. If $P = \sum_{i=0}^{2g} a_i t^i$ then we define the *trace of* f by $\mathrm{trace}(f) := -a_{2g-1}$.

In this context, the degree of an endomorphism f is also sometimes referred to as the *norm of* f; so, with the previous notation, $\mathrm{Norm}(f) := \deg(f) = a_0$.

(12.17) Lemma. *Let* Q *be a field of characteristic zero. Let* A *be a semisimple* Q*-algebra of finite* Q*-dimension, and let* $A = A_1 \times \cdots \times A_h$ *be the decomposition of* A *into a product of simple factors. Let* $\mathrm{Nrd}_{A_j/Q}\colon A_j \to Q$ *be the reduced norm of* A_j *over* Q. *Suppose* $\delta\colon A \to Q$ *is a nonzero map that has the following two properties:*
(a) δ *is a homogeneous polynomial map;*
(b) δ *is multiplicative, meaning that* $\delta(ab) = \delta(a)\delta(b)$ *for all* $a, b \in A$.
Then there exist integers $n_1, \ldots, n_h$ *such that*

$$\delta(a_1, \ldots, a_h) = \mathrm{Nrd}_{A_1/Q}(a_1)^{n_1} \cdots \mathrm{Nrd}_{A_h/Q}(a_h)^{n_h}$$

for all $(a_1, \ldots, a_h) \in A = A_1 \times \cdots \times A_h$.

Proof. By (b) we have $\delta(a_1,\dots,a_h) = \delta(a_1,1,\dots,1)\cdot\delta(1,a_2,1,\dots,1)\cdots\delta(1,\dots,1,a_h)$. Since the function that sends $a_j \in A_j$ to $\delta(1,\dots,1,a_j,1,\dots,1)$ is again homogeneous polynomial and multiplicative, it suffices to treat the case $h = 1$. So from now on we assume that A is a simple Q-algebra. Let K be its centre, which is a finite field extension of Q. Choose an algebraic closure $\overline{Q}$ of Q, and let Σ be the set of embeddings $\sigma\colon K \to \overline{Q}$ that extend the given embedding $Q \hookrightarrow \overline{Q}$.

Let $e_1,\dots,e_u$ be an ordered basis for A as a vector space over Q. Assumption (a) just means that there exists a homogeneous polynomial $D \in Q[t_1,\dots,t_u]$ such that $\delta(c_1e_1+\cdots+c_ue_u) = D(c_1,\dots,c_u)$ for all $c_1,\dots,c_u \in Q$. Because Q is infinite, D is uniquely determined. For any field extension $Q \subset L$ the map δ therefore uniquely extends to a homogeneous polynomial map $\delta_L\colon A_L := L \otimes_Q A \to L$. Moreover, because A is Zariski dense in A_L, the extended map δ_L is again multiplicative.

We have

$$A_{\overline{Q}} = \prod_{\sigma\in\Sigma} A_\sigma \qquad \text{with} \qquad A_\sigma = \overline{Q} \otimes_{\sigma,K} A\,.$$

If m is the degree of A as a central simple K-algebra, each factor A_σ is (non-canonically) isomorphic to $M_m(\overline{Q})$. Write $\delta_\sigma\colon A_\sigma \to \overline{Q}$ for the map given by $a_\sigma \mapsto \delta_{\overline{Q}}(1,\dots,1,a_\sigma,1,\dots,1)$. Because δ_σ is multiplicative and δ is not the zero map, $\delta_\sigma(a) \in \overline{Q}^*$ for every $a \in A_\sigma^*$. Choosing an isomorphism $\iota_\sigma\colon A_\sigma \xrightarrow{\sim} M_m(\overline{Q})$ we conclude that δ_σ gives a character of GL_m over $\overline{Q}$, that is, a homomorphism of algebraic groups $\delta_\sigma\colon \mathrm{GL}_{m,\overline{Q}} \to \mathbb{G}_{m,\overline{Q}}$. But any such character is of the form $\det^\nu$ for some integer ν; see ??. Note that the integer ν does not depend on the choice of ι_σ, as by the Skolem-Noether theorem all automorphisms of $M_m(\overline{Q})$ are inner automorphisms.

