Bas Edixhoven
Gerard van der Geer
Ben Moonen

ABELIAN VARIETIES

(PRELIMINARY VERSION OF THE FIRST CHAPTERS)

Contents

Notation and conventions.

FieldsNot **(0.1)** In general, k denotes an arbitrary field, $\bar{k}$ denotes an algebraic closure of k, and k_s a separable closure.

A=SpecA **(0.2)** If A is a commutative ring, we sometimes simply write A for $\mathrm{Spec}(A)$. Thus, for instance, by an A-scheme we mean a scheme over $\mathrm{Spec}(A)$. If $A \to B$ is a homomorphism of rings and X is an A-scheme then we write $X_B = X \times_A B$ rather than $X \times_{\mathrm{Spec}(A)} \mathrm{Spec}(B)$.

SchemesNot **(0.3)** If X is a scheme then we write $|X|$ for the topological space underlying X and O_X for its structure sheaf. If $f\colon X \to Y$ is a morphism of schemes we write $|f|\colon |X| \to |Y|$ and $f^\sharp\colon O_Y \to f_*O_X$ for the corresponding map on underlying spaces, resp. the corresponding homomorphism of sheaves on Y. If $x \in |X|$ we write $k(x)$ for the residue field. If X is an integral scheme we write $k(X)$ for its field of rational functions.

If S is a scheme and X and T are S-schemes then we write $X(T)$ for the set of T-valued points of X, i.e., the set of morphisms of S-schemes $T \to X$. Often we simply write X_T for the base change of X to T, i.e., $X_T := X \times_S T$, to be viewed as a T-scheme via the canonical morphism $X_T \to T$.

VarietyDef **(0.4)** If k is a field then by a *variety over* k we mean a separated k-scheme of finite type which is geometrically integral. Recall that a k-scheme is said to be geometrically integral if for some algebraically closed field K containing k the scheme X_K is irreducible and reduced. By EGA IV, (4.5.1) and (4.6.1), if this holds for some algebraically closed overfield K then X_K is integral for every field K containing k. A variety of dimension 1 (resp. 2, resp. $n \geqslant 3$) is called a *curve* (resp. *surface*, resp. *n-fold*).

By a *line bundle* (resp. a *vector bundle of rank d*) on a scheme X we mean a locally free O_X-module of rank 1 (resp. of rank d). By a *geometric vector bundle of rank d* on X we mean a group scheme $\pi\colon \mathbb{V} \to X$ over X for which there exists a affine open covering $X = \cup U_\alpha$ such that the restriction of $\mathbb{V}$ to each U_α is isomorphic to $\mathbb{G}_a^d$ over U_α. In particular this means that we have isomorphisms of U_α-schemes $\varphi_\alpha\colon \pi^{-1}(U_\alpha) \xrightarrow{\sim} U_\alpha \times \mathbb{A}^d$, such that all transition morphisms

$$t_{\alpha,\beta}\colon U_{\alpha,\beta} \times \mathbb{A}^d \xrightarrow{\varphi_\beta \circ \varphi_\alpha^{-1}} U_{\alpha,\beta} \times \mathbb{A}^d$$

are linear automorphisms of $U_{\alpha,\beta} \times \mathbb{A}^d$ over $U_{\alpha,\beta} := U_\alpha \cap U_\beta$; this last condition means that $t_{\alpha,\beta}$ is given by a $O(U_{\alpha,\beta})$-linear automorphism of $O(U_{\alpha,\beta})[x_1, \ldots, x_d]$. For $d = 1$ we obtain the notion of a *geometric line bundle*.

If $\mathbb{V}$ is a geometric vector bundle of rank d on X then its sheaf of sections is a vector bundle of rank d. Conversely, if $\mathscr{E}$ is a vector bundle of rank d on X then the scheme $\mathbb{V} := \mathrm{Spec}\left(\mathrm{Sym}(\mathscr{E}^\vee)\right)$ has a natural structure of a geometric vector bundle of rank d. These two constructions are quasi-inverse to each other and establish an equivalence between vector bundles and geometric vector bundles.

EtaleDef **(0.5)** In our definition of an étale morphism of schemes we follow EGA; this means that we only require the morphism to be locally of finite type. Note that in some literature étale morphisms are assumed to be quasi-finite. Thus, for instance, if S is a scheme and I is an index set, the disjoint union $\coprod_{i \in I} S$ is étale over S according to our conventions, also if the set I is infinite.

NumbFieldVal **(0.6)** If K is a number field then by a *prime of* K we mean an equivalence class of valuations of K. See for instance Neukirch [1], Chap. 3. The finite primes of K are in bijection with the maximal ideals of the ring of integers O_K. An infinite prime corresponds either to a real embedding $K \hookrightarrow \mathbb{R}$ or to a pair $\{\iota, \bar{\iota}\}$ of complex embeddings $K \hookrightarrow \mathbb{C}$.

If v is a prime of K, we have a corresponding homomorphism $\mathrm{ord}_v\colon K^* \to \mathbb{R}$ and a normalized absolute value $\| \ \|_v$. If v is a finite prime then we let ord_v be the corresponding valuation, normalized such that $\mathrm{ord}_v(K^*) = \mathbb{Z}$, and we define $\| \ \|_v$ by

$$\|x\|_v := \begin{cases} (q_v)^{-\mathrm{ord}_v(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0, \end{cases}$$

where q_v is the cardinality of the residue field at v. If v is an infinite prime then we let

$$\|x\|_v = \begin{cases} |\iota(x)| & \text{if } v \text{ corresponds to a real embedding } \iota\colon K \to \mathbb{R}, \\ |\iota(x)|^2 & \text{if } v \text{ corresponds to a pair of complex embeddings } \{\iota, \bar{\iota}\}, \end{cases}$$

and we define ord_v by the rule $\mathrm{ord}_v(x) := -\log\big(|\iota(x)|\big)$. Here $|\ |\colon \mathbb{C} \to \mathbb{R}_{\geqslant 0}$ is given by $|a+bi| = \sqrt{a^2+b^2}$.

Definition. Let p be a prime number. We say that a scheme X has characteristic p if the unique morphism $X \to \mathrm{Spec}(\mathbb{Z})$ factors through $\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$. This is equivalent to the requirement that $p \cdot f = 0$ for every open $U \subset X$ and every $f \in O_X(U)$. We say that a scheme X has characteristic 0 if $X \to \mathrm{Spec}(\mathbb{Z})$ factors through $\mathrm{Spec}(\mathbb{Q}) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$. This is equivalent to the requirement that $n \in O_X(U)^*$ for every $n \in \mathbb{Z} \setminus \{0\}$ and every open $U \subset X$.

Note that if $X \to Y$ is a morphism of schemes and Y has characteristic p (with p a prime number or $p = 0$) then X has characteristic p, too.

The absolute Frobenius. Let p be a prime number. Let Y be a scheme of characteristic p. Then we have a morphism $\mathrm{Frob}_Y \colon Y \to Y$, called the *absolute Frobenius morphism of* Y; it is given by
(a) Frob_Y is the identity on the underlying topological space $|Y|$;
(b) $\mathrm{Frob}_Y^\sharp \colon O_Y \to O_Y$ is given on sections by $f \mapsto f^p$.
To describe Frob_Y in another way, consider a covering $\{U_\alpha\}$ of Y by affine open subsets, say $U_\alpha = \mathrm{Spec}(A_\alpha)$. The endomorphism of A_α given by $f \mapsto f^p$ defines a morphism $\mathrm{Frob}_\alpha \colon U_\alpha \to U_\alpha$. On the intersections $U_\alpha \cap U_\beta$ the morphisms Frob_α and Frob_β agree, and by gluing we obtain the absolute Frobenius morphism Frob_Y of Y. Note that Frob_α is none other than the absolute Frobenius morphism of the scheme U_α.

One readily verifies that for any morphism $f \colon X \to Y$ of schemes of characteristic p we have a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Frob}_X} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{\mathrm{Frob}_Y} & Y \end{array} \quad . \tag{1}$$

AG:absFrob

The relative Frobenius. Let us now consider the relative situation, i.e., we fix a base scheme S and consider schemes over S. If $\pi \colon X \to S$ is an S-scheme then in general the absolute Frobenius morphism Frob_X is *not* a morphism of S-schemes, unless for instance $S = \mathrm{Spec}(\mathbb{F}_p)$. To remedy this we define $\pi^{(p)} \colon X^{(p/S)} \to S$ to be the pull-back of $\pi \colon X \to S$ via $\mathrm{Frob}_S \colon S \to S$. Thus, by definition we have $X^{(p/S)} = S \times_{\mathrm{Frob}_S, S} X$ and we have a cartesian diagram

$$\begin{array}{ccc} X^{(p/S)} & \xrightarrow{h} & X \\ {\scriptstyle \pi^{(p)}}\downarrow & & \downarrow{\scriptstyle \pi} \\ S & \xrightarrow{\mathrm{Frob}_S} & S \end{array} \quad . \tag{2}$$

AG:X(p/S)

If there is no risk of confusion we often write $X^{(p)}$ for $X^{(p/S)}$; note however that in general this scheme very much depends on the base scheme S over which we are working.

As the diagram (2) is cartesian, the commutative diagram (1), applied with $Y = S$, gives a commutative diagram **(nog aanpassen)**

$$\begin{array}{ccccc} X & & & & \\ & \searrow F_{X/S} & & & \\ & & X^{(p/S)} & \xrightarrow{W} & X \\ & & {\scriptstyle \pi^{(p)}}\downarrow & & \downarrow{\scriptstyle \pi} \\ & & S & \xrightarrow{\mathrm{Frob}_S} & S \end{array} \quad . \tag{3}$$

AG:relFrob

The morphism of S-schemes $F_{X/S}\colon X \to X^{(p/S)}$ is called the *relative Frobenius morphism of X over S*. By its definition, $F_{X/S}$ is a morphism of S-schemes (in other words, $\pi^{(p)} \circ F_{X/S} = \pi$) and $W \circ F_{X/S}$ is the absolute Frobenius of X.

Example. Suppose $S = \mathrm{Spec}(R)$ and $X = \mathrm{Spec}\big(R[t_1, \ldots, t_m]/I\big)$ for some ideal $I = (f_1, \ldots, f_n) \subset R[t_1, \ldots, t_m]$. Let $f_i^{(p)} \in R[t_1, \ldots, t_m]$ be the polynomial obtained from f_i by raising all coefficients (but not the variables!) to the pth power. Thus, if, in multi-index notation, $f_i = \sum c_\alpha t^\alpha$ then $f_i^{(p)} = \sum c_\alpha^p t^\alpha$. Then $X^{(p)} = \mathrm{Spec}\big(R[t_1, \ldots, t_m]/I^{(p)}\big)$ with $I^{(p)} = (f_1^{(p)}, \ldots, f_n^{(p)})$, and the relative Frobenius morphism $F_{X/S}\colon X \to X^{(p)}$ is given on rings by the homomorphism

$$R[t_1, \ldots, t_m]/I^{(p)} \longrightarrow R[t_1, \ldots, t_m]/I$$

with $r \mapsto r$ for all $r \in R$ and $t_j \mapsto t_j^p$. Note that this is a well-defined homomorphism.

The morphism $W\colon X^{(p)} \to X$ that appears in (3) does not have a standard name in the literature. As one easily checks (see Exercise ??), $\mathrm{Frob}_{X/S} \circ W\colon X^{(p)} \to X^{(p)}$ equals the absolute Frobenius morphism of $X^{(p)}$. Since an absolute Frobenius morphism is the identity on the underlying topological space, it follows that $F_{X/S}\colon X \to X^{(p)}$ induces a homeomorphism $|X| \xrightarrow{\sim} |X^{(p)}|$.

Formation of the relative Frobenius morphism is compatible with base change. This statement means the following. Let $\pi\colon X \to S$ be an S-scheme. Let $T \to S$ be another scheme over S, and consider the morphism $\pi_T\colon X_T \to T$ obtained from π by base-change. The first observation is that $(X_T)^{(p/T)}$ is canonically isomorphic to $(X^{(p/S)})_T$. Identifying the two schemes, the relative Frobenius $F_{X_T/T}$ of X_T over T is equal to the pull-back $(F_{X/S})_T$ of the relative Frobenius of X over S. Proofs of these assertions are left to the reader.

The absolute and relative Frobenii can be iterated. For the absolute Frobenius this is immediate: $\mathrm{Frob}_Y^n\colon Y \to Y$ is simply the nth iterate of Frob_Y. The nth iterate of the relative Frobenius is a morphism $F_{X/S}^n\colon X \to X^{(p^n/S)}$. Its definition is an easy generalization of the definition of $F_{X/S}$. Namely, we define $\pi^{(p^n)}\colon X^{(p^n/S)} \to S$ as the pull-back of $\pi\colon X \to S$ via Frob_S^n. Then Frob_X^n factors as

$$X \xrightarrow{F_{X/S}^n} X^{(p^n/S)} \xrightarrow{h^{(n)}} X$$

with $\pi^{(p^n)} \circ F_{X/S}^n = \pi$. Alternatively,

$$X^{(p^2/S)} = \big(X^{(p/S)}\big)^{(p/S)}, \quad X^{(p^3/S)} = \big(X^{(p^2/S)}\big)^{(p/S)}, \quad \text{etc.},$$

and

$$F_{X/S}^n = \Big(X \xrightarrow{F_{X/S}} X^{(p)} \xrightarrow{F_{X^{(p)}/S}} X^{(p^2)} \longrightarrow \cdots \xrightarrow{F_{X^{(p^{n-1})}/S}} X^{(p^n)}\Big).$$

The geometric Frobenius. Suppose $S = \mathrm{Spec}(\mathbb{F}_q)$, with $q = p^n$. If X is an S-scheme then the nth iterate of the absolute Frobenius morphism $\mathrm{Frob}_X^n\colon X \to X$ is a morphism of S-schemes. In fact, $\mathrm{Frob}_X^n = F_{X/S}^n$. We refer to $\pi_X := \mathrm{Frob}_X^n$ as the *geometric* Frobenius of X.

More generally, suppose that S is a scheme over $\mathrm{Spec}(\mathbb{F}_q)$. If X is an S-scheme then by an *$\mathbb{F}_q$-structure on X* we mean a scheme $X_0 \to \mathrm{Spec}(\mathbb{F}_q)$ together with an isomorphism of S-schemes $X_0 \otimes_{\mathbb{F}_q} S \cong X$. In practice we usually encounter this notion in the situation that $S = \mathrm{Spec}(K)$, where $\mathbb{F}_q \subset K$ is a field extension. Given an $\mathbb{F}_q$-structure on X, the geometric Frobenius morphism π_{X_0} induces, by extension of scalars, a morphism $\pi_X\colon X \to X$; we again refer to this morphism as the geometric Frobenius of X (relative to the given $\mathbb{F}_q$-structure).

An abelian variety is a complete algebraic variety whose points form a group, in such a way that the maps defining the group structure are given by morphisms. It is the analogue in algebraic geometry of the concept of a compact complex Lie group. To give a more precise definition of a abelian variety we take a suitable definition of a group and translate it into the language of complete varieties.

GroupDef **(1.1) Definition.** A *group* consists of a set G together with maps

$$m\colon G \times G \to G \quad \text{(the group law)} \qquad \text{and} \qquad i\colon G \to G \quad \text{(the inverse)}$$

and a distinguished element

$$e \in G \quad \text{(the identity element)}$$

such that we have the following equalities of maps.

(i) Associativity: $m \circ (m \times \mathrm{id}_G) = m \circ (\mathrm{id}_G \times m)\colon G \times G \times G \longrightarrow G$.

(ii) Defining property of the identity element:

$$m \circ (e \times \mathrm{id}_G) = j_1\colon \{e\} \times G \longrightarrow G\,, \qquad \text{and}$$
$$m \circ (\mathrm{id}_G \times e) = j_2\colon G \times \{e\} \longrightarrow G\,,$$

where j_1 and j_2 are the canonical identifications $\{e\} \times G \xrightarrow{\sim} G$ and $G \times \{e\} \xrightarrow{\sim} G$, respectively, and where we write e for the inclusion map $\{e\} \hookrightarrow G$.

(iii) Left and right inverse:

$$e \circ \pi = m \circ (\mathrm{id}_G \times i) \circ \Delta_G = m \circ (i \times \mathrm{id}_G) \circ \Delta_G\colon\ G \longrightarrow G\,,$$

where $\pi\colon G \to \{e\}$ is the constant map and $\Delta_G\colon G \to G \times G$ is the diagonal map.

Written out in diagrams, we require the commutativity of the following diagrams.

(i) Associativity:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mathrm{id}_G \times m} & G \times G \\ {\scriptstyle m \times \mathrm{id}_G}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array}\,.$$

(ii) Identity element:

$$\begin{array}{ccc} \{e\} \times G & \xrightarrow{e \times \mathrm{id}_G} & G \times G \\ {\scriptstyle j_1}\searrow & & \swarrow{\scriptstyle m} \\ & G & \end{array} \qquad \text{and} \qquad \begin{array}{ccc} G \times \{e\} & \xrightarrow{\mathrm{id}_G \times e} & G \times G \\ {\scriptstyle j_2}\searrow & & \swarrow{\scriptstyle m} \\ & G & \end{array}\,.$$

(iii) Two-sided inverse:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & \{e\} \\ {\scriptstyle (\mathrm{id}_G, i)}\downarrow & & \downarrow{\scriptstyle e} \\ G \times G & \xrightarrow[m]{} & G \end{array} \qquad \text{and} \qquad \begin{array}{ccc} G & \xrightarrow{\pi} & \{e\} \\ {\scriptstyle (i, \mathrm{id}_G)}\downarrow & & \downarrow{\scriptstyle e} \\ G \times G & \xrightarrow[m]{} & G \end{array}\,.$$

To simplify notation, one often simply writes the symbol G instead of the quadruple (G, m, i, e), assuming it is clear what m, i and e are.

Adapting this definition to the category of varieties, we obtain the definition of a group variety.

GrVarDef **(1.2) Definition.** A *group variety* over a field k is a k-variety X together with k-morphisms

$$m\colon X \times X \to X \quad \text{(the group law)} \qquad \text{and} \qquad i\colon X \to X \quad \text{(the inverse)}$$

and a k-rational point

$$e \in X(k) \quad \text{(the identity element)}$$

such that we have the following equalities of morphisms:

(i)
$$m \circ (m \times \mathrm{id}_X) = m \circ (\mathrm{id}_X \times m)\colon X \times X \times X \longrightarrow X\,.$$

(ii)
$$m \circ (e \times \mathrm{id}_X) = j_1\colon \operatorname{Spec}(k) \times X \longrightarrow X \qquad \text{and}$$
$$m \circ (\mathrm{id}_X \times e) = j_2\colon X \times \operatorname{Spec}(k) \longrightarrow X\,,$$

where $j_1\colon \operatorname{Spec}(k) \times X \xrightarrow{\sim} X$ and $j_2\colon X \times \operatorname{Spec}(k) \xrightarrow{\sim} X$ are the canonical isomorphisms.

(iii)
$$e \circ \pi = m \circ (\mathrm{id}_X \times i) \circ \Delta_{X/k} = m \circ (i \times \mathrm{id}_X) \circ \Delta_{X/k}\colon\ X \longrightarrow X\,,$$

where $\pi\colon X \to \operatorname{Spec}(k)$ is the structure morphism.

Note that, since we are working with varieties, checking equality of two morphisms as in (i)–(iii) can be done on $\overline{k}$-rational points.

If X is a group variety then the set $X(k)$ of k-rational points naturally inherits the structure of a group. More generally, if T is any k-scheme then the morphisms m, i and e induce a group structure on the set $X(T)$ of T-valued points of X. In this way, the group variety X defines a contravariant functor from the category of k-schemes to the category of groups. In practice it is often most natural to use this "functorial" point of view; we shall further discuss this in Chapter III.

We can now define the main objects of study in this book.