We conclude that there exist integers $\nu(\sigma)$ such that $\delta_{\overline{Q}}$ is given by

$$\delta_{\overline{Q}}\big((a_\sigma)_{\sigma\in\Sigma}\big) = \prod_{\sigma\in\Sigma}\delta_\sigma(a_\sigma) = \prod_{\sigma\in\Sigma}\det\big(\iota_\sigma(a_\sigma)\big)^{\nu(\sigma)}\,.$$

Let us also note that the reduced norm map $\mathrm{Nrd}_{A/Q}\colon A \to Q$ after extension of scalars $Q \subset \overline{Q}$ gives the map $A_{\overline{Q}} \to \overline{Q}$ that sends $(a_\sigma)_{\sigma\in\Sigma}$ to $\prod_{\sigma\in\Sigma}\det\big(\iota_\sigma(a_\sigma)\big)$. So all that is left to prove is that the exponents $\nu(\sigma)$ are all equal. To see this, note that for any $c \in K$ we have

$$\delta(c) = \delta_{\overline{Q}}\big((\sigma(c))_{\sigma\in\Sigma}\big) = \prod_{\sigma\in\Sigma}\det\big(\sigma(c)\big)^{\nu(\sigma)} = \prod_{\sigma\in\Sigma}\sigma(c)^{m\nu(\sigma)}\,. \tag{3}$$

Now it is an easy exercise in Galois theory to see that the RHS of (3) defines a function on K that takes values in Q only if all exponents $m\nu(\sigma)$ are equal. □

(12.18) Theorem. *Let X be an abelian variety over a field k. Let ℓ be a prime number different from $\mathrm{char}(k)$. For $f \in \mathrm{End}^0(X)$, let $P_{\ell,f} \in \mathbb{Q}_\ell[t]$ be the characteristic polynomial of $V_\ell f \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell X)$, i.e., $P_{\ell,f}(t) = \det(t\cdot\mathrm{id} - V_\ell f)$. Then $P_{\ell,f} = P_f$. In particular, the characteristic polynomial of $V_\ell f$ has coefficients in $\mathbb{Q}$ and is independent of ℓ.*

Proof. We know that $A := \mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{End}(X)$ is a semisimple $\mathbb{Q}_\ell$-algebra of finite dimension. Let $A = A_1 \times \cdots \times A_h$ be its decomposition into a product of simple factors. As explained in the proof of (12.17) the degree map $f \mapsto \deg(f)$ extends uniquely to a homogeneous polynomial map $\delta_1\colon A \to \mathbb{Q}_\ell$ of degree $2g$.

The function $\delta_2\colon A \to \mathbb{Q}_\ell$ given by $f \mapsto \det(V_\ell f)$ is also a homogeneous polynomial map of degree $2g$. As δ_1 and δ_2 are both multiplicative, we can apply Lemma (12.17) to each. We conclude that there exist integers n_i and ν_i such that for any $f = (f_1,\dots,f_h) \in A$,

$$\delta_1(f) = \mathrm{Nrd}_{A_1/\mathbb{Q}_\ell}(f_1)^{n_1}\cdots\mathrm{Nrd}_{A_h/\mathbb{Q}_\ell}(f_h)^{n_h}$$

and

$$\delta_2(f) = \mathrm{Nrd}_{A_1/\mathbb{Q}_\ell}(f_1)^{\nu_1} \cdots \mathrm{Nrd}_{A_h/\mathbb{Q}_\ell}(f_h)^{\nu_h}\,.$$

To get further information, we consider the ℓ-adic valuation $v\colon \mathbb{Q}_\ell \to \mathbb{Z} \cup \{\infty\}$. Let $\mathscr{E} := \mathrm{End}(X) \cap \mathrm{End}^0(X)^*$ be the monoid of isogenies $X \to X$. If $f \in \mathscr{E}$ we can write $N := \mathrm{Ker}(f)$ as $N = N_\ell \times N^\ell$, with N^ℓ a group scheme of order prime to ℓ and N_ℓ of ℓ-power order, say $\#N_\ell = \ell^a$. We have $v\big(\deg(f)\big) = a$. On the other hand, we have seen in Proposition (10.6) that $T_\ell f\colon T_\ell X \to T_\ell X$ is injective with cokernel $N_\ell(k_s)$. Because ℓ is relatively prime to $\mathrm{char}(k)$ the group scheme N_ℓ is étale, so $N_\ell(k_s)$ is just an ordinary abelian group of order ℓ^a. From the theory of elementary divisors it then follows that $v\big(\det(V_\ell f)\big) = a$ as well.

Any $\varphi \in \mathrm{End}^0(X)^*$ can be written as $\varphi = q \cdot f$ for some $q \in \mathbb{Q}^*$ and $f \in \mathscr{E}$. As δ_1 and δ_2 are both homogeneous of degree $2g$, it follows that $v\big(\deg(\varphi)\big) = v\big(\det(V_\ell)\big)$. Now the set

$$\Big\{ f \in A \;\Big|\; v\big(\delta_1(f)\big) = v\big(\delta_2(f)\big) \Big\}$$

is closed in A for the ℓ-adic topology, and we have just shown that it contains $\mathrm{End}^0(X)^*$. But $\mathrm{End}^0(X)^*$ is ℓ-adically dense in A, so we conclude that $v\big(\delta_1(f)\big) = v\big(\delta_2(f)\big)$ for all $f \in A$. Applying this to all elements of the form $(1, \ldots, 1, \ell, 1, \ldots, 1) \in A = A_1 \times \cdots \times A_h$, we find that $n_i = \nu_i$ for all i. □

(12.19) Corollary. *For any $f \in \mathrm{End}^0(X)$ we have $P_f(f) = 0$.*

(12.20) Corollary. *If $f \in \mathrm{End}(X)$ then P_f has integral coefficients.*

Proof. Let $f \in \mathrm{End}(X)$. Because $\mathrm{End}(X)$ is finitely generated as an additive group, there is a monic $Q \in \mathbb{Z}[t]$ with $Q(f) = 0$. But then also $Q(V_\ell f) = 0$, which implies that all eigenvalues of $V_\ell f$ are algebraic integers. So the coefficients of $P_{\ell,f} = P_f$ are rational numbers which are at the same time algebraic integers; hence they are integers. □

(12.21) Corollary. *For f, $g \in \mathrm{End}^0(X)$ we have the relations*

$$\deg(fg) = \deg(f) \cdot \deg(g)\,, \quad \mathrm{trace}(f+g) = \mathrm{trace}(f) + \mathrm{trace}(g)\,, \quad \text{and} \quad \mathrm{trace}(fg) = \mathrm{trace}(gf)\,.$$

If p is a prime number and $f \in \mathrm{End}^0(X)$ then it follows from Cor. (12.19) that $P_f\big(f[p^\infty]\big) = 0$. One naturally wonders if P_f can also be interpreted as the characteristic polynomial of $f[p^\infty]$ as an endomorphism of the p-divisible group $X[p^\infty]$. (??Nog verder uitwerken. Later bewijzen dat P_f ook het char pol is van f op de kristallijne cohom??)

(12.22) Remark. Let X be a simple abelian variety over a field k, so that $\mathrm{End}^0(X)$ is a division algebra. If $f \in \mathrm{End}^0(X)$ then $\mathbb{Q}[f] \subset \mathrm{End}^0(X)$ is a number field, and $\mathbb{Q}_\ell[f] := \mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathbb{Q}[f]$ is a product of finite field extensions of $\mathbb{Q}_\ell$, say $\mathbb{Q}_\ell[f] = L_1 \times \cdots \times L_t$. Correspondingly we have a decomposition $V_\ell X = V_1 \oplus \cdots \oplus V_t$. The fact that $P_{\ell,f}$ has coefficients in $\mathbb{Q}$ means precisely that $V_\ell X$ is free as a module over $\mathbb{Q}_\ell[f]$, or, equivalently, that $d_i := \dim_{L_i}(V_i)$ is independent of i. To see this, let h be the minimum polynomial of f over $\mathbb{Q}$. Let $h = h_1 \cdots h_t$ be the prime factorisation of h in $\mathbb{Q}_\ell[t]$, so that $L_i \cong \mathbb{Q}_\ell[t]/(h_i)$. Then $P_{\ell,f}$ equals $h_1^{d_1} \cdots h_t^{d_t}$. Now it is an easy exercise in Galois theory to see that $\prod h_i^{d_i}$ has coefficients in $\mathbb{Q}$ if and only if all exponents d_i are equal.