AbVardef **(1.3) Definition.** An *abelian variety* is a group variety which, as a variety, is complete.

As we shall see, the completeness condition is crucial: abelian varieties form a class of group varieties with very special properties.

A group is a homogeneous space over itself, either via left or via right translations. We have this concept here too.

TranslDef **(1.4) Definition.** Let X be a group variety over a field k, and let $x \in X(k)$ be a k-rational point. We define the *right translation* $t_x\colon X \to X$ and the *left translation* $t'_x\colon X \to X$ to be the compositions

$$t_x = \big(X \cong X \times_k \operatorname{Spec}(k) \xrightarrow{\mathrm{id}_X \times x} X \times_k X \xrightarrow{m} X\big)\,,$$

and

$$t'_x = \big(X \cong \operatorname{Spec}(k) \times_k X \xrightarrow{x \times \mathrm{id}_X} X \times_k X \xrightarrow{m} X\big)\,.$$

On points, these maps are given by $t_x(y) = m(y,x)$ and $t'_x(y) = m(x,y)$.

More generally, if T is a scheme over $\mathrm{Spec}(k)$ and $x \in X(T)$ is a T-valued point of X then we define the right and left translations $t_x\colon X_T \to X_T$ and $t'_x\colon X_T \to X_T$ (with $X_T := X \times_k T$) to be the compositions

$$t_x = \left(X_T \cong X_T \times_T T \xrightarrow{\mathrm{id}_{X_T} \times x_T} X_T \times_T X_T \xrightarrow{m} X_T\right),$$

and

$$t'_x = \left(X_T \cong T \times_T X_T \xrightarrow{x_T \times \mathrm{id}_{X_T}} X_T \times_T X_T \xrightarrow{m} X_T\right),$$

where we write $x_T\colon T \to X_T$ for the morphism $(x, \mathrm{id}_T)\colon T \to X \times_k T = X_T$.

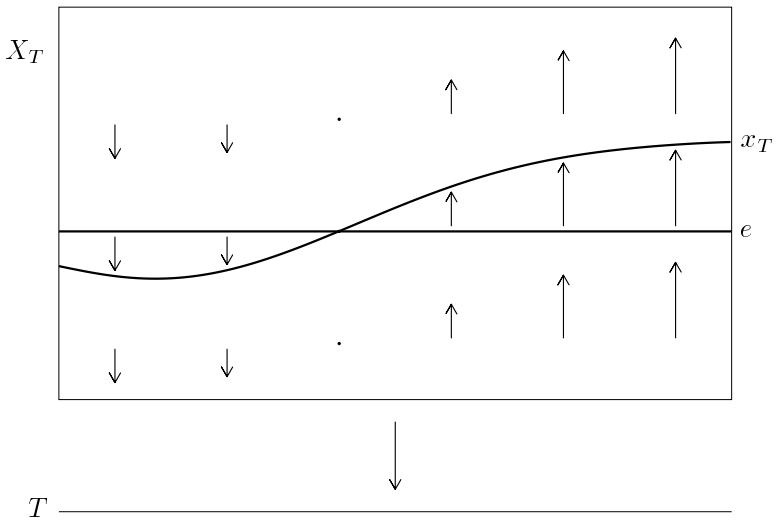


Figure 1.

Given a k-scheme T and two points $x, y \in X(T)$, one easily verifies that $t_y \circ t_x = t_{m(x,y)}$ and $t'_x \circ t'_y = t'_{m(x,y)}$. In particular, it follows that $t_{i(x)} = t_x^{-1}$ and $t'_{i(x)} = (t'_x)^{-1}$.

Geometrically, the fact that a group variety X is a principal homogenous space over itself has the consequence that X, as a variety over k, "looks everywhere the same". As a consequence we obtain that group varieties are smooth and have a trivial tangent bundle.

FreeTangent **(1.5) Proposition.** *Let X be a group variety over a field k. Then X is smooth over k. If we write $T_{X,e}$ for the tangent space at the identity element, there is a natural isomorphism $\mathcal{T}_{X/k} \cong T_{X,e} \otimes_k O_X$. This induces natural isomorphisms $\Omega^n_{X/k} \cong (\wedge^n T^\vee_{X,e}) \otimes_k O_X$. In particular, if $g = \dim(X)$ then $\Omega^g_{X/k} \cong O_X$.*

Proof. Since X is a variety, the smooth locus $\mathrm{sm}(X/k) \subset X$ is open and dense. It is also stable under all translations. Since these make X into a homogenous space over itself, it follows that $\mathrm{sm}(X/k) = X$.

Set $S = \mathrm{Spec}\left(k[\varepsilon]/(\varepsilon^2)\right)$. Let $X_S := X \times_k S$, which we may think of as a "thickened" version of X. Tangent vectors $\tau \in T_{X,e}$ correspond to S-valued points $\tilde{\tau}\colon S \to X$ which reduce to $e\colon \mathrm{Spec}(k) \to X$ modulo ε. (See Exercise 1.2.) A vector field on X is given by an automorphism $X_S \to X_S$ over S which reduces to the identity on X. To a tangent vector τ we can thus associate the vector field $\xi(\tau)$ given by the right translation $t_{\tilde{\tau}}$. The map $T_{X,e} \to \Gamma(X, \mathcal{T}_{X/k})$ given by $\tau \mapsto \xi(\tau)$ is k-linear and induces a homomorphism $\alpha\colon T_{X,e} \otimes_k O_X \to \mathcal{T}_{X/k}$.

We claim that α is an isomorphism. As it is a homomorphism between locally free O_X-modules of the same rank, it suffices to show that α is surjective. If $x \in X$ is a closed point then the map

$$(\alpha_x \bmod m_x)\colon T_{X,e} \otimes_k k(x) \longrightarrow (\mathcal{T}_{X/k})_x \otimes_{O_{X,x}} k(x) = T_{X,x}$$

is the map $T_{X,e} \to T_{X,x}$ induced on tangent spaces by t_x, which is an isomorphism. Applying the Nakayama Lemma, it follows that the map on stalks $\alpha_x\colon T_{X,e} \otimes_k O_{X,x} \to (\mathcal{T}_{X/k})_x$ is surjective. As this holds for all closed points x, it follows that α is surjective.

The last assertion of the proposition now follows from the identities $\Omega^1_{X/k} = \mathcal{T}^\vee_{X/k}$ and $\Omega^n_{X/k} = \wedge^n \Omega^1_{X/k}$. □

lobalVectFields **(1.6) Corollary.** *If X is an abelian variety, every global vector field ξ on X is left invariant, i.e., for every left translation t' we have $t'_*\xi = \xi$.*

Proof. With notation as in the proof of the proposition, note that $t_{\tilde{\tau}}$ commutes with all left translations. It follows that the vector field $\xi(\tau)$ is left invariant. The map $\tau \mapsto \xi(\tau)$ identifies $T_{X,e}$ with the space of left invariant vector fields on X. If X is an abelian variety, these are the only global vector fields on X, since $\Gamma(X, O_X) = k$. □

RatCurves **(1.7) Corollary.** *Any morphism from $\mathbb{P}^1$ to a group variety is constant.*

Proof. Consider a morphism $\varphi\colon \mathbb{P}^1 \to X$, with X a group variety. If φ is non-constant then its image $C \subset X$ is unirational, hence C is a rational curve. Replacing φ by the morphism $\widetilde{C} \to X$ (where $\widetilde{C}$ is the normalization of C), we are reduced to the case that the morphism φ is birational onto its image. Then there exists a point $y \in \mathbb{P}^1$ such that the map on tangent spaces $T_y\varphi\colon T_y\mathbb{P}^1 \to T_{\varphi(y)}X$ is non-zero. Since $\Omega^1_{X/k}$ is free we then can find a global 1-form $\omega \in \Gamma(X, \Omega^1_{X/k})$ such that $\varphi^*\omega$ does not vanish at y. Since $\Gamma(\mathbb{P}^1, \Omega^1_{\mathbb{P}^1/k}) = 0$ this is a contradiction. □

Before we give the first examples of abelian varieties, let us introduce some notation. Consider a smooth complete curve C over a field k. Note that by a curve we mean a variety of dimension 1; in particular, C is assumed to be geometrically reduced and irreducible. By a (Weil) divisor on C we mean a finite formal linear combination $D = m_1P_1 + \cdots + m_rP_r$, where $P_1, \ldots, P_r$ are mutually distinct closed points of C and where $m_1, \ldots, m_r$ are integers. The degree of such a divisor is defined to be $\deg(D) := m_1 \cdot [k(P_1) : k] + \cdots + m_r \cdot [k(P_r) : k]$. If $f \in k(C)^*$ is a non-zero rational function on C, we have an associated divisor $\mathrm{div}(f)$ of degree zero; such divisors are called principal. Two divisors D_1 and D_2 are said to be linearly equivalent, notation $D_1 \sim D_2$, if they differ by a principal divisor. The divisor class group $\mathrm{Cl}(C)$ is then defined to be the group of divisors modulo linear equivalence, with group law induced by addition of divisors. Associating to a divisor its degree gives a homomorphism $\deg\colon \mathrm{Cl}(C) \to \mathbb{Z}$. We set $\mathrm{Cl}^0(C) := \mathrm{Ker}(\deg)$, the class group of degree zero divisors on C.

A divisor $D = m_1P_1 + \cdots + m_rP_r$ is said to be effective, notation $D \geqslant 0$, if all coefficients m_i are in $\mathbb{Z}_{\geqslant 0}$. Given a divisor D on C, write $L(D) = \Gamma\big(C, O_C(D)\big)$ for the k-vector space of rational functions f on C such that $\mathrm{div}(f) + D \geqslant 0$. Also we write $\ell(D) = \dim_k \big(L(D)\big)$. Recall that the theorem of Riemann-Roch says that

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g\,,$$

where K is the canonical divisor class and g is the genus of C.

With these notations, we turn to elliptic curves, the classical examples of abelian varieties, and at the origin of the whole theory.

EllCurveExa **(1.8) Example.** We define an *elliptic curve* to be a complete, non-singular curve of genus 1 over a field k, together with a k-rational point. Let E be such a curve, and let $P \in E(k)$ be the distinguished rational point. The Riemann-Roch theorem tells us that $\ell(nP) := \dim_k \big(L(nP)\big) = n$ for $n \geqslant 1$.

We have $L(P) = k$. Choose a basis $1, x$ of $L(2P)$ and extend it to a basis $1, x, y$ of $L(3P)$. Since $\dim_k \big(L(6P)\big) = 6$, the seven elements $1, x, y, x^2, xy, y^2, x^3 \in L(6P)$ satisfy a linear relation. Looking at pole orders, we see that the terms y^2 and x^3 must both occur with a non-zero coefficient, and possibly after rescaling x and y by a unit we may assume that there is a relation of the form

DefBE:Weier $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad \text{with } a_i \in k\,. \tag{1}$$

The functions x and y define a rational map

$$E \dashrightarrow \mathbb{P}^2 \qquad \text{by} \quad a \mapsto \big(1 : x(a) : y(a)\big) \qquad \text{for } a \neq P\,.$$

This rational map extends to an embedding of E into $\mathbb{P}^2$ which sends P to $(0 : 1 : 0)$. It realizes E as the non-singular cubic curve in $\mathbb{P}^2$ given by the affine equation (1), called a Weierstrass equation for E. The non-singularity of this curve can be expressed by saying that a certain expression in the coefficients a_i, called the discriminant of the equation, is invertible. It is easily seen from (1) that the image of P is a flex point, i.e., a point where the tangent has a threefold intersection with the curve. (Alternatively, this is obvious from the fact that the embedding $E \hookrightarrow \mathbb{P}^2$ is given by the linear system $|3P|$.)

In order to define the structure of an abelian variety on E, let us first show that the map

$$\alpha\colon E(k) \to \mathrm{Cl}^0(E) \qquad \text{given by } Q \mapsto [Q - P]$$

is a bijection. If $\alpha(Q) = \alpha(Q')$ while $Q \neq Q'$, then Q and Q' are linearly equivalent and $\dim_k \big(L(Q)\big) \geqslant 2$, which contradicts Riemann-Roch. Thus α is injective. Conversely, if A is a divisor of degree zero then $\dim_k \big((L(A + P)\big) = 1$, so there exists an effective divisor of degree 1 which is linearly equivalent to $A + P$. This divisor is necessarily a k-rational point, say Q, and $\alpha(Q) = [A]$. This shows that α is a bijection.

We obtain a group structure on $E(k)$ by transporting the natural group structure on $\mathrm{Cl}^0(E)$ via α. Clearly, if $k \subset K$ is a field extension then the group laws obtained on $E(k)$ and $E_K(K) = E(K)$ are compatible, in the sense that the natural inclusion $E(k) \subset E(K)$ is a homomorphism. The point P is the identity element for the group law.

The group law just defined has the following geometric interpretation. To avoid confusion with the addition of divisors, we shall write $(A, B) \mapsto A \oplus B$ for the group law and $A \mapsto \ominus A$ for the inverse.

A+B+CLem **(1.9) Lemma.** *Let K be a field containing k. Let A, B and C be K-rational points of E. Then $A \oplus B \oplus C = P$ in the group $E(K)$ if and only if A, B and C are the three intersection points of E_K with a line.*

Proof. By construction, $A \oplus B \oplus C = P$ means that $A \oplus B \oplus C$ is linearly equivalent to $3P$. The lemma is therefore a reformulation of the fact that the embedding $E \hookrightarrow \mathbb{P}^2$ is given by the linear system $|3P|$. □

The addition of K-rational points is now given as follows. To add A and B one takes the line through A and B (by which we mean the tangent line to E at A if $A = B$). This line intersects E in a third point R (possibly equal to A or B). Note that if A and B are K-rational then so is R. Then one takes the line through R and P, which intersects E in a third point S. This is the sum of A and B. To see this, note that by the lemma we have the relations: $A \oplus B \oplus R = P$ and $R \oplus P \oplus S = P$. Since P is the identity element we get $A \oplus B = S$, as claimed. Similarly, the inverse of an element A is the third intersection point of E with the line through A and P.

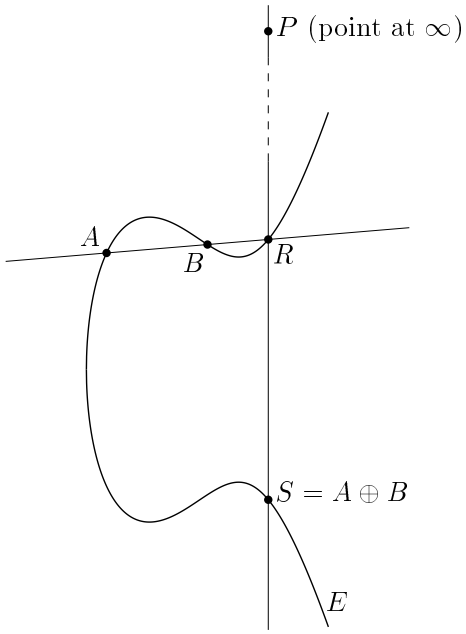


Figure 2.

We claim that the group structure on $E(K)$ comes from the structure of a group variety on E. In other words: we want to show that there exist morphisms $m\colon E \times E \to E$ and $i\colon E \to E$ such that the group structure on $E(K)$ is the one induced by m and i. To see this, let $k \subset K$ again be a field extension. If $A,\ B \in E(K)$ then $R = \ominus(A \oplus B)$ is the third intersection point of E with the line through A and B. Direct computation shows that if we work on an affine open subset $U \subset \mathbb{P}^2$ containing A and B then the projective coordinates of R can be expressed as polynomials, with coefficients in k, in the coordinates of A and B. This shows that $(A, B) \mapsto \ominus(A \oplus B)$ is given by a morphism $\varphi\colon E \times E \to E$. Taking $B = P$ we find that $A \mapsto \ominus A$ is given by a morphism $i\colon E \to E$, and composing φ and i we get the addition morphism m.

Explicit formulas for i and m can be found in Silverman [1], Chapter III, §2.

We conclude that the quadruple (E, m, i, P) defines an abelian variety of dimension 1 over k. As we have seen, abelian varieties have a trivial tangent bundle. Therefore, if X is a 1-dimensional abelian variety, it has genus 1: *abelian varieties of dimension 1 are elliptic curves*.

To get a feeling for the complexity of elliptic curves we take E to be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 + y = x^3 - x$, with origin $P_\infty = (0 : 1 : 0)$. Let Q be the rational point $(-1, -1)$. If for $n = 1, \ldots, 20$ we plot the coordinates of $n \cdot Q = Q \oplus \cdots \oplus Q$ as rational numbers, or even if we just plot the absolute value of the numerator of the x-coordinate we find a parabola shape which indicates that the "arithmetic complexity" of the point $n \cdot Q$

grows quadratically in n; see Figure 3. [**opmerking:** Verwijzen naar een plaats waar we dit verder bespreken. Zoals het er nu staat is het een losse flodder.]

1
6
20
1357
8385
12551561
1849037896
4881674119706
2786836257692691
79799551268268089761
280251129922563291422645
54202648602164057575419038802
32393368023905447401291531504800400
14256048814831828489707800904733974972 01
59692956540775884607815785047798822983634 0351
13565337063840965918878276933339623388477773474852 21
23897505191109140186309909376606354352699564527703566259 16
47551938020942325784141569050513811957803129798534598981096547726
43276783438948886312588030404441444313405755534366254416432880924019065
66655479518893093532610447590226207125008330695731551720689810858664307580428417

Figure 3.

g=2Exa **(1.10) Example.** Now we try to generalize the above example, taking a curve of genus 2. So, let C be a smooth projective curve of genus $g = 2$ over a field k. Then C is a hyperelliptic curve and can be described as a double cover $\pi\colon C \to \mathbb{P}^1_k$ of the projective line. Let i be the hyperelliptic involution of C. Consider the surface $C \times C$, on which we have an involution ι given by $(a, b) \mapsto (b, a)$. The quotient $C^{(2)} = (C \times C)/\iota$ is a non-singular surface that parametrizes the effective divisors of degree 2 on C; we shall give further details on this in Chapter 14, §2.

The image of the anti-diagonal $\Delta^- = \big\{\big(a, i(a)\big) \;\big|\; a \in C\big\}$ under the canonical map $C^2 \to C^{(2)}$ is a curve $Y \subset C^{(2)}$ which is isomorphic to $C/i = \mathbb{P}^1$ and has self-intersection number $\frac{1}{2}(\Delta^-)^2 = (2 - 2g)/2 = -1$; hence we find that Y is an exceptional curve. (Of course, Y is just the g^1_2 of canonical divisors on the curve, viewed as a subvariety of the variety $C^{(2)}$ of effective divisors of degree 2.) By elementary theory of algebraic surfaces we can blow Y down, obtaining a non-singular projective surface S.

Consider the map $\tilde{\alpha}\colon C^{(2)}(k) \to \mathrm{Cl}^0(C)$ given by $D \mapsto [D] - [K]$, where $[K]$ is the canonical divisor class. Since $\big[a + i(a)\big] = [K]$ for every $a \in C$, this map factors through the contraction of the curve Y and we get a map $\alpha\colon S(k) \to \mathrm{Cl}^0(C)$. We claim that α is bijective. If D_1 and D_2 are effective divisors of degree 2 with $\tilde{\alpha}(D_1) = \tilde{(}D_2)$ then clearly $D_1 \sim D_2$. If $D_1 \neq D_2$ then $\ell(D_i) \geqslant 2$ $(i = 1, 2)$; hence by Riemann-Roch the degree zero divisors $K - D_i$ are effective, which implies that D_1 and D_2 are canonical, i.e., D_1, $D_2 \in Y$. This shows that α is injective. It is surjective by Riemann-Roch.

Transporting the natural group structure on $\mathrm{Cl}^0(C)$ via α, we obtain a group structure on $S(k)$. The formation of this group structure is compatible with field extensions $k \subset K$. The identity element of $S(k)$ is the point $[K] \in C^{(2)}(k)$, which is the point obtained by contracting Y.