It is not true, in general, that $V_\ell X$, as a module over $\mathrm{End}^0(X)$, is "defined over $\mathbb{Q}$". That is, in general there is no $\mathrm{End}^0(X)$-module W such that $V_\ell X \cong \mathbb{Q}_\ell \otimes_{\mathbb{Q}} W$ as modules over

$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathrm{End}^0(X)$. The easiest counterexample is provided by a supersingular elliptic curve X over an algebraically closed field of characteristic p. In this case $D := \mathrm{End}^0(X)$ is a quaternion algebra with center $\mathbb{Q}$, and if W is any left D-module of finite type then the $\mathbb{Q}$-dimension of W is divisible by 4, whereas $V_\ell X$ is 2-dimensional. Such examples only occur in positive characteristic, and this has interesting consequences for the types of endomorphism algebras that can occur. We shall come back to this in ?? below.

§ 3. *The Rosati involution.*

(12.23) Let $\lambda\colon X \to X^t$ be a polarization. If $f \in \mathrm{End}^0(X)$ then we have $f^t \in \mathrm{End}^0(X^t)$, and in $\mathrm{End}^0(X)$ we can form the element $f^\dagger := \lambda^{-1} \circ f^t \circ \lambda$:

$$\begin{array}{ccc} X & \xrightarrow{\lambda} & X^t \\ & & {\scriptstyle f^t}\big\downarrow \\ X & \xleftarrow{\lambda^{-1}} & X^t \end{array}$$

Note that in general the arrow λ^{-1} only exists in the category of abelian varieties up to isogeny; unless λ is a principal polarization it does not exist as a true homomorphism $X^t \to X$. If we want to stay in the usual category of abelian varieties, consider a homomorphism $\mu\colon X^t \to X$ such that $\mu \circ \lambda = [n]_X$ for some $n > 0$, and write $f = (1/m) \cdot g$ for some $g \in \mathrm{End}(X)$ and $m \in \mathbb{Z}_{>0}$. Then $h := \mu \circ g^t \circ \lambda$ is a true endomorphism of X, and by definition we have $f^\dagger := (1/mn) \cdot h \in \mathrm{End}^0(X)$.

It is readily checked that the map $\dagger\colon \mathrm{End}^0(X) \to \mathrm{End}^0(X)$ given by $f \mapsto f^\dagger$ is additive, that $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$, and that $(f^\dagger)^\dagger = f$. Hence $\dagger$ is an involution of the algebra $\mathrm{End}^0(X)$. It is called the *Rosati involution* associated to λ.

Note that $\dagger$ does not necessarily preserve the subring $\mathrm{End}(X) \subset \mathrm{End}^0(X)$, but if λ is a principal polarization then of course it does.

The Rosati involution depends on the chosen polarization. If $\mu\colon X \to X^t$ is another polarization then $\alpha := \lambda^{-1} \circ \mu$ is a well-defined element of $\mathrm{End}^0(X)$, and we can write $\mu = \lambda \circ \alpha$. If $f \mapsto f^\ddagger$ is the Rosati involution associated to μ then $f^\ddagger = \alpha^{-1} \circ f^\dagger \circ \alpha$.

Note that $\deg(f^\dagger) = \deg(f)$ for all f. As $[n]_X^\dagger = [n]_X$, it follows that in fact $P_{f^\dagger} = P_f$; in particular also $\mathrm{trace}(f^\dagger) = \mathrm{trace}(f)$.

(12.24) Lemma. *Let X be an abelian variety over a field k. Let ℓ be a prime number with $\ell \neq \mathrm{char}(k)$. Let $\lambda\colon X \to X^t$ be a homomorphism, $f \mapsto f^\dagger$ the associated Rosati involution, and let $E^\lambda\colon V_\ell X \times V_\ell X \to \mathbb{Q}_\ell(1)$ be the Riemann form of λ. Then for all $f \in \mathrm{End}(X)$ and all x, $y \in V_\ell X$ we have*

$$E^\lambda\big(V_\ell f(x), y\big) = E^\lambda\big(x, V_\ell f^\dagger(y)\big)\,.$$

In other words, if $\varphi \mapsto \varphi^*$ is the adjoint involution on $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell X)$ associated to the pairing E^λ, then the map $V_\ell\colon \mathrm{End}^0(X) \to \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell X)$ is a $*$-homomorphism of algebras with involution.