We claim that the addition and inverse on $S(k)$ are given by morphisms. For the inverse this is easy: using that $a + i(a) \sim K$ for all $a \in C(k)$ it follows that the inverse is the automorphism of S induced by the automorphism $(a, b) \mapsto \big(i(a), i(b)\big)$ of C^2.

To see that addition is given by a morphism, consider the projection $\pi\colon C^5 \to C^4$ onto the first four factors. This map has four natural sections $(p_1, p_2, p_3, p_4) \mapsto (p_1, \ldots, p_4, p_i)$, and this defines a relative effective divisor D of degree 4 on C^5 over C^4. Let K be a fixed canonical

divisor on the last factor C. By the Riemann-Roch theorem for the curve C over the function field $k(C^4)$ the divisor $D - K$ is linearly equivalent to an effective divisor of degreee 2 on C over $k(C^4)$. It follows that D is linearly equivalent to a divisor of the form $E + \pi^*(G)$, with E a relative effective divisor of degree 2 and G a divisor on C^4. For $P \in C^4$ the restriction of E to the fibre $\{P\} \times C$ is an effective divisor of degree 2, hence determines a point $\psi(P)$ of $C^{(2)}$. This gives a map $\psi\colon C^4 \to C^{(2)}$ which is clearly a morphism. If $\beta\colon C^{(2)} \to S$ is the blowing-down of $Y \subset C^{(2)}$ then the composition $\beta \circ \psi C^4 \to S$ factors through $\beta \times \beta$. The resulting morphism $S \times S \to S$ is precisely the addition on S. [**opmerking:** dit voorbeeld moet verder opgepoetst worden.]

The preceding two examples suggest that, given a smooth projective curve C over a field k, there should exist an abelian variety whose points parametrize the degree zero divisor classes on C. If C has a k-rational point then such an abelian variety indeed exists (as we shall see later), though the construction will not be as explicit and direct as in the above two examples. The resulting abelian variety is called the jacobian of the curve.

ComplToriExa **(1.11) Example.** In this example we work over the field $k = \mathbb{C}$. Consider a complex vector space V of finite dimension n. For an additive subgroup $L \subset V$ the following conditions are equivalent:

(i) $L \subset V$ is discrete and co-compact, i.e., the euclidean topology on V induces the discrete topology on L and the quotient $X := V/L$ is compact for the quotient topology;
(ii) the natural map $L \otimes_{\mathbb{Z}} \mathbb{R} \to V$ is bijective;
(iii) there is an $\mathbb{R}$-basis $e_1, \ldots, e_{2n}$ of V such that $L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_{2n}$.

A subgroup satisfying these conditions is called a *lattice* in V.

Given a lattice $L \subset V$, the quotient X naturally inherits the structure of a compact (complex analytic) Lie group. Lie groups of this form are called *complex tori*. (This usage of the word torus is not to be confused with its meaning in the theory of linear algebraic groups.)

Let us first consider the case $n = 1$. By a well-known theorem of Riemann, every compact Riemann surface is algebraic. Since X has genus 1, it can be embedded as a non-singular cubic curve in $\mathbb{P}^2_{\mathbb{C}}$, see (1.8). If $\varphi\colon X \hookrightarrow \mathbb{P}^2_{\mathbb{C}}$ is such an embedding, write $E = \varphi(X)$ and $P = \varphi(0 \bmod L)$. We see that (E, P) is an elliptic curve (taking P to be the identity element). The structure of a group variety on E as defined in (1.8) is the same as the group structure on X, in the sense that $\varphi\colon X \xrightarrow{\sim} E^{\mathrm{an}}$ is an isomorphism of Lie groups.

For $n \geqslant 2$ it is *not* true that any n-dimensional complex torus $X = V/L$ is algebraic; in fact, "most" of them are not. What is true, however, is that every abelian variety over $\mathbb{C}$ can analytically be described as a complex torus. In this way, complex tori provide "explicit" examples of abelian varieties. We will return to this in Chapter ??.

The group structure of an abelian variety imposes strong conditions on the geometry of the underlying variety. The following lemma is important in making this explicit.

Rigidity **(1.12) Rigidity Lemma.** *Let X, Y and Z be algebraic varieties over a field k. Suppose that X is complete. If $f\colon X \times Y \to Z$ is a morphism with the property that, for some $y \in Y(k)$, the fibre $X \times \{y\}$ is mapped to a point $z \in Z(k)$ then f factors through the projection $\mathrm{pr}_Y\colon X \times Y \to Y$.*

Proof. We may assume that $k = \overline{k}$. Choose a point $x_0 \in X(k)$, and define a morphism $g\colon Y \to Z$ by $g(y) = f(x_0, y)$. Our goal is to show that $f = g \circ \mathrm{pr}_Y$. As $X \times Y$ is reduced it suffices to

prove this on k-rational points. hom

Let $U \subset Z$ be an affine open neighbourhood of z. Since X is complete, the projection hom
$\mathrm{pr}_Y\colon X \times Y \to Y$ is a closed map, so that $V := \mathrm{pr}_Y\big(f^{-1}(Z-U)\big)$ is closed in Y. By construction, hom
if $P \notin V$ then $f(X \times \{P\}) \subset U$. Since X is complete and U is affine, this is possible only if f is constant on $X \times \{P\}$. This shows that $f = g \circ \mathrm{pr}_Y$ on the non-empty open set $X \times (Y - V)$. Because $X \times Y$ is irreducible, it follows that $f = g \circ \mathrm{pr}_Y$ everywhere. □

HomomDef **(1.13) Definition.** Let (X, m_X, i_X, e_X) and (Y, m_Y, i_Y, e_Y) be group varieties. A morphism $f\colon X \to Y$ is called a *homomorphism* if

$$f \circ m_X = m_Y \circ (f \times f)\,.$$

If this holds then also $f(e_X) = e_Y$ and $f \circ i_X = i_Y \circ f$.

The rigidity of abelian varieties is illustrated by the fact that up to a translation every morphism is a homomorphism:

MorAV **(1.14) Proposition.** *Let X and Y be abelian varieties and let $f\colon X \to Y$ be a morphism. Then f is the composition $f = t_{f(e_X)} \circ h$ of a homomorphism $h\colon X \to Y$ and a translation $t_{f(e_X)}$ over $f(e_X)$ on Y.*

Proof. Set $y := i_Y\big(f(e_X)\big)$, and define $h := t_y \circ f$. By construction we have $h(e_X) = e_Y$. Consider the composite morphism

$$g := (X \times X \xrightarrow{(h\circ m_X)\times\left(i_Y \circ m_Y \circ (h\times h)\right)} Y \times Y \xrightarrow{m_Y} Y)\,.$$

(To understand what this morphism does: if we use the additive notation for the group structures on X and Y then g is given on points by $g(x, x') = h(x + x') - h(x') - h(x)$.) We have

$$g(\{e_X\} \times X) = g(X \times \{e_X\}) = \{e_Y\}\,.$$

By the Rigidity Lemma this implies that g factors both through the first and through the second projection $X \times X \to X$, hence g equals the constant map with value e_Y. This means that $h \circ m_X = m_Y \circ (h \times h)$, i.e., h is a homomorphism. □

UniqAVStr **(1.15) Corollary.** (i) *If X is a variety over a field k and $e \in X(k)$ then there is at most one structure of an abelian variety on X for which e is the identity element.*

(ii) *If (X, m, i, e) is an abelian variety then the group structure on X is commutative, i.e., $m \circ s = m\colon X \times X \to X$, where $s\colon X \times X \to X \times X$ is the morphism switching the two factors. In particular, for every k-scheme T the group $X(T)$ is abelian.*

Proof. (i) If (X, m, i, e) and (X, n, j, e) are abelian varieties then m and n are equal when restricted to $X \times \{e\}$ and $\{e\} \times X$. Applying (1.12) to $m \circ (m, i \circ n)\colon X \times X \to X$, which is constant when restricted to $X \times \{e\}$ and $\{e\} \times X$, we get $m = n$. This readily implies that $i = j$ too.

(ii) By the previous proposition, the map $i\colon X \to X$ is a homomorphism. This implies that the group structure is abelian. □

NCGrVar **(1.16) Remark.** It is worthwile to note that in deriving the commutativity of the group the completeness of the variety is essential. Examples of non-commutative group varieties are linear

algebraic groups (i.e., matrix groups) like GL_n for $n > 1$, the orthogonal groups O_n for $n > 1$ and symplectic groups Sp_{2n}. hom

AddNotat **(1.17) Notation.** From now on we shall mostly use the additive notation for abelian varieties, writing $x + y$ for $m(x, y)$, writing $-x$ for $i(x)$, and 0 for e. Since abelian varieties are abelian as group varieties, we no longer have to distinguish between left and right translations. Also we can add homomorphisms: given two homomorphisms of abelian varieties f, $g\colon X \to Y$, we define $f + g$ to be the composition

$$f + g := m_Y \circ (f, g)\colon X \longrightarrow Y \times Y \longrightarrow Y\,,$$

and we set $-f := f \circ i_X = i_Y \circ f$. This makes the set $\mathrm{Hom}_{\mathsf{AV}}(X, Y)$ of homomorphisms of X to Y into an abelian group.

As we have seen, also the set $\mathrm{Hom}_{\mathsf{Sch}/k}(X, Y) = Y(X)$ of X-valued points of Y has a natural structure of an abelian group. By Proposition (1.14), $\mathrm{Hom}_{\mathsf{AV}}(X, Y)$ is just the subgroup of $\mathrm{Hom}_{\mathsf{Sch}/k}(X, Y)$ consisting of those morphisms $f\colon X \to Y$ such that $f(0_X) = 0_Y$, and $\mathrm{Hom}_{\mathsf{Sch}/k}(X, Y) = \mathrm{Hom}_{\mathsf{AV}}(X, Y) \times Y(k)$ as groups. We shall adopt the convention that $\mathrm{Hom}(X, Y)$ stands for $\mathrm{Hom}_{\mathsf{AV}}(X, Y)$. If there is a risk of confusion we shall indicate what we mean by a subscript "AV" or "Sch/k".

We close this chapter with another result that can be thought of as a rigidity property of abelian varieties.

ExtendMap **(1.18) Theorem.** *Let X be an abelian variety over a field k. If V is a smooth k-variety then any rational map $f\colon V \dashrightarrow X$ extends to a morphism $V \to X$.*

Proof. We may assume that $k = \overline{k}$, for if a morphism $V_{\overline{k}} \to X_{\overline{k}}$ is defined over k on some dense open subset of $V_{\overline{k}}$, then it is defined over k. Let $U \subseteq V$ be the maximal open subset on which f is defined. Our goal is to show that $U = V$.

If $P \in |V|$ is a point of codimension 1 then the local ring $O_{V,P}$ is a discrete valuation ring, because V is regular. By the valuative criterion for properness the map $f\colon \mathrm{Spec}\big(k(V)\big) \to X$ extends to a morphism $\mathrm{Spec}(O_{V,P}) \to X$. Because X is locally of finite type over k, this last morphism extends to a morphism $Y \to X$ for some open $Y \subset V$ containing P. (Argue on rings.) Hence $\mathrm{codim}_X(X \setminus U) \geqslant 2$.

Consider the rational map $F\colon V \times V \dashrightarrow X$ given on points by $(v, w) \mapsto f(v) - f(w)$. Let $W \subset V \times V$ be the domain of definition of F. We claim that f is defined at a point $v \in V(k)$ if and only if F is defined at (v, v). In the "only if" direction this is immediate, as clearly $U \times U \subseteq W$. For the converse, suppose F is defined at (v, v). Then $\big(V \times \{v\}\big) \cap W$ is an open subset of $V \cong V \times \{v\}$ containing v. Hence we can choose a point $u \in U(k)$ such that $(u, v) \in W$. Then $\big(\{u\} \times V\big) \cap W$ is an open subset of $V \cong \{u\} \times V$ containing v, on which f is defined because we have the relation $f(w) = f(u) - F(u, w)$.

Our job is now to show that the domain of definition W contains the diagonal $\Delta \subset V \times V$. Consider the homomorphism on function fields $F^\sharp\colon k(X) \to k(V \times V)$. Note that F maps $\Delta \cap W$ to $0 \in X$. It follows that F is regular at a point $(v, v) \in \Delta(k)$ if and only if $F^\sharp$ maps $O_{X,0} \subset k(X)$ into $O_{V\times V,(v,v)}$. Suppose that f is not regular at some point $v \in V(k)$, and choose an element $\varphi \in O_{X,0}$ with $F^\sharp(\varphi) \notin O_{V\times V,(v,v)}$. Let D be the polar divisor of $F^\sharp(\varphi)$, i.e.,

$$D = \sum \mathrm{ord}_P\big(F^\sharp(\varphi)\big) \cdot [P]$$

where the sum runs over all codimension 1 points $P \in |V \times V|$ with $\mathrm{ord}_P\big(F^\sharp(\varphi)\big) < 0$. If (w,w) is a k-valued point in $\Delta \cap |D|$ then $F^\sharp(\varphi)$ is not in $O_{V\times V,(w,w)}$, hence F is not regular at (w,w). But $V \times V$ is a regular scheme, so $D \subset V \times V$ is locally a principal divisor. Then also $\Delta \cap |D|$ is locally defined, inside Δ, by a single equation, and it follows that $\Delta \cap |D|$ has codimension $\leqslant 1$ in Δ. Hence f is not regular on a subset of V of codimension $\leqslant 1$, contradicting our earlier conclusion that $\mathrm{codim}_X(X\backslash U) \geqslant 2$. [**opmerking:** Erg helder vind ik het argument nog niet.] □

Exercises.

Ex:Prod **(1.1)** Let X_1 and X_2 be varieties over a field k.

(i) If X_1 and X_2 are given the structure of a group variety, show that their product $X_1 \times X_2$ naturally inherits the structure of a group variety.

(ii) Suppose $Y := X_1 \times X_2$ carries the structure of an abelian variety. Show that X_1 and X_2 each have a unique structure of an abelian variety such that $Y = X_1 \times X_2$ *as abelian varieties*.

Ex:k[e]tgt **(1.2)** Let X be a variety over a field k. Write $k[\varepsilon]$ for the ring of dual numbers over k (i.e., $\varepsilon^2 = 0$), and let $S := \mathrm{Spec}\big(k[\varepsilon]\big)$. Write $\mathrm{Aut}^{(1)}(X_S/S)$ for the group of automorphisms of X_S over S which reduce to the identity on the special fibre $X \hookrightarrow X_S$.

(i) Let x be a k-valued point of X (thought of either as a morphism of k-schemes $x\colon \mathrm{Spec}(k) \to X$ or as a point $x \in |X|$ with $k(x) = k$). Show that the tangent space $T_{X,x} := (m_x/m_x^2)^*$ is in natural bijection with the space of $k[\varepsilon]$-valued points of X which reduce to x modulo ε. (Cf. HAG, Chap. II, Exercise 2.8.)

(ii) Suppose $X = \mathrm{Spec}(A)$ is affine. It is immediate from the definitions that

$$H^0(X, \mathscr{T}_{X/k}) \cong \mathrm{Hom}_k(\Omega^1_{A/k}, A) \cong \mathrm{Der}_k(A, A)\,.$$

Use this to show that $H^0(X, \mathscr{T}_{X/k})$ is a naturally isomorphic with $\mathrm{Aut}^{(1)}(X_S/S)$.

(iii) Show, by taking an affine covering and using (ii), that for arbitrary variety X we have a natural isomorphism

$$h\colon H^0(X, \mathscr{T}_{X/k}) \xrightarrow{\sim} \mathrm{Aut}^{(1)}(X_S/S)\,.$$

(iv) Suppose X is a group variety over k. If $x \in X(k)$ and $\tau\colon S \to X$ is a tangent vector at x, check that the associated global vector field $\xi := h^{-1}(t_\tau)$ is right-invariant, meaning that $t_{y,*}\xi = \xi$ for all $y \in X$. [**opmerking:** Dit is volgens mij een beetje los uit de pols. Waarom rechts-invariant en niet links? Bovendien sluit het niet aan op de tekst, want daarin hebben we het juist over de links-invariante vv. Controleren en aanpassen.]

Ex:RingVar **(1.3)** A *ring variety* over a field k is a commutative group variety $(X, +, 0)$ over k, together with a ring multiplication morphism $X \times_k X \to X$ written as $(x, y) \mapsto x \cdot y$, and a k-rational point $1 \in X(k)$, such that the ring multiplication is associative: $x\cdot(y\cdot z) = (x\cdot y)\cdot z$, distributive: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, and 1 is a 2-sided identity element: $1 \cdot x = x = x \cdot 1$. Show that the only complete ring variety is a point. (In fact, you do not need the identity element for this.)

Ex:HomXxXYxY **(1.4)** Let X_1, X_2, Y_1 and Y_2 be abelian varieties over a field k. Show that

$$\begin{aligned}\mathrm{Hom}_{\mathsf{AV}}(X_1 \times X_2, Y_1 \times Y_2)\\ \cong \mathrm{Hom}_{\mathsf{AV}}(X_1, Y_1) \times \mathrm{Hom}_{\mathsf{AV}}(X_1, Y_2) \times \mathrm{Hom}_{\mathsf{AV}}(X_2, Y_1) \times \mathrm{Hom}_{\mathsf{AV}}(X_2, Y_2)\,.\end{aligned}$$

Does a similar statement hold if we everywhere replace "$\mathrm{Hom}_{\mathsf{AV}}$" by "$\mathrm{Hom}_{\mathsf{Sch}}$" ?

Notes. If one wishes to go back to classical antiquity one may put the origin of the theory of abelian varieties with Diophantos ($\pm$ 200 – $\pm$ 284) who showed how to construct a third rational solution of certain cubic equations in two unknowns from two given ones. The roots in a not so distant past may be layed with Giulio Carlo Fagnano (1682–1766) and others who considered addition laws for elliptic integrals. From this the theory of elliptic functions was developed. The theory of elliptic functions played a major role in 19th century mathematics. Niels Henrik Abel (1802–1829), after which our subject is named, had a decisive influence on its development. Other names that deserve to be mentioned are Adrien-Marie Legendre (1752–1833), Carl-Friedrich Gauss (1777–1855) and Carl Gustav Jacobi (1804–1851).

Bernhard Riemann (1826–1866) designed a completely new theory of abelian functions in which the algebraic curve was no longer the central character, but abelian integrals and their periods and the associated complex torus. The theory of abelian functions was further developed by Leopold Kronecker (1823–1891), Karl Weierstrass (1815–1897) and Henri Poincaré (1854–1912). After Emile Picard (1856– 1941) abelian functions were viewed as the meromorphic functions on a complex abelian variety.

It was André Weil (1906–1998) who made the variety the central character of the subject when he developed a theory of abelian varieties over arbitrary fields; he was motivated by the analogue of Emil Artin (1898–1962) of the Riemann hypothesis for curves over finite fields and the proof by Helmut Hasse (1898–1979) for genus 1. See Weil [2]. David Mumford (1937) recasted the theory of Weil in terms of Grothendieck's theory of schemes. His book MAV is a classic. We refer to Klein [1] and Dieudonné [2] for more on the history of our subject. The Rigidity Lemma is due to Mumford.

Chapter II. Line bundles and divisors on abelian varieties.

In this chapter we study line bundles and divisors on abelian varieties. One of the main goals is to prove that abelian varieties are projective. The Theorem of the Square (2.9) plays a key role. Since abelian varieties are nonsingular, a Weil divisor defines a Cartier divisor and a line bundle, and we have a natural isomorphism $\mathrm{Cl}(X) \xrightarrow{\sim} \mathrm{Pic}(X)$. We shall mainly work with line bundles, but sometimes (Weil) divisors are more convenient.