Proof. Let $E\colon V_\ell X \times V_\ell X^t \to \mathbb{Q}_\ell$ be the $\mathbb{Q}_\ell$-linear extension of the pairing defined in (11.23), so that $E^\lambda(x, y) = E\big(x, V_\ell\lambda(y)\big)$.

By definition of the Rosati involution we have $V_\ell\lambda \circ V_\ell f^\dagger = V_\ell(\lambda \circ f^\dagger) = V_\ell f^t \circ V_\ell\lambda$. Hence

$$E^\lambda\big(x, V_\ell f^\dagger(y)\big) = E\big(x, V_\ell f^t \circ V_\ell\lambda(y)\big)\,.$$

By (i) of Prop. (11.21) this equals $E(V_\ell f(x), V_\ell \lambda(y)) = E^\lambda\big(V_\ell f(x), y\big)$. □

(12.25) Proposition. *Let X be an abelian variety over a field k. Let λ be a polarization of X, and let $f \mapsto f^\dagger$ be the associated Rosati involution on* $\mathrm{End}^0(X)$. *Then the map* $\mathrm{NS}(X) \to \mathrm{End}^0(X)$ *given by* $[M] \mapsto \lambda^{-1} \circ \varphi_M$ *induces an isomorphism of $\mathbb{Q}$-vector spaces*

$$i\colon \mathrm{NS}(X) \otimes \mathbb{Q} \xrightarrow{\sim} \left\{ f \in \mathrm{End}^0(X) \;\middle|\; f = f^\dagger \right\}.$$

In particular, the Picard number of X equals the $\mathbb{Q}$-dimension of the space of $\dagger$-symmetric elements in $\mathrm{End}^0(X)$.

Proof. By Cor. (11.3) the map $[M] \mapsto \varphi_M$ gives an isomorphism $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{symm}}(X, X^t)$; hence also $\mathrm{NS}(X) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{Hom}^{0,\mathrm{symm}}(X, X^t)$. Now consider the isomorphism $\mathrm{End}^0(X) \xrightarrow{\sim} \mathrm{Hom}^0(X, X^t)$ given by $f \mapsto \lambda \circ f$. Using that $\lambda = \lambda^t$ one easily checks that under this isomorphism the $\dagger$-symmetric elements of $\mathrm{End}^0(X)$ correspond with the symmetric elements in $\mathrm{Hom}^0(X, X^t)$. □

(12.26) Theorem. (Positivity of the Rosati involution) *Let X be an abelian variety of dimension g over a field k. Let $\dagger$ be the Rosati involution associated to a polarization λ.*

(i) *If $\lambda = \varphi_L$ for some ample bundle L then for $f \in \mathrm{End}(X)$ we have*

$$\mathrm{trace}(f f^\dagger) = 2g \cdot \frac{c_1(L)^{g-1} \cdot c_1(f^*L)}{c_1(L)^g}.$$

(ii) *The bilinear form* $\mathrm{End}^0(X) \times \mathrm{End}^0(X) \to \mathbb{Q}$ *given by* $(f, g) \mapsto \mathrm{trace}(f \cdot g^\dagger)$ *is symmetric and positive definite.*

Part (ii) of the theorem can be reformulated by saying that the Rosati involution is a positive involution; see Appendix A, (A.11).

Proof. (i) By Prop. (7.6) we have $\varphi_{f^*L} = f^t \circ \varphi_L \circ f$. Hence for all $n \in \mathbb{Z}$ we get

$$\begin{aligned} \deg(\varphi_{f^*L^{-1} \otimes L^n}) &= \deg(n\varphi_L - \varphi_{f^*L}) \\ &= \deg(n\varphi_L - f^t \varphi_L f) \\ &= \deg(\varphi_L n - \varphi_L f^\dagger f) \\ &= \deg(\varphi_L) \cdot \deg(n - f^\dagger f) = \chi(L)^2 \cdot P_{f^\dagger f}(n). \end{aligned} \tag{4}$$