The following abuse of notation will prove handy. If L is a line bundle on a product variety $X \times Y$ and x is a point of X then we shall write L_x for the restriction of L to $\{x\} \times Y$. Strictly speaking we should write $\mathrm{Spec}\big(k(x)\big)$ instead of $\{x\}$ but where possible we prefer the latter, more geometric, notation. Similarly, if y is a point of Y we denote by L_y the restriction $L_{|X\times\{y\}}$. Here, of course, x shall always be a point of X and y a point of Y.

In this chapter, varieties shall always be varieties over some ground field k, which in most cases shall not be mentioned.

§1. *The theorem of the square.*

LineBonProd **(2.1) Theorem.** *Let X and Y be varieties. Suppose X is complete. Let L and M be two line bundles on $X \times Y$. If for all closed points $y \in Y$ we have $L_y \cong M_y$ there exists a line bundle N on Y such that $L \cong M \otimes p^*N$, where $p = \mathrm{pr}_Y\colon X \times Y \to Y$ is the projection onto Y.*

Proof. This is a standard fact of algebraic geometry. A proof using cohomology runs as follows. Since $L_y \otimes M_y^{-1}$ is the trivial bundle and X_y is complete, the space of sections $H^0(X_y, L_y \otimes M_y^{-1})$ is isomorphic to $k(y)$, the residue field of y. This implies that $p_*(L \otimes M^{-1})$ is locally free of rank one, hence a line bundle (see MAV, §5 or HAG, Chap. III, § 12). We shall prove that the natural map

$$\alpha\colon p^*p_*(L \otimes M^{-1}) \to L \otimes M^{-1}$$

is an isomorphism. If we restict to a fibre we find the map

$$O_{X_y} \otimes \Gamma(X_y, O_{X_y}) \to O_{X_y}$$

which is an isomorphism. By Nakayama's Lemma, this implies that α is surjective and by comparing ranks we conclude that it is an isomorphism. □

As an easy consequence we find a useful prinicple.

See-saw **(2.2) See-saw Principle.** *If, in addition to the assumptions of* (2.1)*, we have $L_x = M_x$ for some point $x \in X$ then $L \cong M$.*

Proof. We have $L \cong M \otimes \mathrm{pr}_Y^*N$. Over $\{x\} \times Y$ this gives $L_x \cong M_x \otimes (\mathrm{pr}_Y^*N)_x$. Therefore, $(\mathrm{pr}_Y^*N)_x$ is trivial, and this implies that N is trivial. □

MaxTriv1 **(2.3) Lemma.** *Let X and Y be varieties, with X complete. For a line bundle L on $X \times Y$, the set $\{y \in Y \mid L_y$ is trivial$\}$ is closed in Y.*

Proof. If M is a line bundle on a complete variety then M is trivial if and only if both $H^0(M)$ and $H^0(M^{-1})$ are non-zero. Hence

ineBund:MaxTriv
$$\{y \in Y \mid L_y \text{ is trivial}\} = \{y \in Y \mid h^0(L_y) > 0\} \cap \{y \in Y \mid h^0(L_y^{-1}) > 0\}\,. \tag{1}$$

But the functions $y \mapsto h^0(L_y)$ and $y \mapsto h^0(L^{-1})$ are upper semi-continuous on Y; see MAV, § 5 or HAG, Chap. III, Thm. 12.8. So the two sets in the right hand side of (1) are closed in Y. □

Actually, there is a refinement of this which says the following.

MaxTrivProp **(2.4) Proposition.** *Let X be a complete variety over a field k, let Y be a k-scheme, and let L be a line bundle on $X \times Y$. Then there exists a closed subscheme $Y_0 \hookrightarrow Y$ which is* the maximal subscheme of Y over which L is trivial; *i.e.,* (i) *the restriction of L to $X \times Y_0$ is the pull back (under pr_{Y_0}) of a line bundle on Y_0, and* (ii) *if $\varphi\colon Z \to Y$ is a morphism such that $(\mathrm{id}_X \times \varphi)^*(L)$ is the pullback of a line bundle on Z under p_Z^* then φ factors through Y_0.*

For the proof we refer to MAV, §10. In Chapter 6 we shall discuss Picard schemes; once we know the existence and some properties of $\mathrm{Pic}_{X/k}$ the assertion of the lemma is a formal consequence. (See (6.4).)

The following theorem is again a general fact from algebraic geometry and could be accepted as a black box. As it turns out, it is of crucial importance for the theory of abelian varieties. In view of its importance we give a proof.

LineBonXYZ **(2.5) Theorem.** *Let X and Y be complete varieties over k and let Z be a connected, locally noetherian k-scheme. Consider points $x \in X$ and $y \in Y$, and let z be a point of Z. If L is a line bundle on $X \times Y \times Z$ whose restriction to $\{x\} \times Y \times Z$, to $X \times \{y\} \times Z$ and to $X \times Y \times \{z\}$ is trivial then L is trivial.*

Proof. We follow the proof given by Mumford in MAV §10. First we remark that that if $k \subset K$ is a field extension then a line bundle M on a k-variety V is trivial if and only if the line bundle M_K on V_K is trivial. (See Exercise (2.1).) To prove the assertion we may therefore first replace the field k by an extension. Hence we may assume that the points x, y and z are k-rational points; this will be used in the definition of the morphisms i_1 and i_2 below.

We view L as a family of line bundles on $X \times Y$ parametrized by Z. Let Z' be the maximal closed subscheme of Z over which L is trivial, as discussed above. We have $z \in Z'$. We shall show that $Z' = Z$ by showing that Z' is an open subscheme and using the connectedness of Z.

Let ζ be a point of Z'. Write $\mathfrak{m}$ for the maximal ideal of the local ring $O_{Z,\zeta}$ and $I \subset O_{Z,\zeta}$ for the ideal defining (the germ of) Z'. We have to show that $I = (0)$. Suppose not. By Krull's Theorem (here we use that Z is locally noetherian) we have $\cap_n \mathfrak{m}^n = (0)$, hence there exists a positive integer n such that $I \subset \mathfrak{m}^n, I \not\subset \mathfrak{m}^{n+1}$. Put $a_1 = (I, \mathfrak{m}^{n+1})$, and choose an ideal a_2 with

$$\mathfrak{m}^{n+1} \subset a_2 \subset (I, \mathfrak{m}^{n+1}) = a_1 \qquad \text{and} \qquad \dim_{k(\zeta)}(a_1/a_2) = 1\,.$$

(Note that such ideals exist.) Let $Z_i \subset \mathrm{Spec}(O_{Z,\zeta})$ be the closed subscheme defined by the ideal a_i $(i = 1, 2)$. We will show that the restriction of L to $X \times Y \times Z_2$ is trivial. This implies that Z_2 is contained in Z', which is a contradiction, since $I \not\subset a_2$.

Write L_i for the restriction of L to $X \times Y \times Z_i$. By construction, L_1 is trivial; choose a trivializing global section s. The inclusion $Z_1 \hookrightarrow Z_2$ induces a restriction map $\Gamma(L_2) \to \Gamma(L_1)$. We claim: L_2 is trivial if and only if s can be lifted to a global section of L_2. To see this,

suppose first that we have a lift s'. The schemes $X \times Y \times Z_1$ and $X \times Y \times Z_2$ have the same underlying point sets. If $s'(P) = 0$ for some point P then also $s(P) = 0$, but this contradicts the assumption that s is a trivialization of L_1. Hence s' is nowhere zero, and since L_2 is locally free of rank 1 this implies that s' trivializes L_2. Conversely, if L_2 is trivial then the restriction map $\Gamma(L_2) \to \Gamma(L_1)$ is just $\Gamma(O_{Z_2}) \to \Gamma(O_{Z_1})$ and this is surjective.

The obstruction for lifting s to a global section of L_2 is an element $\xi \in H^1(X \times Y, O_{X\times Y})$. We know that the restrictions of L_2 to $\{x\} \times Y \times Z_2$ and to $X \times \{y\} \times Z_2$ are trivial. Writing $i_1 = (\mathrm{id}_X, y)\colon X \hookrightarrow X \times Y$ and $i_2 = (x, \mathrm{id}_Y)\colon Y \hookrightarrow X \times Y$, this means that ξ has trivial image under $i_1^*\colon H^1(X \times Y, O_{X\times Y}) \to H^1(X, O_X)$ and under $i_2^*\colon H^1(X \times Y, O_{X\times Y}) \to H^1(Y, O_Y)$. But the map (i_1^*, i_2^*) gives a (Künneth) isomorphism

$$H^1(X \times Y, O_{X\times Y}) \xrightarrow{\sim} H^1(X, O_X) \oplus H^1(Y, O_Y)\,,$$

hence $\xi = 0$ and s can be lifted. □

LBXYZRem **(2.6) Remark.** The previous theorem gives a strong general result about line bundles on a product of three complete varieties. Note that the analogous statement for line bundles on a product of two complete varieties is false in general. More precisely, suppose X and Y are complete k-varieties and L is a line bundle on $X \times Y$. If there exist points $x \in X$ and $y \in Y$ such that $L_x \cong O_Y$ and $L_y \cong O_X$ then it is not true in general that $L \cong O_{X\times Y}$. For instance, take $X = Y$ to be an elliptic curve, and consider the divisor

$$D = \Delta_X - \big(\{0\} \times X\big) - \big(X \times \{0\}\big)$$

where $\Delta_X \subset X \times X$ is the diagonal. Note that $L = O_{X\times X}(D)$ restricts to the trivial bundle on $\{0\} \times X$ and on $X \times \{0\}$. (Use that the divisor $1 \cdot 0$ $(= 1 \cdot e_X)$ on X is linearly equivalent to a divisor whose support does not contain 0.) But L is certainly not the trivial bundle: if it were, $L_{|\{P\}\times X} = O_X(P - e_X) \cong O_X$ for all points $P \in X$. But then there is a function f on X with one zero and one pole and X would have to be a rational curve, which we know it is not.

Theorem (2.5), together with the previous remark, is a reflection of the quadratic character of line bundles. To explain this, let us make the analogy with functions on the real line. The quadratic functions $f(x) = ax^2 + bx + c$ are characterized by their property that

$$f(x + y + z) - f(x + y) - f(x + z) - f(y + z) + f(x) + f(y) + f(z)$$

is constant. The analogue of this for line bundles on abelian varieties is the celebrated Theorem of the Cube. Before we state it, we introduce a notational convention. If X is an abelian variety and $I = \{i_1, \ldots, i_r\} \subset \{1, 2, \ldots, n\}$ then we write

$$p_I\colon X^n \to X\,, \qquad \text{or} \quad p_{i_1\cdots i_r}\colon X^n \to X\,,$$

for the morphism sending $(x_1, x_2, \ldots, x_n)$ to $x_{i_1} + \cdots + x_{i_r}$. Thus, for example, p_i is the projection onto the ith factor, $p_{12} = p_1 + p_2$, etc. With this notation we have the following important corollary to the theorem.

Cube **(2.7) Theorem of the Cube.** *Let L be a line bundle on X. Then the line bundle*

$$\begin{aligned}\Theta(L) &:= \bigotimes_{I\subset\{1,2,3\}} p_I^* L^{\otimes(-1)^{1+\#I}} \\ &= p_{123}^* L \otimes p_{12}^* L^{-1} \otimes p_{13}^* L^{-1} \otimes p_{23}^* L^{-1} \otimes p_1^* L \otimes p_2^* L \otimes p_3^* L\end{aligned}$$

on $X \times X \times X$ is trivial.

Proof. Restriction of $\Theta(L)$ to $\{0\} \times X \times X$ gives the bundle

$$m^*L \otimes p_2^*L^{-1} \otimes p_3^*L^{-1} \otimes m^*L^{-1} \otimes O_{X\times X} \otimes p_2^*L \otimes p_3^*L$$

which is obviously trivial. Similarly for $X \times \{0\} \times X$ and $X \times X \times \{0\}$. By (2.5) the result follows. □

We could sharpen the corollary by saying that $\Theta(L)$ is canonically trivial, see Exercise (2.2).

CubeCor1 **(2.8) Corollary.** *Let Y be a scheme and let X be an abelian variety. For every triple f, g, h of morphisms $Y \to X$ and for every line bundle L on X, the bundle*

$$(f+g+h)^*L \otimes (f+g)^*L^{-1} \otimes (f+h)^*L^{-1} \otimes (g+h)^*L^{-1} \otimes f^*L \otimes g^*L \otimes h^*L$$

on Y is trivial.

Proof. Consider $(f,g,h)\colon Y \to X \times X \times X$ and use (2.7). □

Another important corollary is the following.

Square **(2.9) Theorem of the Square.** *Let X be an abelian variety and let L be a line bundle on X. Then for all $x, y \in X(k)$,*

$$t_{x+y}^*L \otimes L \cong t_x^*L \otimes t_y^*L\,.$$

More generally, let T be a k-scheme and write L_T for the pull-back of L to X_T. Then

$$t_{x+y}^*L_T \otimes L_T \cong t_x^*L_T \otimes t_y^*L_T \otimes \mathrm{pr}_T^*\big((x+y)^*L \otimes x^*L^{-1} \otimes y^*L^{-1}\big)$$

for all $x, y \in X(T)$.

Proof. In the first formulation, this is immediate from (2.8) by taking for f the identity on X and for g and h the constant maps with images x and y. For the general form, take $f = \mathrm{pr}_X\colon X_T = X \times_k T \to X$, take $g = x \circ \mathrm{pr}_T$ and $h = y \circ \mathrm{pr}_T$. Then

$$f + g = \mathrm{pr}_X \circ t_x\,, \quad f + h = \mathrm{pr}_X \circ t_y\,, \quad g + h = (x+y) \circ \mathrm{pr}_T$$

and

$$f + g + h = \mathrm{pr}_X \circ t_{x+y}\,.$$

Now again apply (2.8). □

The theorem allows the following interpretation. (Compare this with what we have seen in Examples (1.8) and (1.10).)

SquareCor1 **(2.10) Corollary.** *Let L be a line bundle on an abelian variety X. Let $\mathrm{Pic}(X)$ be the group of isomorphism classes of line bundles on X. Then the map $\varphi_L\colon X(k) \to \mathrm{Pic}(X)$ given by $x \mapsto [t_x^*L \otimes L^{-1}]$ is a homomorphism.*

Proof. Immediate from (2.9). □

phiLsign **(2.11) Remark.** The homomorphisms φ_L will play a very important role in the theory. In later chapters (see in particular Chapters 6 and 7) we shall introduce the dual X^t of an abelian

variety X, and we shall interprete φ_L as a homomorphism $X \to X^t$. The homomorphisms $\lambda\colon X \to X^t$ that are (geometrically) of the form φ_L for an ample line bundle L are called polarizations; see Chapter 11.

At this point, let us already caution the reader that there is a sign convention in the theory that can easily lead to misunderstanding. In the theory of elliptic curves one usually describes line bundles of degree 0 (which is what the dual elliptic curve is about!) in the form $O_E(P-O)$. More precisely: if E is an elliptic curve with origin O then the map $P \mapsto O_E(P-O)$ gives an isomorphism $E \xrightarrow{\sim} E^t = \mathrm{Pic}^0_{E/k}$. This map is *not* the polarization associated to the ample line bundle $L = O_E(O)$; rather it is *minus* that map. In general, if D is a divisor on an abelian variety X then $t_x^* O_X(D)$ is $O_X\big((t_{-x}(D)\big) = O_X(D-x)$, not $O_X(D+x)$. So if $L = O_E(O)$ on an elliptic curve E, the map φ_L is given on points by $P \mapsto O_E(O-P)$.

The same remark applies to the theory of Jacobians (see in particular Chapter 14). If C is a smooth projective curve over a field k, and if $P_0 \in C(k)$ is a k-rational point then we have a natural morphism φ from C to its Jacobian variety $J = \mathrm{Jac}(C) := \mathrm{Pic}^0_{C/k}$. In most literature one considers the map $C \to J$ given on points by $P \mapsto O_C(P-P_0)$. However, we have a canonical principal polarization on J (see again Chapter 14 for further details), and in connection with this it is more natural to consider the morphism $\varphi\colon C \to J$ given by $P \mapsto O_C(P_0-P)$.

Let X be an abelian variety. For every $n \in \mathbb{Z}$ we have a homomorphism $[n] = [n]_X\colon X \to X$ called "multiplication by n". For $n \geqslant 1$, it sends $x \in X(k)$ to $x + \cdots + x$ (n terms); for $n = -m \leqslant -1$ we have $[n]_X = i_X \circ [m]_X$. If there is no risk of confusion, we shall often simply write n for $[n]$; in particular this includes the abbreviations 1 for $[1] = \mathrm{id}_X$, 0 for $[0]$ (the constant map with value 0), and -1 or (-1) for $[-1] = -\mathrm{id}_X$. The effect of n on line bundles is described by the following result.

CubeCor2 **(2.12) Corollary.** *For every line bundle L on an abelian variety X we have*

$$n^*L \cong L^{n(n+1)/2} \otimes (-1)^* L^{n(n-1)/2}\,.$$

Proof. Set $f = n$, $g = 1$, and $h = -1$. Applying (2.8), one finds that

$$n^*L \otimes (n+1)^*L^{-1} \otimes (n-1)^*L^{-1} \otimes n^*L \otimes L \otimes (-1)^*L$$

is trivial, i.e.,

$$n^*L^2 \otimes (n+1)^*L^{-1} \otimes (n-1)^*L^{-1} \cong (L \otimes (-1)^*L)^{-1}\,.$$

The assertion now follows by induction, starting from the cases $n = -1$, 0, 1. □

In particular, if the line bundle L is symmetric, by which we mean that $(-1)^*L \cong L$, then we find that $n^*L \cong L^{n^2}$ for all n. For instance, if M is an arbitrary line bundle then $L_+ := M \otimes (-1)^*M$ is symmetric. Similarly, $L_- := M \otimes (-1)^*M^{-1}$ is an example of an anti-symmetric line bundle, i.e., a line bundle L for which $(-1)^*L \cong L^{-1}$; for such line bundles we have $n^*L \cong L^n$ for all n. Note the contrast between the quadratic effect of n^* in the symmetric case and the linear effect in the anti-symmetric case. Further note that with the notation just introduced we have $M^2 \cong L_+ \otimes L_-$; so we find that the square of a line bundle can be written as the product of a symmetric and an anti-symmetric part. This is a theme we shall explore in much greater detail in later chapters.

We now turn to the question whether abelian varieties are projective. As it turns out the answer is "yes". We give two proofs of this. A fairly short proof is given in (2.26); the Theorem of the Square plays a key role in this argument. The other proof we give is longer—it takes up most of this section—but along the way we shall obtain a number of results that are interesting in their own right. We think that Proposition (2.20) is particularly remarkable.

We shall need a couple of facts about group schemes. Since these form the main objects of study of the next two chapters, we shall simply use what we need, and refer forward to the next chapter for a precise explanation. What is needed in this chapter can be summarized as follows.

AVsubvarFact **(2.13) Fact.** *Let X be an abelian variety over a field k. Suppose $Y \hookrightarrow X$ is a closed subgroup scheme. If Y^0 is the connected component of Y containing the origin then Y^0 is an open and closed subgroup scheme of Y and Y^0 is geometrically irreducible. If furthermore k is perfect then the reduced underlying scheme $Y^0_{\mathrm{red}} \hookrightarrow X$ is an abelian subvariety of X.*

For the proof of this statement, see Prop. (3.17) and Exercise (3.2).

AVsubvarRem **(2.14) Remark.** The fact just stated is weaker than what is actually true. Namely, the conclusion that $Y^0_{\mathrm{red}} \hookrightarrow X$ is an abelian subvariety of X holds true without the assumption that the base field k is perfect. We shall see this in Prop. (5.31), once we have more theory at our disposal. If we already knew the stronger version of the above fact at this stage, it would simplify some of the arguments that we shall give. For instance, in the rest of this chapter we shall sometimes work over $\overline{k}$ and then later draw conclusions that are valid over an arbitrary field. The reason for this detour is that, at this stage, we can apply (2.13) only over a perfect field.