Let $Q \in \mathbb{Q}[t]$ be the polynomial (of degree g) such that $Q(n) = \big(n\, c_1(L) - c_1(f^*L)\big)^g$ for all n. Concretely, $Q = \sum_{j=0}^g b_j t^j$ with $b_j = \binom{g}{j}(-1)^{g-j} \cdot \big(c_1(L)^j \cdot c_1(f^*L)^{g-1}\big)$. By Riemann-Roch (9.11), $\deg\big(\varphi_{f^*L^{-1} \otimes L^n}\big) = \chi(f^*L^{-1} \otimes L^n)^2 = Q(n)^2$. Comparing with (4) we find that

$$P_{f^\dagger f} = \big(\chi(L)^{-1} \cdot Q\big)^2$$

as polynomials. Comparing coefficients in degree $2g - 1$ this gives

$$\begin{aligned} \mathrm{trace}(f f^\dagger) = \mathrm{trace}(f^\dagger f) &= -2\chi(L)^{-1} \cdot b_g \cdot b_{g-1} \\ &= 2\chi(L)^{-1} \cdot c_1(L)^g \cdot g \cdot \big(c_1(L)^{g-1} \cdot c_1(f^*L)\big) \\ &= 2g \cdot \big(c_1(L)^{g-1} \cdot c_1(f^*L)\big). \end{aligned}$$

(ii) Symmetry of the form follows from the fact, noted in (12.23), that $\mathrm{trace}(h^\dagger) = \mathrm{trace}(h)$. To see that $\mathrm{trace}(ff^\dagger) > 0$ for all $f \neq 0$ we may assume that $k = \overline{k}$ and write $\lambda = \varphi_L$ for some ample bundle L. As $f \mapsto \mathrm{trace}(ff^\dagger)$ is homogeneous of degree 2, we may further assume that f is a true endomorphism. Now use (i) and apply Lemma (12.9). □

§ 4. *The Albert classification.*

(12.27) Let X be a simple abelian variety over a field k, and choose a polarization λ. To the pair (X, λ) we associate the pair $(D, \dagger)$ with $D = \mathrm{End}^0(X)$ the endomorphism algebra and $\dagger$ the Rosati involution. We know that D is a simple $\mathbb{Q}$-algebra of finite dimension and that $\dagger$ is a positive involution.

Let K be the center of D (so that D is a central simple K-algebra), and let $K_0 := \{x \in K \mid x^\dagger = x\}$ be the subfield of symmetric elements in K. We know that either $K_0 = K$, in which case $\dagger$ is said to be of the first kind, or that $K_0 \subset K$ is a quadratic extension, in which case $\dagger$ is said to be of the second kind.

By a theorem of Albert (see Appendix???) the pair $(D, \dagger)$ is of one of four types. For convenience we again describe the possibilities. Recall that if A is a quaternion algebra over a field L, its canonical involution is the involution given by $a \mapsto \mathrm{Trd}_{A/L}(a) - a$. We write $\mathbb{H}$ for the Hamiltonian quaternion algebra over $\mathbb{R}$.

Type I: $K_0 = K = D$ is a totally real field.
$\dagger = \mathrm{id}_D$.

Type II: $K_0 = K$ is a totally real field, and D is a quaternion algebra over K with $D \otimes_{K,\sigma} \mathbb{R} \cong M_2(\mathbb{R})$ for every embedding $\sigma\colon K \to \mathbb{R}$.

Let $d \mapsto d^*$ be the canonical involution on D. Then there exists an element $a \in D$ such that $a^2 \in K$ is totally negative, and such that $d^\dagger = ad^*a^{-1}$ for all $d \in D$.

We have an isomorphism $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{\sigma\colon K \to \mathbb{R}} M_2(\mathbb{R})$ such that the involution $\dagger$ on $D \otimes_{\mathbb{Q}} \mathbb{R}$ corresponds to the involution $(A_1, \ldots, A_e) \mapsto (A_1^t, \ldots, A_e^t)$.

Type III: $K_0 = K$ is a totally real field, and D is a quaternion algebra over K with $D \otimes_{K,\sigma} \mathbb{R} \cong \mathbb{H}$ for every embedding $\sigma\colon K \to \mathbb{R}$.

$\dagger$ is the canonical involution on D.

We have an isomorphism $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{\sigma\colon K \to \mathbb{R}} \mathbb{H}$ such that the involution $\dagger$ on $D \otimes_{\mathbb{Q}} \mathbb{R}$ corresponds to the involution $(\alpha_1, \ldots, \alpha_e) \mapsto (\bar{\alpha}_1, \ldots, \bar{\alpha}_e)$.