Suppose $X = A \times B$ is an abelian variety which is a product of positive dimensional abelian varieties A and B, and suppose M is a line bundle on A. If $\mathrm{pr}_A\colon A \times B \to A$ is the projection onto A then the bundle $L := \mathrm{pr}_A^* M$ is invariant under translation over the points of $\{0_A\} \times B \subset X$. Obviously, L is not ample. This suggests that if L is a line bundle on X which is invariant under many translations, then L might not be ample.

MumfBundDef **(2.15) Definition.** Let L be a line bundle on an abelian variety X. On $X \times X$ we define the *Mumford line bundle* $\Lambda(L)$ by

$$\Lambda(L) := m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}\,.$$

As we shall see, $\Lambda(L)$ is a very useful bundle. The restriction of $\Lambda(L)$ to a vertical fibre $\{x\} \times X$ and to a horizontal fibre $X \times \{x\}$ is $t_x^* L \otimes L^{-1}$. In particular, $\Lambda(L)$ is trivial on $\{0\} \times X$ and on $X \times \{0\}$.

K(L)Def **(2.16) Definition.** With the above notation, we define $K(L) \subseteq X$ as the maximal closed subscheme (in the sense of (2.4)) such that $\Lambda(L)_{|X \times K(L)}$ is trivial over $K(L)$, i.e., such that $\Lambda(L)_{|X \times K(L)} \cong \mathrm{pr}_2^* M$ for some line bundle M on $K(L)$.

It follows from the universal property in (2.4) that the formation of $K(L)$ is compatible with base-change. In particular, if $k \subset k'$ is a field extension, writing L' for the pull-back of L to $X \times_k k'$, we have $K(L') = K(L) \times_k k'$.

Roughly speaking, a point belongs to $K(L)$ if L is invariant under translation by this point. A more precise statement is given by the following lemma.

K(L)Lem **(2.17) Lemma.** *Let T be a k-scheme and $x\colon T \to X$ a T-valued point of X.*

(i) *The morphism x factors through $K(L)$ if and only if $t_x^*L_T \otimes L_T^{-1}$ is the pull-back of a line bundle on T.*

(ii) *If $t_x^*L_T \otimes L_T^{-1} \cong \mathrm{pr}_T^*M$ then $M \cong x^*L$.*

(iii) *We have $\Lambda(L)_{|X\times K(L)} \cong O_{X\times K(L)}$.*

In (iii), note that a priori we only knew that $\Lambda(L)_{|X\times K(L)}$ is the pull-back of a line bundle on $K(L)$.

Proof. As usual, L_T denotes the pull-back of L via the projection $\mathrm{pr}_X\colon X_T \to X$. Since $\mathrm{pr}_X \circ t_x\colon X_T \to X_T \to X$ is equal to the composition $m\circ(\mathrm{id}_X\times x)\colon X_T = X\times_k T \to X\times_k X \to X$, we find

$$t_x^*L_T \cong (\mathrm{id}_X \times x)^* m^* L\,.$$

Note that we can write L_T as $L_T = (\mathrm{id}_X \times x)^* p_1^* L$. This gives

LineBund:txLL-1
$$t_x^*L_T \otimes L_T^{-1} \cong (\mathrm{id}_X \times x)^*\Lambda(L) \otimes (\mathrm{id}_X \times x)^* p_2^* L = (\mathrm{id}_X \times x)^*\Lambda(L) \otimes (\mathrm{pr}_T^* x^* L)\,. \qquad (2)$$

Using the defining properties of $K(L)$ as given in Proposition (2.4), the assertion of (i) readily follows from this formula.

For (ii) note that $t_x^*L_T \otimes L_T^{-1}$ restricts to x^*L on $\{0\}\times T$.

For (iii), take $T = K(L)$, and let $x\colon K(L) \to X$ be the inclusion. By (2), $t_x^*L_T \otimes L_T^{-1} = \Lambda(L)_{|X\times K(L)} \otimes \big(p_2^*L\big)_{|X\times K(L)}$, which is of the form $p_2^*M \otimes p_2^*(L_{|K(L)})$ for some line bundle M on $K(L)$. On the other hand, $x^*L = L_{|K(L)}$. Now apply (ii) to find that $M = O_{K(L)}$. □

K(L)isSg **(2.18) Proposition.** *The subscheme $K(L)$ is a subgroup scheme of X.*

Proof. Strictly speaking we have not yet defined the notion of a subgroup scheme; see Definition (3.7) below. With that definition the proposition boils down to the statement that $K(L)(T) \subset X(T)$ is a subgroup, for any k-scheme T. This follows from (i) of the Lemma together with the Theorem of the Square. □

The following lemma shows that an ample line bundle is invariant under only finitely many translations.

LampK(L)fin **(2.19) Lemma.** *If L is ample then $K(L)$ is a finite group scheme.*

Proof. Without loss of generality we may assume that k is algebraically closed. Set $Y := K(L)^0_{\mathrm{red}} \subset X$ which, as we noted in (2.13), is an abelian subvariety of X. The restriction L' of L to Y is again ample. By (iii) of Lemma (2.17) the bundle $\Lambda(L')$ on $Y\times Y$ is trivial. Pulling this bundle back to Y via $(1,-1)\colon Y \to Y\times Y$ gives that $L'\otimes(-1)^*L'$ is trivial on Y. But L' is ample, hence $(-1)^*L'$ and $L'\otimes(-1)^*L'$ are ample too. It follows that $\dim(Y) = 0$. Hence $K(L)$ is finite. □

We would like to have a converse to this fact. To obtain this we first prove the following remarkable result.

FibreProp **(2.20) Proposition.** *Let X be an abelian variety over an algebraically closed field k. Let $f\colon X \to Y$ be a morphism of k-varieties. For $x \in X$, let C_x denote the connected component of*

the fibre over $f(x)$ such that $x \in C_x$, and write F_x for the reduced scheme underlying C_x. Then F_0 is an abelian subvariety of X and $F_x = t_x(F_0) = x + F_0$ for all $x \in X(k)$.

Proof. Consider the morphism $\varphi\colon X \times F_x \to Y$ obtained by restricting $f \circ m$ to $X \times F_x$. Clearly $\varphi(\{0\} \times F_x) = \{f(x)\}$. Since F_x is complete and connected, the Rigidity Lemma (1.12) implies that φ maps the fibres $\{z\} \times F_x$ to a point. In particular, we find that $f(y-x+F_x) = f(y)$ for all $x, y \in X(k)$. Putting $y = z$, $x = 0$ gives $z + F_0 \subseteq F_z$; putting $y = 0$, $x = z$ gives $-z + F_z \subseteq F_0$. This shows that $F_z = z + F_0$.

To see that F_0 is a subgroup scheme of X we take a geometric point $a \in F_0(k)$. Then obviously $F_a = F_0$ so that $a + F_0 = F_a = F_0$. Since F_0 is reduced, it follows that F_0 is a subgroup scheme of X. By (2.13) it is then an abelian subvariety. □

To illustrate the proposition, suppose X is a simple abelian variety (over $k = \overline{k}$), meaning that it does not have any non-trivial abelian subvarieties. Then the conclusion is that every morphism from X to another k-variety is either constant or finite. So the proposition puts strong restrictions on the geometry of abelian varieties.

We give another interpretation of F_0. For this, let D be an *effective* divisor on X and let $L = O_X(D)$ be the corresponding line bundle. We claim that linear system $|2D|$ has no base-points, i.e., the sections of $L^{\otimes 2}$ define a morphism of X to projective space. To see this we have to show that for every geometric point y of X there exists an element $E \in |2D|$ that does not contain y. Now the Theorem of the Square tells us that the divisors of the form

LB:txDt-xD
$$t_x^* D + t_{-x}^* D \tag{3}$$

belong to $|2D|$. It is easy to see that given y there exists a geometric point x such that y does not belong to the support of the divisor (3). This means that the map $\varphi\colon X \to \mathbb{P}(\Gamma(X, L^{\otimes 2})^*)$ defined by the sections of $L^{\otimes 2}$ is a morphism. Note that we also have a morphism

$$f\colon X \to \mathbb{P} = |2D|, \quad x \mapsto t_x^* D + t_{-x}^* D\,.$$

The relation between φ and f shall be discussed in ??.

We now again assume that $k = \overline{k}$. For an effective divisor D on X we define the reduced closed subscheme $H(D) \subset X$ by

$$H(D)(\overline{k}) = \left\{ x \in X(\overline{k}) \;\middle|\; t_x^* D = D \right\}.$$

By $t_x^* D = D$ we here mean equality of divisors, not of divisor classes. Clearly $H(D)$ is a subgroup scheme of X.

F0K(L)Lem **(2.21) Lemma.** *Assume $k = \overline{k}$ and let L be an effective line bundle on the abelian variety X. Let $f\colon X \to \mathbb{P}^n$ be the morphism defined by the sections of $L^{\otimes 2}$. As in* (2.20) *let F_0 be the reduced connected fibre of f containing* 0*. Then $H(D)^0 = F_0 = K(L)^0_{\mathrm{red}}$, where the superscript "^{0}" denotes the connected component containing* 0*.*

Proof. Let $x \in F_0$. It follows from (2.20) that $f \circ t_x = f$. Hence if $s \in \Gamma(X, L^{\otimes 2})$ then s and $t_x^* s$ have the same zero divisor. We apply this to $s = t^2$, where t is a section of L with divisor D. This gives $t_x^* D = D$, i.e., $x \in H(D)$. This shows that $F_0 \subseteq H(D)$, and since F_0 is connected we find $F_0 \subseteq H(D)^0$. Next, it is obvious that $H(D)^0$ is contained in $K(L)^0_{\mathrm{red}}$. To prove that $K(L)^0_{\mathrm{red}} \subseteq F_0$, write L' for the restriction of L to $K(L)^0_{\mathrm{red}}$. By (2.13), $K(L)^0_{\mathrm{red}}$ is an abelian

subvariety of X. Clearly it suffices to show that L' is trivial. Now L', hence also $(-1)^*L'$, has a non-trivial global section. On the other hand, $(-1)^*L' \cong (L')^{-1}$, as we have seen already in the proof of (2.19). Hence L' is trivial. □

As we shall see in the next chapters, there exists a quotient $X' := X/F_0$ which is again an abelian variety. The Stein factorisation of the morphism f is given by $X \twoheadrightarrow X' \to \mathbb{P}^n$, and L is the pull-back of a bundle on X'.

KLfinAmp **(2.22) Proposition.** *Let L be a line bundle on an abelian variety X which has a non-zero global section. If $K(L)$ is a finite group scheme then L is ample.*

Proof. We may work over an algebraic closure of k. (Note that if a line bundle L becomes ample after extension of the ground field then it is already ample.) Let D be the divisor of the given section. By (2.21) the fibre F_0 is reduced to a point and by (2.20) it follows that f is quasi-finite. Since f is also proper, it is finite. By general theory (see HAG, Chap. III, Exercise 5.7), if the sections of $L^{\otimes 2}$ define a finite morphism $X \to \mathbb{P}^n$ then L is ample. □

LAmpCor **(2.23) Corollary.** *Let D be an effective divisor on an abelian variety X over an algebraically closed field. Set $L = O_X(D)$. Then the following are equivalent:*

(a) *$H(D)$ is finite,*
(b) *$K(L)$ is finite,*
(c) *L is ample.*

For later use we introduce some terminology.

nondegLBDef **(2.24) Definition.** A line bundle L on an abelian variety is said to be *non-degenerate* if $K(L)$ is finite.

So, an *effective* line bundle is non-degenerate if and only if it is ample.

AVProjective **(2.25) Theorem.** *An abelian variety is a projective variety.*

Proof. We first prove this for $k = \overline{k}$. Choose a quasi-affine open subset $U \subset X$ such that $X \setminus U = \cup_{i\in I} D_i$ for certain prime divisors D_i. Set $D = \sum_{i\in I} D_i$. By the preceding results it suffices to show that $H(D)$ is finite. If $x \in H(D)$ then t_x transforms U into itself. Assuming—as we may—that $0 \in U$, we find that $H(D)$ is contained in U. But $H(D)$ is proper, since $F_0 = H(D)^0$ (as in (2.21)). It follows that $H(D)$ is finite.

If k is arbitrary, we first choose an ample divisor $D \subset X_{\overline{k}}$. Then D is defined over a finite extension k' of k. If k' is Galois over k (which we may assume if k'/k is separable) then

$$\tilde{D} := \sum_{\sigma\in \mathrm{Gal}(k'/k)} {}^{\sigma}D$$

is an ample divisor on $X_{\overline{k}}$ which descends to X. If k'/k is purely inseparable such that $\alpha^{p^m} \in k$ for all $\alpha \in k'$ then $p^m \cdot D$ is an ample divisor which descends to X (clear from working at charts). Combination of these two cases gives the theorem. □

ProjLang **(2.26)** We give another proof of the theorem. Choose a collection of prime divisors $D_1, \ldots, D_n$, all containing 0, such that the (scheme-theoretic) intersection $\cap_{i=1}^n D_i$ reduces to the single closed point 0. Set $D = \sum_{i=1}^n D_i$. We claim that $3D$ is a very ample divisor. To prove this we may pass to an algebraic closure of the ground field, so we will now assume that $k = \overline{k}$.

First let us show that the linear system $|3D|$ separates points. Thus, given points $P \neq Q$ of X we want to find a divisor Δ, linearly equivalent to $3D$, with $P \in \mathrm{Supp}(\Delta)$ but $Q \notin \mathrm{Supp}(\Delta)$. The divisor we take shall be of the form

$$\Delta = \sum_{i=1}^{n} t_{a_i}^* D_i + t_{b_i}^* D_i + t_{-a_i-b_i}^* D_i \tag{4}$$

LB:Delta

for certain points a_i, $b_i \in X$. Note that by the Theorem of the Square, any divisor of this form is linearly equivalent to $3D$. As $P \neq Q$ and $\cap D_i = \{0\}$, one of the D_i does not contain $P - Q$. Say it is D_1. Take $a_1 = P$, and choose the points b_1, a_i and b_i (for $2 \leqslant i \leqslant n$) such that Q is not in the support of

$$t_{b_1}^* D_1 + t_{-P-b_1}^* D_1 + \sum_{i=2}^{n} t_{a_i}^* D_i + t_{b_i}^* D_i + t_{-a_i-b_i}^* D_i \,. \tag{5}$$

LB:divisor

With these choices the divisor Δ given by (4) has the required properties.

Essentially the same argument shows that $|3D|$ also separates tangent vectors. Namely, suppose $P \in X$ and $0 \neq \tau \in T_{X,P}$. As the scheme-theoretic intersection $\cap_{i=1}^n D_i$ reduces to the single closed point 0, there is an index i such that $t_{-P}^* \tau \in T_{X,0}$ does not lie in the subspace $T_{D_i,0} \subset T_{X,0}$. Say this holds for $i = 1$. Take $a_1 = P$, and take the remaining points a_i and b_i such that P is not in the support of the divisor given by (5). This gives a divisor Δ with $P \in \mathrm{Supp}(\Delta)$ but τ not tangent to Δ. □

Later we shall prove that if D is an ample divisor on an abelian variety, then $3D$ is very ample. In general $2D$ will not be very ample. For an example, take an elliptic curve E and let $D = P$, a point. Then $L(2P) = \Gamma\big(E, O(2P)\big)$ has dimension 2, and $|2P|$ defines a morphism $E \to \mathbb{P}^1$ of degree 2 with ramification divisor of degree 4. (In fact, if $\mathrm{char}(k) \neq 2$ this morphism is ramified in 4 points.)

§3. *Projective embeddings of abelian varieties.*

Any smooth projective variety of dimension g can be embedded into $\mathbb{P}^{2g+1}$, see [??]. We shall now show that an abelian variety of dimension g cannot be embedded into $\mathbb{P}^{2g-1}$ and that an embedding into $\mathbb{P}^{2g}$ exists only for elliptic curves and for certain abelian surfaces. So in some sense abelian varieties do not fit easily into projective space; this also helps to explain why it is so difficult to write down explicit examples of abelian varieties.

In the proof of the next result we shall use the Chow ring $\mathrm{CH}(X)$ of X; we could also work with a suitable cohomology theory (e.g., Betti cohomology or étale cohomology). In fact, all we need are a couple of basic formulas which can be found in Fulton's book [1]. The Chow ring of an abelian variety is further studied in Chap. 13.

AVembThm **(2.27) Theorem.** *No abelian variety of dimension g can be embedded into $\mathbb{P}^{2g-1}$. No abelian variety of dimension $g \geqslant 3$ can be embedded into $\mathbb{P}^{2g}$.*

Proof. Let X be an abelian variety, $\dim(X) = g$, and suppose we have an embedding $i\colon X \hookrightarrow \mathbb{P} = \mathbb{P}^m$. Consider the exact sequence of sheaves ("adjunction sequence")

$$0 \to T_X \to i^* T_{\mathbb{P}} \to N \to 0 \,, \tag{6}$$

LB:adjunct

where N is the normal bundle of X in $\mathbb{P}$ and T_X (resp. $T_{\mathbb{P}}$) is the tangent bundle of X (resp. $\mathbb{P}$). Write $h \in \mathrm{CH}(X)$ for the class of a hyperplane section and $c_i = c_i(N)$ (for $i = 1, \ldots, g-1$) for the ith Chern class of N. We know that the tangent bundle of X is trivial. Therefore, the equality of total Chern classes resulting from (6) reads:

$$(1+h)^{m+1} = 1 + \sum_{i=1}^{m-g} c_i \,.$$

(See Fulton [1], 3.2.12.) This implies immediately that $h^{m-g+1} = 0$ in $\mathrm{CH}^g(X)$. But $\deg(h^g)$ equals the degree, say d, of X in $\mathbb{P}^m$ which is non-zero. We thus find $m - g + 1 \geqslant g + 1$, i.e., $m \geqslant 2g$.

We now consider the case of an embedding into $\mathbb{P}^{2g}$. The previous argument gives

$$c_g = \binom{2g+1}{g} \cdot h^g \,.$$

Aplying the degree map we find

LB:degcg
$$\deg(c_g) = \binom{2g+1}{g} \deg(h^g) = \binom{2g+1}{g} d \,. \tag{7}$$

But since $2\dim(X) = \dim(\mathbb{P}^g)$, the degree of the highest Chern class c_g of the normal bundle N on X is the self-intersection number of X in $\mathbb{P}^{2g}$, (see Fulton [1], §6.3), which is d^2. Together with (7) this gives

$$d = \binom{2g+1}{g} \,.$$

On the other hand, if we apply the Hirzebruch-Riemann-Roch theorem to the line bundle $L = O(1)$ and use that the Chern classes of X vanish we find that

$$\chi(L) = c_1(L)^g / g! \,,$$

where $\chi(L) = \sum_{i=0}^{g} (-1)^i \dim_k H^i(X, L)$ is the Euler-Poincaré characteristic of L. Since $\chi(L) \in \mathbb{Z}$ it follows that $g!$ divides $\deg(h^g) = d$. (For more details on Riemann-Roch see Chapter IX.) But one easily checks that

$$g! \text{ divides } \binom{2g+1}{g} \quad \Rightarrow \quad g < 3 \,.$$

This finishes the proof. □

The proof of the theorem shows that the possibilities for $g = 1$ and $g = 2$ are the cubic curves in $\mathbb{P}^2$ and abelian surfaces of degree 10 in $\mathbb{P}^4$. We have met the cubic curves in (1.8). That there exist abelian surfaces of degree 10 in $\mathbb{P}^4$ was shown first by Comessatti in 1909. He considered complex abelian surfaces $\mathbb{C}^2/\Lambda$, where $\Lambda \subset \mathbb{C}^2$ is the lattice obtained from a suitable embedding of $O_K \oplus O_K$, with O_K the ring of integers of $K = \mathbb{Q}(\sqrt{5})$. Horrocks and Mumford found abelian surfaces in $\mathbb{P}^4$ as zero sets of sections of the Horrocks-Mumford bundle, an indecomposable rank two vector bundle on $\mathbb{P}^2$. For further discussion we refer to Chap. ??.

Exercises.

Ex:dimH0 **(2.1)** Let $k \subset K$ be a field extension. Let X be a k-variety and F a sheaf of O_X-modules. Write X_K for the K-variety obtained from X by extension of scalars, and let $F_K := (X_K \to X)^* F$. Show that $\dim_k H^0(X, F) = \dim_K H^0(X_K, F_K)$. Also show that $F \cong O_X$ if and only if $F_K \cong O_{X_K}$.

Ex:ThmCube **(2.2)** Show that the isomorphism in the Theorem of the Cube is canonical. By this we mean that to a given line bundle L on an abelian variety X we can associate an isomorphism $\tau_{X,L}\colon \Theta(L) \xrightarrow{\sim} O_{X\times X\times X}$ in a functorial way, i.e, such that for every homomorphism $f\colon Y \to X$ we have $f^*(\tau_{X,L}) = \tau_{Y,f^*L}$ (via the canonical isomorphisms $\Theta(f^*L) \cong (f\times f\times f)^*\Theta(L)$ and $O_{Y\times Y\times Y} \cong (f\times f\times f)^* O_{X\times X\times X}$).

Ex:DivMult **(2.3)** Let X be an abelian variety over an algebraically closed field. Show that every effective divisor on X is linearly equivalent to an effective divisor without multiple components.

Ex:EmbP1power **(2.4)** Prove that no abelian variety of dimension g can be embedded into $(\mathbb{P}^1)^{2g-1}$. Analyze when an abelian variety of dimension g can be embedded into $(\mathbb{P}^1)^{2g}$.

Ex:thetanf **(2.5)** Let A and B be two abelian groups, written additively, and let $n \geqslant 0$ be an integer. If $f\colon A \to B$ is a map (not necessarily a homomorphism), define a map $\theta_n(f)\colon A^n \to B$ by

$$\theta_n(f)\big(a_1, \dots, a_n\big) = \sum_I (-1)^{n+\#I} f(a_I)\,,$$

where I runs over the non-empty subsets of $\{1, 2, \dots, n\}$ and $a_I := \sum_{i\in I} a_i$. For instance, $\theta_0(f)\colon \{0\} \to B$ is the map with value 0 (by convention), $\theta_1(f) = f$, and

$$\theta_2(f)\big(a, a'\big) = f(a+a') - f(a) - f(a')$$
$$\theta_3(f)\big(a, a', a''\big) = f(a+a'+a'') - f(a+a') - f(a+a'') - f(a'+a'') + f(a) + f(a') + f(a'')\,.$$

(i) Show that $\theta_n(f)\colon A^n \to B$ is symmetric, i.e., invariant under the action of the group S_n on A^n by permutation of the factors.

(ii) For $n \geqslant 1$, show that we have a relation

$$\theta_{n+1}(f)\big(a_1, \dots, a_n, a_{n+1}\big) = \theta_n(f)\big(a_1, \dots, a_n + a_{n+1}\big) - \theta_n(f)\big(a_1, \dots, a_n\big) - \theta_n(f)\big(a_1, \dots, a_{n+1}\big)\,.$$

(iii) Use (i) and (ii) to show that $\theta_{n+1}(f) = 0$ if and only if the map $\theta_n(f)\colon A^n \to B$ is n-linear.

(iv) Let L be a line bundle on an abelian variety X over a field k. If T is a k-scheme, show that the map $X(T) \times X(T) \to \mathrm{Pic}(T)$ given by $(x_1, x_2) \mapsto (x_1 + x_2)^* L \otimes x_1^* L^{-1} \otimes x_2^* L^{-1}$ is bilinear.

Notes. The Theorem of the Square and of the Cube are the pivotal theorems for divisors or line bundles on abelian varieties. They are due to Weil [3]. Our discussion owes much to Mumford's book MAV. Solomon Lefschetz (1884–1972) gave a criterion for complex tori to be embeddable into projective space. This was remodelled by Weil to give the projectivity of abelian varieties; see Weil [5]. Our first proof of Theorem (2.25) follows MAV; the argument given in (2.26) is the one found in Lang [1]. The definition of $K(L)$ goes back to Weil. Proposition (2.20) is due to M.V. Nori. Theorem (2.27) is due to Barth [1] and Van de Ven [1].

As we have seen in the previous chapter, group schemes come naturally into play in the study of abelian varieties. For example, if we look at kernels of homomorphisms between abelian varieties then in general this leads to group schemes that are not group varieties. In the next chapters we shall have to deal with group schemes more often, so it is worthwile to set up some general theory.

The present chapter mainly deals with some basic notions, covering most of what is needed to develop the general theory of abelian varieties. We begin by introducing group schemes in a relative setting, i.e., working over an arbitrary basis. After this, in order to avoid too many technicalities, we shall focus on group schemes over a field and affine group schemes.

§1. *Definitions and examples.*

The definition of a group scheme is a variation on that of group variety, where we consider arbitrary schemes rather than only varieties. This leads to the following, somewhat cumbersome, definition.

GrSchDef **(3.1) Definition.** (i) Let S be a scheme. A *group scheme over* S, or an *S-group scheme*, is an S-scheme $\pi\colon G \to S$ together with S-morphisms $m\colon G \times_S G \to G$ (group law, or multiplication), $i\colon G \to G$ (inverse), and $e\colon S \to G$ (identity section), such that the following identities of morphisms hold:

$$m\circ(m \times \mathrm{id}_G) = m\circ(\mathrm{id}_G \times m)\colon\ G \times_S G \times_S G \to G\,,$$
$$m\circ(e \times \mathrm{id}_G) = j_1\colon\ S \times_S G \to G\,,$$
$$m\circ(\mathrm{id}_G \times e) = j_2\colon\ G \times_S S \to G\,,$$

and

$$e\circ\pi = m\circ(\mathrm{id}_G \times i)\circ\Delta_{G/S} = m\circ(i \times \mathrm{id}_G)\circ\Delta_{G/S}\colon\ G \to G\,,$$

where $j_1\colon S\times_S G \xrightarrow{\sim} G$ and $j_2\colon G\times_S S \xrightarrow{\sim} G$ are the canonical isomorphisms. (Cf. the definitions and diagrams in (1.1).)

(ii) A group scheme G over S is said to be *commutative* if, writing $s\colon G \times_S G \to G \times_S G$ for the isomorphism switching the two factors, we have the identity $m = m\circ s\colon G \times_S G \to G$.

(iii) Let $(\pi_1\colon G_1 \to S, m_1, i_1, e_1)$ and $(\pi_2\colon G_2 \to S, m_2, i_2, e_2)$ be two group schemes over S. A *homomorphism of S-group schemes* from G_1 to G_2 is a morphism of schemes $f\colon G_1 \to G_2$ over S such that $f\circ m_1 = m_2\circ(f \times f)\colon G_1 \times_S G_1 \to G_2$. (This condition implies that $f\circ e_1 = e_2$ and $f\circ i_1 = i_2\circ f$.)

In practice it will usually either be understood what m, i and e are, or it will be unnecessary to make them explicit; in such case we will simply speak about "a group scheme G over S" without further specification. (In fact, we already did so in parts (ii) and (iii) of the definition.)

If G is a group scheme over S and if $S' \to S$ is a morphism of schemes, then the pull-back $G' := G \times_S S'$ inherits the structure of an S'-group scheme. In particular, if $s \in S$ then the fibre $G_s := G \times_S \mathrm{Spec}\big(k(s)\big)$ is a group scheme over the residue field $k(s)$.

Given an S-group scheme G and an integer n, we define $[n] = [n]_G \colon G \to G$ to be the morphism which on sections—using multiplicative notation for the group law—is given by $g \mapsto g^n$. If $n \geqslant 1$ it factors as

$$[n] = (G \xrightarrow{\Delta^n_{G/S}} G^n_S \xrightarrow{m^{(n)}} G)\,,$$

where $m^{(n)}$ is the "iterated multiplication map", given on sections by $(g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$. For commutative group schemes $[n]$ is usually called "multiplication by n".

GrFunctors **(3.2)** The definitions given in (3.1) are sometimes not so practicable. For instance, to define a group scheme one would have to give a scheme G, then one needs to define the morphisms m, i and e, and finally one would have to verify that a number of morphisms agree. Would it not be much simpler to describe a group as a scheme whose points form a group? Fortunately this can be done; it provides a way of looking at group schemes that is often more natural than the definition given above.

Suppose we have a scheme X over some base scheme S. For many purposes the underlying point set $|X|$ is not a good object to work with. For instance, if X is a group variety then $|X|$ will in general not inherit a group structure. However, there is another meaning of the term "point of X", and this notion is a very convenient one. Namely, recall that if $T \to S$ is another S-scheme then by a T-valued point of X we mean a morphism of schemes $x \colon T \to X$ over S. The set of such points is denoted $X(T)$. As a particular case, suppose $S = \operatorname{Spec}(k)$ and $T = \operatorname{Spec}(K)$, where $k \subset K$ is a field extension. Then one would also refer to a T-valued point of X as a "K-rational point", or in some contexts also as a "point of X with coordinates in K".

It is useful to place our discussion in a more general context. For this, consider a category C. The example to keep in mind is the category $C = \mathsf{Sch}_{/S}$ of schemes over a base scheme S. Write $\widehat{C}$ for the category of contravariant functors $C \to \mathsf{Sets}$ with morphisms of functors as the morphisms in $\widehat{C}$. For $X \in C$, the functor $h_X = \operatorname{Hom}_C(-, X)$ is an object of $\widehat{C}$. Sending X to h_X gives a covariant functor $h \colon C \to \widehat{C}$. The basic observation is that in this process we lose no information, as made precise by the following fundamental lemma.

YonLem **(3.3) Yoneda Lemma.** *The functor $h \colon C \to \widehat{C}$ is fully faithful. That is, for all objects X and X' of C, the natural map $\operatorname{Hom}_C(X, X') \to \operatorname{Hom}_{\widehat{C}}(h_X, h_{X'})$ is a bijection. More generally: for every $F \in \widehat{C}$ and $X \in C$, there is a canonical bijection $F(X) \to \operatorname{Hom}_{\widehat{C}}(h_X, F)$.*

Proof. Suppose given $F \in \widehat{C}$ and $X \in C$. The identity morphism id_X is an element of $h_X(X)$. If $\alpha \in \operatorname{Hom}_{\widehat{C}}(h_X, F)$ then define $\psi(\alpha) := \alpha(\mathrm{id}_X) \in F(X)$. This gives a map $\psi \colon \operatorname{Hom}_{\widehat{C}}(h_X, F) \to F(X)$. In the other direction, suppose we have $\beta \in F(X)$. If $x \colon T \to X$ is an element of $h_X(T)$ for some $T \in C$, define $\varphi(\beta)(x) \in F(T)$ to be the image of β under $F(x) \colon F(X) \to F(T)$. Now it is straightforward to verify that this gives a map $\varphi \colon F(X) \to \operatorname{Hom}_{\widehat{C}}(h_X, F)$ which is an inverse of ψ. □

ReprFun **(3.4) Definition.** A functor $F \in \widehat{C}$ is said to be *representable* if it is isomorphic to a functor h_X for some $X \in C$. If this holds then it follows from the Yoneda lemma that X is uniquely determined by F up to C-isomorphism, and any such X is said to *represent* the functor F.

GrFunII **(3.5)** Continuing the discussion of (3.2), we define the notion of a group object in the category C via the embedding into $\widehat{C}$. Thus, if X is an object of C then we define a C-group law on X to be a lifting of the functor $h_X \colon C \to \mathsf{Sets}$ to a group-valued functor $\tilde{h}_X \colon C \to \mathsf{Gr}$. Concretely, to

give a group law on an object X means that for each object T in C we have to specify a group law on the set $h_X(T) = \mathrm{Hom}_C(T, X)$, such that for every morphism $f\colon T_1 \to T_2$ the induced map $h_X(f)\colon h_X(T_2) \to h_X(T_1)$ is a homomorphism of groups. An object of C together with a C-group law on it is called a *C-group*, or a *group object in C*. In exactly the same way we can define other algebraic structures in a category, such as the notion of a ring object in C.

Let us now suppose that C is a category with finite products. This means that C has a final object (the empty product), which we shall call S, and that for any two objects X and Y there exists a product $X \times Y$. If G is a group object in C then the group structure on h_G gives a morphism of functors

$$m\colon h_{G\times_S G} = h_G \times h_G \longrightarrow h_G\,.$$

The Yoneda lemma tells us that this morphism is induced by a unique morphism $m_G\colon G\times_S G \to G$. In a similar way we obtain morphisms $i_G\colon G \to G$ and $e_G\colon S \to G$, and these morphisms satisfy the relations of (3.1)(i). Conversely, data (m_G, i_G, e_G) satisfying these relations define a C-group structure on the object G.

Applying the preceding remarks to the category $\mathsf{Sch}_{/S}$ of schemes over S, which is a category with finite products and with S as final object, we see that a group scheme G over S is the same as a representable group functor on $\mathsf{Sch}_{/S}$ together with the choice of a representing object (namely G). The conclusion of this discussion is so important that we state it as a proposition.

GrFunProp **(3.6) Proposition.** *Let G be a scheme over a base scheme S. Then the following data are equivalent:*

(i) *the structure of an S-group scheme on G, in the sense of* Definition (3.1)*;*

(ii) *a group structure on the sets $G(T)$, functorial in $T \in \mathsf{Sch}_{/S}$.*

For homomorphisms we have a similar assertion: if G_1 and G_2 are S-group schemes then the following data are equivalent:

(i) *a homomorphism of S-group schemes $f\colon G_1 \to G_2$, in the sense of* Definition (3.1)*;*

(ii) *group homomorphisms $f(T)\colon G_1(T) \to G_2(T)$, functorial in $T \in \mathsf{Sch}_{/S}$.*

In practise we often identify a group scheme G with the functor of points h_G, and we use the same notation G for both of them.

Already in the simplest examples we will see that this is useful, since it is often easier to understand a group scheme in terms of its functor of points than by giving the structure morphisms m, i and e. Before we turn to examples, let us use the functorial language to define the notion of a subgroup scheme.

SubgrSchDef **(3.7) Definition.** Let G be a group scheme over S. A subscheme (resp. an open subscheme, resp. a closed subscheme) $H \subset G$ is called an *S-subgroup scheme* (resp. an *open S-subgroup scheme*, resp. a *closed S-subgroup scheme*) of G if h_H is a subgroup functor of h_G, i.e., if $H(T) \subset G(T)$ is a subgroup for every S-scheme T. A subgroup scheme $H \subset G$ is said to be *normal* in G if $H(T)$ is a normal subgroup of $G(T)$ for every S-scheme T.

In the sequel, if we speak about subgroup schemes it shall be understood that we give H the structure of an S-group scheme induced by that on G. An alternative, but equivalent, definition of the notion of a subgroup scheme is given in Exercise (3.1).

GrSchExa **(3.8) Examples.** 1. The *additive group*. Let S be a base scheme. The additive group over S, denoted $\mathbb{G}_{a,S}$, corresponds to the functor which associates to an S-scheme T the additive group $\Gamma(T, O_T)$. For simplicity, let us assume that $S = \mathrm{Spec}(R)$ is affine. Then $\mathbb{G}_{a,S}$ is represented by

the affine S-scheme $\mathbb{A}^1_S = \mathrm{Spec}\big(R[x]\big)$. The structure of a group scheme is given, on rings, by the following homomorphisms:

$\tilde{m}\colon R[x] \to R[x] \otimes_R R[x]$	given by	$x \mapsto x \otimes 1 + 1 \otimes x\,,$	defining the group law;
$\tilde{i}\colon R[x] \to R[x]$	given by	$x \mapsto -x\,,$	defining the inverse;
$\tilde{e}\colon R[x] \to R$	given by	$x \mapsto 0\,,$	defining the identity.

(See (3.9) below for further discussion of how to describe an affine group scheme in terms of a Hopf algebra.)

2. The *multiplicative group*. This group scheme, denoted $\mathbb{G}_{m,S}$, represents the functor which associates to an S-scheme T the multiplicative group $\Gamma(T, O_T)^*$ of invertible elements of $\Gamma(T, O_T)$. As a scheme, $\mathbb{G}_m = \mathrm{Spec}\,\big(O_S[x, x^{-1}]\big)$. The structure of a group scheme is defined by the homomorphisms given by

$x \mapsto x \otimes x$	defining the multiplication;
$x \mapsto x^{-1}$	defining the inverse;
$x \mapsto 1$	defining the identity element.

3. *n-th Roots of unity*. Given a positive integer n, we have an S-group scheme $\mu_{n,S}$ which associates to an S-scheme T the subgroup of $\mathbb{G}_m(T)$ of elements whose order divides n. The O_S-algebra defining this group scheme is $O_S[x, x^{-1}]/(x^n - 1)$ with the group law given as in Example 2. Put differently, $\mu_{n,S}$ is a closed subgroup scheme of $\mathbb{G}_{m,S}$.

4. *p^n-th Roots of zero*. Let p be a prime number and suppose that $\mathrm{char}(S) = p$. Consider the closed subscheme $\alpha_{p^n,S} \subset \mathbb{G}_{a,S}$ defined by the ideal (x^{p^n}); so $\alpha_{p^n,S} := \mathrm{Spec}\,\big(O_S[x]/(x^{p^n})\big)$. As is not hard to verify, this is in fact a closed subgroup scheme of $\mathbb{G}_{a,S}$. If $S = \mathrm{Spec}(k)$ for a field k of characteristic p then geometrically $\alpha_{p^n,k}$ is just a "fat point" (a point together with its $(p^n - 1)$st infinitesimal neighbourhood); but as a group scheme it has an interesting structure. If T is an S-scheme then $\alpha_{p^n}(T) = \{f \in \Gamma(T, O_T) \mid f^{p^n} = 0\}$, with group structure given by addition.

5. *Constant group schemes*. Let M be an arbitrary (abstract) group. Let $M_S := S^{(M)}$, the direct sum of copies of S indexed by the set M. If T is an S-scheme then $M_S(T)$ is the set of locally constant functions of $|T|$ to M. The group structure on M clearly induces the structure of a group functor on M_S (multiplication of functions), so that M_S becomes a group scheme. The terminology "constant group scheme" should not be taken to mean that the functor $T \mapsto M_S(T)$ has constant value M; in fact, if M is non-trivial then $M_S(T) = M$ only if T is connected.

In Examples 1–3 and 5, the group schemes as described here are all defined over $\mathrm{Spec}(\mathbb{Z})$. That is, in each case we have $G_S = G_{\mathbb{Z}} \times_{\mathrm{Spec}(\mathbb{Z})} S$ where $G_{\mathbb{Z}}$ is "the same" example but now over the basis $\mathrm{Spec}(\mathbb{Z})$. The group schemes α_{p^n} of Example 4 are defined over $\mathrm{Spec}(\mathbb{F}_p)$. The subscript "$_S$" is sometimes omitted if the basis is $\mathrm{Spec}(\mathbb{Z})$ resp. $\mathrm{Spec}(\mathbb{F}_p)$, or if it is understood over which basis we are working.

If $G = \mathrm{Spec}(A)$ is a finite k-group scheme then by the *rank* of G we mean the k-dimension of its affine algebra A. Thus, for instance, the constant group scheme $(\mathbb{Z}/p\mathbb{Z})_k$, and (for $\mathrm{char}(k) = p$) the group schemes $\mu_{p,k}$ and $\alpha_{p,k}$ all have rank p.

6. As is clear from the definitions, a group variety over a field k is the same as a geometrically integral group scheme over k. In particular, abelian varieties are group schemes.