Type IV: K_0 is a totally real field, K is a totally imaginary quadratic field extension of K. Write $a \mapsto \bar{a}$ for the unique non-trivial automorphism of K over K_0; this automorphism is usually referred to as complex conjugation. If v is a finite place of K, write $\bar{v}$ for its complex conjugate. The algebra D is a central simple algebra over K such that: (a) If v is a finite place of K with $v = \bar{v}$ then $\mathrm{inv}_v(D) = 0$; (b) For any place v of K we have $\mathrm{inv}_v(D) + \mathrm{inv}_{\bar{v}}(D) = 0$ in $\mathbb{Q}/\mathbb{Z}$.

If m is the degree of D as a central simple K-algebra, we have an isomorphism $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{\sigma\colon K_0 \to \mathbb{R}} M_m(\mathbb{C})$ such that the involution $\dagger$ on $D \otimes_{\mathbb{Q}} \mathbb{R}$ corresponds to the involution $(A_1, \ldots, A_{e_0}) \mapsto (\overline{A}_1^t, \ldots, \overline{A}_{e_0}^t)$.

(12.28) Retaining the notation and assumptions of (12.27), write

$$e_0 := [K_0 : \mathbb{Q}]\,, \qquad e := [K : \mathbb{Q}]\,, \quad \text{and} \quad m := [D : K]^{1/2}\,.$$

(So m is just the degree of D as a central simple K-algebra.)

Write $D^{\mathrm{symm}} := \{d \in D \mid d^\dagger = d\}$. By Prop. (12.25), the Picard number $\rho(X) := \operatorname{rank} \mathrm{NS}(X)$ can be calculated as $\rho(X) = \eta \cdot \dim_{\mathbb{Q}}(D) = \eta \cdot em^2$, where

$$\eta := \frac{\dim_{\mathbb{Q}}(D^{\mathrm{symm}})}{\dim_{\mathbb{Q}}(D)}\,.$$

For each of the types the factor η is easily calculated from the given description of $D \otimes_{\mathbb{Q}} \mathbb{R}$. We find that $\eta = 1$ for Type I, $\eta = 3/4$ for Type II, $\eta = 1/4$ for Type III, and $\eta = 1/2$ for Type IV.

The invariants involved can be summarized as follows.

Type I	Type II	Type III	Type IV
D	D	D	D
$\Vert$	$\vert_4$	$\vert_4$	$\vert_{m^2}$
K	K	K	K
$\Vert$	$\Vert$	$\Vert$	$\vert_2$
K_0	K_0	K_0	K_0
$\vert_{e_0=e}$	$\vert_{e_0=e}$	$\vert_{e_0=e}$	$\vert_{e_0}$
$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$
$\rho = e$	$\rho = 3e$	$\rho = e$	$\rho = e_0m^2$

As we shall prove next, there are some numerical restrictions on e_0, e and d in relation to $g = \dim(X)$. In case $\mathrm{char}(k) = 0$ the restrictions are a little stronger than when $\mathrm{char}(k) = p > 0$.

Exercises.

(12.1) Let X and Y be abelian varieties over a field k.

(i) If ℓ is a prime number with $\ell \neq \mathrm{char}(k)$, show that an element $f \in \mathrm{Hom}^0(X, Y)$ is a quasi-isogeny if and only if $V_\ell(f)$: $V_\ell X \to V_\ell Y$ is an isomorphism.

(ii) If $\mathrm{char}(k) = p$, show that an element $f \in \mathrm{Hom}(X, Y)$ is an isogeny if and only if the induced homomorphism $f[p^\infty]$: $X[p^\infty] \to Y[p^\infty]$ is an isogeny.

(12.2) Let X and Y be abelian varieties over a field k. Let $k \subset K$ be a field extension.

(i) Show that the natural map $\mathrm{Hom}_k(X, Y) \hookrightarrow \mathrm{Hom}_K(X_K, Y_K)$ has a torsion-free cokernel.

(ii) If $\mathrm{End}^0_k(X) = \mathrm{End}^0_K(X_K)$, show that also $\mathrm{End}_k(X) = \mathrm{End}_K(X_K)$.

Notes. In the proof of Thm. (12.2) one has to pay attention in the case of a non-perfect ground field, as it is not a priori clear that (in the notation of our proof) W^0_{red} is an abelian subvariety of X. In some papers this point is overlooked; see e.g. Milne [1], proof of 12.1.