7. Using the Yoneda lemma one easily sees that, for a group scheme G over a basis S, the morphism $i\colon G \to G$ is a homomorphism of group schemes if and only if G is commutative.

8. Let S be a basis with $\mathrm{char}(S) = p$. If G is an S-group scheme then $G^{(p/S)}$ naturally inherits the structure of an S-group scheme (being the pull-back of G via the absolute Frobenius morphism $\mathrm{Frob}_S\colon S \to S$). The relative Frobenius morphism $F_{G/S}\colon G \to G^{(p/S)}$ is a homomorphism of S-group schemes.

9. Let V be a finite dimensional vector space over a field k. Then we can form the group variety $\mathrm{GL}(V)$ over k. If $T = \mathrm{Spec}(R)$ is an affine k-scheme then $\mathrm{GL}(V)(T)$ is the group of invertible R-linear transformations of $V \otimes_k R$. If $d = \dim_k(V)$ then $\mathrm{GL}(V)$ is non-canonically (choice of a k-basis for V) isomorphic to the group variety $\mathrm{GL}_{d,k}$ of invertible $d \times d$ matrices; as a scheme the latter is given by

$$\mathrm{GL}_{d,k} = \mathrm{Spec}\left(k[T_{ij}, U;\, 1 \leqslant i, j \leqslant d]/(\det \cdot U - 1)\right),$$

where $\det \in k[T_{ij}]$ is the determinant polynomial. (So " $U = \det^{-1}$ ".) We leave it to the reader to write out the formulas for the group law.

More generally, if V is a vector bundle on a scheme S then we can form the group scheme $\mathrm{GL}(V/S)$ whose T-valued points are the vector bundle automorphisms of V_T over T. If V has rank d then this group scheme is locally on S isomorphic to a group scheme $\mathrm{GL}_{d,S}$ of invertible $d \times d$ matrices.

10. As another illustration of the functorial point of view, let us define semi-direct products. Let N and Q be two group schemes over a basis S. Consider the contravariant functor $\underline{\mathrm{Aut}}(N)\colon \mathsf{Sch}_{/S} \to \mathsf{Gr}$ which associates to an S-scheme T the group of automorphisms of N_T as a T-group scheme. Suppose we are given an action of Q on N by group scheme automorphisms; by this we mean that we are given a homomorphism of group functors

$$\rho\colon Q \to \underline{\mathrm{Aut}}(N).$$

Then we can form the semi-direct product group scheme $N \rtimes_\rho Q$. The underlying scheme is just the product scheme $N \times_S Q$. The group structure is defined on T-valued points by

$$(n, q) \cdot (n', q') = \left(n \cdot \rho(q)(n'), q \cdot q'\right),$$

as expected. By (3.6) this defines an S-group scheme $N \rtimes_\rho Q$.

Here is an application. In ordinary group theory we know that every group of order p^2 is commutative. The analogue of this in the context of group schemes does not hold. Namely, if k is a field of characteristic $p > 0$ then there exists a group scheme of rank p^2 over k that is not commutative. We construct it as a semi-direct product. First note that there is a natural action of the group scheme $\mathbb{G}_m$ on the group scheme $\mathbb{G}_a$; on points it is given by the usual action of $\mathbb{G}_m(T) = \Gamma(T, O_T)^*$ on $\mathbb{G}_a(T) = \Gamma(T, O_T)$. This action restricts to a (non-trivial) action of $\mu_{p,k} \subset \mathbb{G}_{m,k}$ on $\alpha_{p,k} \subset \mathbb{G}_{a,k}$. Then the semi-direct product $\alpha_p \rtimes \mu_p$ has rank p^2 but is not commutative.

AffGrSch **(3.9)** *Affine group schemes.* Let $S = \mathrm{Spec}(R)$ be an affine base scheme. Suppose $G = \mathrm{Spec}(A)$ is an S-group scheme which is affine as a scheme. Then the morphisms m, i and e giving G its structure of a group scheme correspond to R-linear homomorphisms

$\tilde{m}\colon A \to A \otimes_R A$	called co-multiplication,
$\tilde{i}\colon A \to A$	called antipode or co-inverse,
$\tilde{e}\colon A \to R$	called augmentation or co-unit.

These homomorphisms satisfy a number of identities, corresponding to the identities in the definition of a group scheme; see (3.1)(i). For instance, the associativity of the group law corresponds to the identity

$$(\tilde{m} \otimes 1) \circ \tilde{m} = (1 \otimes \tilde{m}) \circ \tilde{m} \colon A \to A \otimes_R A \otimes_R A \,.$$

We leave it to the reader to write out the other identities.

A unitary R-algebra equipped with maps $\tilde{m}$, $\tilde{e}$ and $\tilde{i}$ satisfying these identities is called a *Hopf algebra* or a *co-algebra* over R. A Hopf algebra is said to be co-commutative if $s \circ \tilde{m} = \tilde{m} \colon A \to A \otimes_R A$, where $s \colon A \otimes_R A \to A \otimes_R A$ is given by $x \otimes y \mapsto y \otimes x$. Thus, the category of affine group schemes over R is anti-equivalent to the category of commutative R-Hopf algebras, with commutative group schemes corresponding to Hopf algebras that are both commutative and co-commutative. For general theory of Hopf algebras we refer to ??. Note that in the literature Hopf algebras can be non-commutative algebras. *In this chapter, Hopf algebras are assumed to be commutative.*

The ideal $I := \mathrm{Ker}(\tilde{e} \colon A \to R)$ is called the *augmentation ideal*. Note that $A = R \cdot 1 \oplus I$ as R-module, since the R-algebra structure map $R \to A$ is a section of the augmentation. Note that the condition that $e \colon S \to G$ is a two-sided identity element is equivalent to the relation

BasGS:com
$$\tilde{m}(\alpha) = (\alpha \otimes 1) + (1 \otimes \alpha) \bmod I \otimes I \tag{1}$$

in the ring $A \otimes_R A$. For the co-inverse we then easily find the relation

BasGS:coi
$$\tilde{i}(\alpha) = -\alpha \bmod I^2 \,, \quad \text{if } \alpha \in I \,. \tag{2}$$

(Exercise (3.3) asks you to prove this.)

The above has a natural generalization. Namely, suppose that G is a group scheme over an arbitrary basis S such that the structural morphism $\pi \colon G \to S$ is affine. (In this situation we say that G is an affine group scheme over S; cf. (3.10) below.) Let $A_G := \pi_* O_G$, which is a sheaf of O_S-algebras. Then $G \cong \mathrm{Spec}(A_G)$ as S-schemes, and the structure of a group scheme is given by homomorphisms of (sheaves of) O_S-algebras

$$\tilde{m} \colon A_G \to A_G \otimes_{O_S} A_G \,, \quad \tilde{i} \colon A_G \to A_G \,, \quad \text{and} \quad \tilde{e} \colon A_G \to O_S$$

making A_G into a sheaf of commutative Hopf algebras over O_S. Note that the unit section $e \colon S \to G$ gives an isomorphism between S and the closed subscheme of G defined by the augmentation ideal $I := \mathrm{Ker}(\tilde{e})$.

§2. *Elementary properties of group schemes.*

GSterminol **(3.10)** Let us set up some terminology for group schemes. As a general rule, if P is a property of morphisms of schemes (or of schemes) then we say that a group scheme G over S with structural morphism $\pi \colon G \to S$ has property P if π has this property as a morphism of schemes (or if G, as a scheme, has this property). Thus, for example, we say that an S-group scheme G is noetherian, or finite, if G is a noetherian scheme, resp. if π is a finite morphism. Other properties for which the rule applies: the property of a morphism of schemes of being quasi-compact, quasi-separated, (locally) of finite type, (locally) of finite presentation, finite and locally free, separated, proper,

flat, and unramified, smooth, or étale. Similarly, if the basis S is the spectrum of a field k then we say that G is (geometrically) reduced, irreducible, connected or integral if G has this property as a k-scheme.

Note that we call G an *affine group scheme over* S if π is an affine morphism; we do not require that G is affine as a scheme. Also note that if G is a finite S-group scheme then this does not say that $G(T)$ is finite for every S-scheme T. For instance, we have described the group scheme α_p (over a field k of characteristic p) as a "fat point", so it should have a positive dimensional tangent space. Indeed, $\alpha_p(k) = \{1\}$ but $\alpha_p\big(k[\varepsilon]\big) = \{1 + a\varepsilon \mid a \in k\}$. We find that the tangent space of α_p at the origin has k-dimension 1 and that $\alpha_p\big(k[\varepsilon]\big)$ is infinite if k is infinite.

Let us also recall how the predicate "universal(ly)" is used. Here the general rule is the following: we say that $\pi\colon G \to S$ universally has property P if for every morphism $f\colon S' \to S$, writing $\pi'\colon G' \to S'$ for the morphism obtained from π by base-change via f, property P holds for G' over S'.

Let us now discuss some basic properties of group schemes. We begin with a general lemma.

SectLem **(3.11) Lemma.** (i) *Let*

$$\begin{array}{ccc} X' & \xrightarrow{i} & X \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle g} \\ Y' & \xrightarrow{j} & Y \end{array}$$

be a cartesian diagram in the category of schemes. If g is an immersion (resp. a closed immersion, resp. an open immersion) then so is g'.

(ii) *Let $f\colon Y \to X$ be a morphism of schemes. If $s\colon X \to Y$ is a section of f then s is an immersion. If f is separated then s is a closed immersion.*

(iii) *If $s\colon X \to Y$ is a section of a morphism f, as in* (ii)*, then s maps closed points of X to closed points of Y.*

Proof. (i) Suppose g is an immersion. This means we have a subscheme $Z \subset Y$ such that g induces an isomorphism $X \xrightarrow{\sim} Z$. If Z is an open subscheme (i.e., g an open immersion) then $Y' \times_Y Z$ is naturally isomorphic to the open subscheme $j^{-1}(Z)$ of Y', and the claim follows. If Z is a closed subscheme defined by some ideal $I \subset O_Y$ (i.e, g a closed immersion) then $Y' \times_Y Z$ is naturally isomorphic to the closed subscheme of Y' defined by the ideal generated by $j^{-1}(I)$; again the claim follows. The case of a general immersion follows by combining the two previous cases.

(ii) By (i), it suffices to show that the commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad s \quad} & Y \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle \Delta_{Y/X}} \\ Y & \xrightarrow{\mathrm{id}_Y \times (s \circ f)} & Y \times_X Y \end{array} \tag{3}$$

BasGS:diagr

is cartesian. This can be done by working on affine open sets. Alternatively, if T is any scheme then the corresponding diagram of T-valued points is a cartesian diagram of sets, as one easily checks. It then follows from the Yoneda lemma that (3) is cartesian.

(iii) Let $P \in X$ be a closed point. Choose an affine open $U \subset Y$ containing $s(P)$. It suffices to check that $s(P)$ is a closed point of U. (This is special about working with points, as opposed

to arbitrary subschemes.) But $U \to X$ is affine, hence separated, so (i) tells us that $s(P)$ is a closed point of U. Alternatively, the assertion becomes obvious by working on rings. □

SepGrSch **(3.12) Proposition.** (i) *An S-group scheme G is separated if and only if the unit section e is a closed immersion.*

(ii) *If S is a discrete scheme (e.g., the spectrum of a field) then every S-group scheme is separated.*

Proof. (i) The "only if" follows from (ii) of the lemma. For the converse, consider the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi} & S \\ {\scriptstyle \Delta_{G/S}}\downarrow & & \downarrow{\scriptstyle e} \\ G \times_S G & \xrightarrow{m \circ (\mathrm{id}_G \times i)} & G \end{array}$$

For every S-scheme T it is clear that this diagram is cartesian on T-valued points. By the Yoneda lemma it follows that the diagram is cartesian. Now apply (i) of the lemma.

(ii) Since separatedness is a local property on the basis, it suffices to consider the case that S is a 1-point scheme. Then the unit section is closed, by (iii) of the lemma. Now apply (i). □

As the following example shows, the result of (ii) is in some sense the best possible. Namely, suppose that S is a scheme which is *not* discrete. Then S has a non-isolated closed point s (i.e., a closed point s which is not open). Define G as the S-scheme obtained by gluing two copies of S along $S \setminus \{s\}$. Then G is not separated over S, and one easily shows that G has a structure of S-group scheme with $G_s \cong (\mathbb{Z}/2\mathbb{Z})_{k(s)}$. Notice that in this example G is even étale over S.

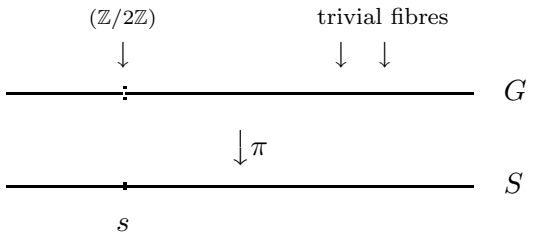


Figure 3.

KerDef **(3.13) Definition.** (i) Let G be an S-group scheme with unit section $e\colon S \to G$. Define $e_G = e(S) \subset G$ (a subscheme of G) to be the image of the immersion e.

(ii) Let $f\colon G \to G'$ be a homomorphism of S-group schemes. Then we define the *kernel of f* to be the subgroup scheme $\mathrm{Ker}(f) := f^{-1}(e_{G'})$ of G.

Note that the diagram

$$\begin{array}{ccc} \mathrm{Ker}(f) & \hookrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle f} \\ S & \xrightarrow{e} & G' \end{array}$$

is cartesian. In particular, $\mathrm{Ker}(f)$ represents the contravariant functor $\mathsf{Sch}_{/S} \to \mathsf{Gr}$ given by

$$T \mapsto \mathrm{Ker}\Big(f(T)\colon G(T) \longrightarrow G'(T)\Big)$$

and is a normal subgroup scheme of G. If G' is separated over S then $\mathrm{Ker}(f) \subset G$ is a closed subgroup scheme.

As examples of kernels we have, taking $S = \mathrm{Spec}(\mathbb{F}_p)$ as our base scheme,

$$\mu_p = \mathrm{Ker}(F\colon \mathbb{G}_m \to \mathbb{G}_m)\,, \quad \alpha_p = \mathrm{Ker}(F\colon \mathbb{G}_a \to \mathbb{G}_a)\,,$$

where in both cases F denotes the Frobenius endomorphism.

TranslGS **(3.14)** *Left and right translations; sheaves of differentials.* Let G be a group scheme over a basis S. Given an S-scheme T and a point $g \in G(T)$, the right translation $t_g\colon G_T \to G_T$ and the left translation $t'_g\colon G_T \to G_T$ are defined just as in (1.4). Using the Yoneda lemma we can also define t_g and t'_g by saying that for every T-scheme T', the maps $t_g(T')\colon G(T') \to G(T')$ and $t'_g(T')\colon G(T') \to G(T')$ are given by $\gamma \mapsto \gamma g$ resp. $\gamma \mapsto g\gamma$. Here we view g as an element of $G(T')$ via the canonical homomorphism $G(T) \to G(T')$.

If in the above we take $T = G$ and $g = \mathrm{id}_G \in G(G)$ then the resulting translations τ and $\tau'\colon G \times_S G \to G \times_S G$ are given by $(g_1, g_2) \to (g_1 g_2, g_2)$, resp. $(g_1, g_2) \to (g_2 g_1, g_2)$. Here we view $G \times_S G$ as a scheme over G via the second projection. We call τ and τ' the *universal right (resp. left) translation*. The point is that any other right translation $t_g\colon G \times_S T \to G \times_S T$ as above is the pull-back of τ via $\mathrm{id}_G \times g$ (i.e., the pull-back via g on the basis), and similarly for left translations.

As we have seen in (1.5), the translations on G are important in the study of sheaves of differentials. We will formulate everything using right translations. A 1-form $\alpha \in \Gamma(G, \Omega^1_{G/S})$ is said to be (right) invariant if it is universally invariant under right translations; by this we mean that for every $T \to S$ and $g \in G(T)$, writing $\alpha_T \in \Gamma(T, \Omega^1_{G_T/T})$ for the pull-back of α via $G_T \to G$, we have $t_g^* \alpha_T = \alpha_T$. In fact, it suffices to check this in the universal case: α is invariant if and only if $p_1^*\alpha \in \Gamma(G \times_S G, p_1^* \Omega^1_{G/S})$ is invariant under τ. The invariant differentials form a subsheaf $(\pi_* \Omega^1_{G/S})^G$ of $\pi_* \Omega^1_{G/S}$.

For the next result we need one more notation: if $\pi\colon G \to S$ is a group scheme with unit section $e\colon S \to G$, then we write

$$\omega_{G/S} := e^* \Omega^1_{G/S}\,,$$

which is a sheaf of O_S-modules. If S is the spectrum of a field then $\omega_{G/S}$ is just cotangent space of G at the origin.

FreeTangGS **(3.15) Proposition.** *Let $\pi\colon G \to S$ be a group scheme. Then there is a canonical isomorphism $\pi^* \omega_{G/S} \xrightarrow{\sim} \Omega^1_{G/S}$. The corresponding homomorphism $\omega_{G/S} \to \pi_* \Omega^1_{G/S}$ (by adjunction of the functors π^* and π_*) induces an isomorphism $\omega_{G/S} \xrightarrow{\sim} (\pi_* \Omega^1_{G/S})^G$.*

Proof. As in (1.5), the geometric idea is that an invariant 1-form on G can be reobtained from its value along the zero section by using the translations, and that, by a similar proces, an arbitrary 1-form can be written as a function on G times an invariant form. To turn this idea into a formal proof we use the universal translation τ.

As above, we view $G \times_S G$ as a G-scheme via p_2. Then τ is an automorphism of $G \times_S G$ over G, so we have a natural isomorphism

BasGS:tauOmeg
$$\tau^* \Omega^1_{G \times_S G/G} \xrightarrow{\sim} \Omega^1_{G \times_S G/G}\,. \tag{4}$$

We observe that $G \times_S G/G$ is the pull back under p_1 of G/S; this gives that $\Omega^1_{G \times_S G/G} = p_1^* \Omega^1_{G/S}$. As $\tau = (m, p_2)\colon G \times_S G \to G \times_S G$, we find that (4) can be rewritten as

$$m^* \Omega^1_{G/S} \xrightarrow{\sim} p_1^* \Omega^1_{G/S}\,.$$

Pulling back via $(e\circ\pi, \mathrm{id}_G)\colon G \to G \times_S G$ gives the isomorphism

BasGS:Omega1
$$\Omega^1_{G/S} \xrightarrow{\sim} \pi^* e^* \Omega^1_{G/S} = \pi^* \omega_{G/S}\,. \tag{5}$$

By adjunction, (5) gives rise to a homomorphism $\pi^*\colon \omega_{G/S} \to \pi_*\Omega^1_{G/S}$ associating to a section $\beta \in \Gamma(S, \omega_{G/S})$ the 1-form $\pi^*\beta \in \Gamma(G, \pi^*\omega_{G/S}) = \Gamma(G, \Omega^1_{G/S})$. The isomorphism (5) is constructed in such a way that $\pi^*\beta$ is an invariant form. Clearly $e^*(\pi^*\beta) = \beta$. Conversely, if $\alpha \in \Gamma(G, \Omega^1_{G/S})$ is an invariant form then $m^*(\alpha) = \tau^*\big(p_1^*(\alpha)\big) = p_1^*(\alpha)$. Pulling back (as in the above argument) via $(e\circ\pi, \mathrm{id}_G)$ then gives that $\alpha = \pi^* e^*(\alpha)$. This shows that the map $(\pi_*\Omega^1_{G/S})^G \to \omega_{G/S}$ given on sections by $\alpha \mapsto e^*\alpha$ is an inverse of π^*. □

IdCompGS **(3.16)** *The identity component of a group scheme over a field.* Let G be a group scheme over a field k. By (3.12), G is separated over k. The image of the identity section is a single closed point $e = e_G$ of degree 1.

Assume in addition that G is locally of finite type over k. Then the scheme G is locally noetherian, hence locally connected. If we write G^0 for the connected component of G containing e, it follows that G^0 is an open subscheme of G. We call G^0 the *identity component* of G.

Geometrically, one expects that the existence of a group structure implies that G, as a k-scheme, "looks everywhere the same", so that certain properties need to be tested only at the origin. The following proposition shows that for smoothness and reducedness this is indeed the case. Note, however, that our intuition is a geometric one: in general we can only expect that "G looks everywhere locally the same" if we work over $k = \overline{k}$. In the following proposition it is good to keep some simple examples in mind. For instance, let p be a prime number and consider the group scheme μ_p over the field $\mathbb{Q}$. The underlying topological space consists of two closed points: the origin $e = 1$, and a point P corresponding to the non-trivial pth roots of unity. If we extend scalars from $\mathbb{Q}$ to a field containing a pth root of unity then the identity component $(\mu_p)^0 = \{e\}$ stays connected but the other component $\{P\}$ splits up into a disjoint union of $p-1$ connected components.

GSfieldProp **(3.17) Proposition.** *Let G be a group scheme, locally of finite type over a field k.*

(i) *The identity component G^0 is an open and closed subgroup scheme of G which is geometrically irreducible. In particular: for any field extension $k \subset K$, we have $(G^0)_K = (G_K)^0$.*

(ii) *The following properties are equivalent:*

(a1) *$G \otimes_k K$ is reduced for some perfect field K containing k;*

(a2) *the ring $O_{G,e} \otimes_k K$ is reduced for some perfect field K containing k;*

(b1) *G is smooth over k;*

(b2) *G^0 is smooth over k;*

(b3) *G is smooth over k at the origin.*

(iii) *Every connected component of G is irreducible and of finite type over k.*

Proof. (i) We first prove that G^0 is geometrically connected; that it is even geometrically irreducible will then follow from (iii). More generally, we show that if X is a connected k-scheme, locally of finite type, that has a k-rational point $x \in X(k)$ then X is geometrically connected. (See EGA IV, 4.5.14 for a more general result.)

Let $\overline{k}$ be an algebraic closure of k. First we show that the projection $p\colon X_{\overline{k}} \to X$ is open and closed. Suppose $\{V_\alpha\}_{\alpha\in I}$ is an open covering of X. Then $\{V_{\alpha,\overline{k}}\}_{\alpha\in I}$ is a covering of $X_{\overline{k}}$. If each $V_{\alpha,\overline{k}} \to V_\alpha$ is open and closed then the same is true for p. Hence we may assume that X is

affine and of finite type over k. Let $Z \subset X_{\overline{k}}$ be closed. Then there is a finite extension $k \subset K$ inside $\overline{k}$ such that Z is defined over K; concretely this means that there is closed subscheme $Z_K \subset X_K$ with $Z = Z_K \otimes_K \overline{k}$. Hence it suffices to show that the morphism $p_K\colon X_K \to X$ is open and closed. But this is immediate from the fact that p_K is finite and flat. (Use HAG, Chap. III, Ex. 9.1 or EGA IV, Thm. 2.4.6.)

Now suppose we have two non-empty open and closed subsets U_1 and U_2 of $X_{\overline{k}}$. Because X is connected, it follows that $p(U_1) = p(U_2) = X$. The unique point $\overline{x} \in X_{\overline{k}}$ lying over x is therefore contained in $U_1 \cap U_2$; hence $U_1 \cap U_2$ is non-empty. This shows that $X_{\overline{k}}$ is connected.

(ii) The essential step is to prove that (a2) $\Rightarrow$ (b1); all other implications are easy. (For (b3) $\Rightarrow$ (b1) use (3.15).) One easily reduces to the case that $k = \overline{k}$ and that G is reduced at the origin. Using the translations on G it then follows that G is reduced. In this situation, the same argument as in (1.5) applies, showing that G is smooth over k.

For (iii) one first shows that G^0 is irreducible and quasi-compact. We have already shown that $(G^0)_K = (G_K)^0$ for any field extension $k \subset K$, so we may assume that $k = \overline{k}$, in which case we can pass to the reduced underlying group scheme G^0_{red}; see Exercise (3.2). Note that G^0_{red} has the same underlying topological space as G^0. By (ii), G^0_{red} is smooth over k. Every point of G^0_{red} therefore has an open neighbourhood of the form $U = \mathrm{Spec}(A)$ with A a regular ring. As a regular ring is a domain, such an affine scheme U is irreducible. Now suppose G^0_{red} is reducible. Because it is connected, there exist two irreducible components $C_1 \neq C_2$ with $C_1 \cap C_2 \neq \emptyset$. (See EGA 0_{I}, Cor. 2.1.10.) If $y \in C_1 \cap C_2$, let $U = \mathrm{Spec}(A)$ be an affine open neighbourhood of y in G^0_{red} with A regular. Then one of $C_1 \cap U$ and $C_2 \cap U$ contains the other, say $C_2 \cap U \subseteq C_1 \cap U$. But $C_2 \cap U$ is dense in C_2, hence $C_2 \subseteq C_1$. As C_1 and C_2 are irreducible components we must have $C_2 = C_1$, contradicting the assumption.

To prove quasi-compactness of G^0, take a non-empty affine open part $U \subset G^0$. Then U is dense in G^0, as G^0 is irreducible. Hence for every $g \in G^0(k)$ the two sets $g \cdot U^{-1}$ and U intersect. It follows that the map $U \times U \to G^0$ given by multiplication is surjective. But $U \times U$ is quasi-compact, hence so is G^0.

Now we look at the other connected components, working again over an arbitrary field k. If $H \subset G$ is a connected component, choose a closed point $h \in H$. Because G is locally of finite type over k, there is a finite normal field extension $k \subset L$ such that L contains the residue field $k(h)$. As in the proof of (i), the projection $p\colon H \otimes_k L \to H$ is open and closed. One easily shows that all points in $p^{-1}(h)$ are rational over L. If $\tilde{h} \in p^{-1}(h)$ is one of these points then using the translation $t_{\tilde{h}}$ one sees that the connected component $C(\tilde{h})$ of H_L containing $\tilde{h}$ is isomorphic to G^0_L as an L-scheme. Then $p(C(\tilde{h})) \subset H$ is irreducible, closed and open. As H is connected it follows that $p(C(\tilde{h})) = H$ and that H is irreducible. Finally, the preceding arguments show that $H \otimes_k L$ is the union of the components $C(\tilde{h})$ for all $\tilde{h}$ in the finite set $p^{-1}(h)$. As each of these components is isomorphic to G^0_L, which is quasi-compact, it follows that H is quasi-compact. □

G0PropRem **(3.18) Remarks.** (i) Let G be a k-group scheme as in the proposition. Suppose that $G \otimes_k K$ is reduced (or that $O_{G,e} \otimes_k K$ is reduced) for some non-perfect field K containing k. Then it is not necessarily true that G is smooth over k. Here is an example: Suppose $K = k$ is a non-perfect field of characteristic p. Choose an element $\alpha \in k$ not in k^p. Let G be the k-scheme $G = \mathrm{Spec}\big(k[X,Y]/(X^p + \alpha Y^p)\big)$. View $\mathbb{A}^2_k = \mathrm{Spec}\big(k[X,Y]\big)$ as a k-group scheme by identifying it with $\mathbb{G}_{a,k} \times \mathbb{G}_{a,k}$. Then G is a closed subgroup scheme of $\mathbb{A}^2_k$. One easily checks that G is reduced, but clearly it is not geometrically reduced (extend to the field $k(\sqrt[p]{\alpha})$), and therefore G is not a smooth group scheme over k.

(ii) In (iii) of the proposition, let us note that the connected components of G are in general *not* geometrically irreducible; see the example given before the proposition.

ComultOGeRem **(3.19) Remark.** Let G be a group scheme, locally of finite type over a field k. In case G is affine, we have seen in (3.9) that we can study it through its Hopf algebra. For arbitrary G there is no immediate substitute for this, not even if we are only interested in the local structure of G at the origin. Note that the group law does not, in general, induce a co-multiplication on the local ring $O_{G,e}$. We do have a homomorphism $O_{G,e} \to O_{G\times_k G,(e,e)}$ but $O_{G\times_k G,(e,e)}$ is in general of course not the same as $O_{G,e} \otimes_k O_{G,e}$; rather it is a localisation of it. In some cases, however, something slightly weaker already suffices to obtain interesting conclusions. In the proof of the next result we shall exploit the fact that, with $\mathfrak{m} \subset O_{G,e}$ the maximal ideal, we do have a homomorphism $\tilde{m}\colon O_{G,e} \to (O_{G,e}/\mathfrak{m}^q) \otimes_k (O_{G,e}/\mathfrak{m}^q)$ for which the analogue of (1) in section (3.9) holds.

Another possibility is to consider the completed local ring $\hat{O}_{G,e}$. The group law on G induces a co-multiplication $\tilde{m}\colon \hat{O}_{G,e} \to \hat{O}_{G,e}\hat{\otimes}_k\hat{O}_{G,e}$ (completed tensor product). In this way we can associate to a group variety G a (smooth) formal group $\hat{G} = \mathrm{Spf}\big(\hat{O}_{G,e}\big)$. We shall further go into this in ??.

char0red **(3.20) Theorem.** (Cartier) *Let G be a group scheme, locally of finite type over a field k of characteristic zero. Then G is reduced, hence smooth over k.*

Proof. We follow the elementary proof due to Oort [2]. Let $A := O_{G,e}$ be the local ring of G at the identity element. Write $\mathfrak{m} \subset A$ for the maximal ideal and $\mathrm{nil}(A) \subset A$ for the nilradical. Since we are over a perfect field, the reduced scheme G_{red} underlying G is a subgroup scheme (Exercise (3.2)), and by (ii) of Prop. (3.17) this implies that $A_{\mathrm{red}} := A/\mathrm{nil}(A)$ is a regular local ring. Writing $\mathfrak{m}_{\mathrm{red}} := \mathfrak{m}/\mathrm{nil}(A) \subset A_{\mathrm{red}}$, this gives

$$\dim(A) = \dim(A_{\mathrm{red}}) = \dim_k(\mathfrak{m}_{\mathrm{red}}/\mathfrak{m}_{\mathrm{red}}^2) = \dim_k\big(\mathfrak{m}/\mathfrak{m}^2 + \mathrm{nil}(A)\big)\,.$$

In particular, we see that it suffices to show that $\mathrm{nil}(A) \subset \mathfrak{m}^2$. Indeed, if this holds then $\dim(A) = \dim(\mathfrak{m}/\mathfrak{m}^2)$, hence A is regular, hence $\mathrm{nil}(A) = 0$.

Choose $0 \neq x \in \mathrm{nil}(A)$, and let n be the positive integer such that $x^{n-1} \neq 0$ and $x^n = 0$. Because A is noetherian, we have $\cap_{q\geqslant 0}\,\mathfrak{m}^q = (0)$, so there exists an integer $q \geqslant 2$ with $x^{n-1} \notin \mathfrak{m}^q$. Consider $B := A/\mathfrak{m}^q$ and $\bar{\mathfrak{m}} := \mathfrak{m}/\mathfrak{m}^q \subset B$, and let $\bar{x} \in B$ denote the class of $x \in A$ modulo $\mathfrak{m}^q$. As remarked above, the group law on G induces a homomorphism $\tilde{m}\colon A \to B \otimes_k B$. Just as in (3.9), the fact that $e \in G(k)$ is a two-sided identity element implies that we have

BasGS:combis $$\tilde{m}(x) = (\bar{x}\otimes 1) + (1\otimes\bar{x}) + y \qquad \text{with } y \in \bar{\mathfrak{m}} \otimes_k \bar{\mathfrak{m}}\,. \tag{6}$$

(See also Exercise (3.3).) This gives

$$\begin{aligned} 0 = \tilde{m}(x^n) = \tilde{m}(x)^n &= ((\bar{x}\otimes 1) + (1\otimes\bar{x}) + y)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot (\bar{x}\otimes 1)^{n-i} \cdot ((1\otimes\bar{x}) + y)^i\,. \end{aligned}$$

From this we get the relation

$$n\cdot(\bar{x}^{n-1}\otimes\bar{x}) \in \Big((\bar{x}^{n-1}\cdot\bar{\mathfrak{m}})\otimes_k B + B\otimes_k \bar{\mathfrak{m}}^2\Big) \subset B\otimes_k B\,.$$

But $\mathrm{char}(k) = 0$, so that n is a unit, so that even $(\bar{x}^{n-1} \otimes \bar{x}) \in (\bar{x}^{n-1} \cdot \bar{\mathfrak{m}}) \otimes_k B + B \otimes_k \bar{\mathfrak{m}}^2$. Now remark that a relation of the form $y_1 \otimes y_2 \in J_1 \otimes_k B + B \otimes_k J_2$ implies that either $y_1 \in J_1$ or $y_2 \in J_2$. (To see this, simply view B, J_1 and J_2 as k-vector spaces.) But by the Nakayama Lemma, $\bar{x}^{n-1} \in \bar{x}^{n-1} \cdot \bar{\mathfrak{m}}$ implies $\bar{x}^{n-1} = 0$, which contradicts our choice of q. We conclude that $\bar{x} \in \bar{\mathfrak{m}}^2$; hence $x \in \mathfrak{m}^2$, and we are done. □

The conclusion of this theorem does not hold over fields of positive characteristic. For example, if $\mathrm{char}(k) = p > 0$ then the group schemes $\mu_{p,k}$ and $\alpha_{p,k}$ are not reduced, hence not smooth over k. (The argument of the above proof breaks down if n is divisible by p.)

§3. *Cartier duality.*

CDualSetup **(3.21)** *Cartier duality of finite commutative group schemes.* We now discuss some aspects of finite commutative group schemes that play an important role in the study of abelian varieties. In particular, the Cartier duality that we shall discuss here comes naturally into play when we discuss the dual of an abelian variety; see Chapter 7.

The Cartier dual of a group scheme can be defined in two ways: working functorially or working with the underlying Hopf algebras. We first give two constructions of a dual group; after that we prove that they actually describe the same object.

The functorial approach is based on the study of *characters*, by which we mean homomorphisms of the group scheme to the multiplicative group $\mathbb{G}_m$. More precisely, suppose G is any commutative group scheme over a basis S. Then we can define a new contravariant group functor $Hom(G, \mathbb{G}_{m,S})$ on the category of S-schemes by

$$Hom(G, \mathbb{G}_{m,S})\colon T \mapsto \mathrm{Hom}_{\mathsf{GSch}_{/T}}(G_T, \mathbb{G}_{m,T})\,.$$

Next we define a dual object in terms of the Hopf algebra. For this we need to assume that G is commutative and finite locally free over S. As in (3.9) above, write $A := \pi_* O_G$. This A is a finite locally free sheaf of O_S-modules which comes equipped with the structure of a sheaf of co-commutative O_S-Hopf algebras. (Recall that all our Hopf algebras are assumed to be commutative.) Thus we have the following maps:

algebra structure map	$a\colon O_S \to A\,,$	augmentation	$\tilde{e}\colon A \to O_S\,,$
ring multiplication	$\mu\colon A \otimes_{O_S} A \to A\,,$	co-multiplication	$\tilde{m}\colon A \to A \otimes_{O_S} A\,,$
		co-inverse	$\tilde{i}\colon A \to A\,.$

We define a new sheaf of co-commutative O_S-Hopf algebras A^D as follows: first we set $A^D := Hom_{O_S}(A, O_S)$ as an O_S-module. The above maps induce O_S-linear maps

$$\begin{aligned} &a^D\colon A^D \to O_S\,, && \tilde{e}^D\colon O_S \to A^D\,,\\ &\mu^D\colon A^D \to A^D \otimes_{O_S} A^D\,, && \tilde{m}^D\colon A^D \otimes_{O_S} A^D \to A^D\,,\\ & && \tilde{i}^D\colon A^D \to A^D\,. \end{aligned}$$

We give A^D the structure of a sheaf of O_S-algebras by defining $\tilde{m}^D$ to be the multiplication and $\tilde{e}^D$ to be the algebra structure morphism. Next we define a Hopf algebra structure by using μ^D as the co-multiplication, $\tilde{i}^D$ as the co-inverse, and a^D as the co-unit. We leave it to the

reader (Exercise (3.8)) to verify that this gives A^D a well-defined structure of a co-commutative O_S-Hopf algebra. Schematically, if we write the structure maps of a Hopf algebra in a diagram

$$\begin{array}{ccc} & \vdots & \\ \text{multiplication} & \vdots & \text{co-multiplication} \\ & \text{antipode} & \\ \text{algebra structure map} & \vdots & \text{augmentation map} \\ & \vdots & \end{array}$$

then the diagram corresponding to A^D is obtained from that of A by first dualizing all maps and then reflecting in the dotted line.

We write $\alpha\colon A \to (A^D)^D$ for the O_S-linear map which sends a local section $s \in A(U)$ to the section ev_s = "evaluation at s" $\in \mathit{Hom}_{O_S}\big(\mathit{Hom}_{O_S}(A, O_S), O_S\big)(U)$.

CDualThm **(3.22) Theorem.** (Cartier Duality) *Let $\pi\colon G \to S$ be a commutative S-group scheme which is finite and locally free over S. Write $A := \pi_* O_G$, and define the sheaf of co-commutative Hopf algebras A^D over O_S as above. Then $G^D := \mathrm{Spec}(A^D)$ is a commutative, finite locally free S-group scheme which represents the contravariant functor $\mathit{Hom}(G, \mathbb{G}_{m,S})\colon \mathsf{Sch}_{/S} \to \mathsf{Gr}$ given by*

$$T \mapsto \mathrm{Hom}_{\mathsf{GSch}_{/T}}(G_T, \mathbb{G}_{m,T})\,.$$

The homomorphism $(G^D)^D \to G$ induced by the map $\alpha\colon A \to (A^D)^D$ is an isomorphism.

Proof. That G^D is indeed a commutative group scheme is equivalent to saying that A^D is a sheaf of co-commutative Hopf algebras, which we have left as an exercise to the reader. That G^D is again finite and locally free over S (of the same rank as G) is clear, and so is the claim that $(G^D)^D \to G$ is an isomorphism.

Note that the functor $G \mapsto G^D$ is compatible with base-change: if T is an S-scheme and G is a commutative, finite locally free S-group scheme then $(G_T)^D \cong (G^D)_T$ canonically. In particular, to prove that G^D represents the functor $\mathit{Hom}(G, \mathbb{G}_{m,S})$ we may assume that the basis is affine, say $S = \mathrm{Spec}(R)$, and it suffices to show that $G^D(S)$ is naturally isomorphic to the group $\mathrm{Hom}_{\mathsf{GSch}_{/S}}(G, \mathbb{G}_{m,S})$. As S is affine we may view A simply as an R-Hopf algebra (i.e., replace the sheaf A by its R-algebra of global sections).

Among the identities that are satisfied by the structure homomorphisms we have that $(\tilde{e} \otimes \mathrm{id}) \circ \tilde{m}\colon A \to R \otimes_R A \cong A$ is the identity and that $(\tilde{i}, \mathrm{id}) \circ \tilde{m}\colon A \to A$ is equal to the composition $a \circ \tilde{e}\colon A \to R \to A$. In particular, if $b \in A$ is an element with $\tilde{m}(b) = b \otimes b$ then it follows that $\tilde{e}(b) \cdot b = b$ and that $\tilde{i}(b) \cdot b = \tilde{e}(b)$. It follows that

$$\{b \in A^* \mid \tilde{m}(b) = b \otimes b\} = \{b \in A \mid \tilde{m}(b) = b \otimes b \quad \text{and} \quad \tilde{e}(b) = 1\}\,.$$

Write A^{gl} for this set. (Its elements are sometimes referred to as the "group-like" elements of A.) One easily checks that A^{gl} is a subgroup of A^*.

With these remarks in mind, let us compute $\mathrm{Hom}_{\mathsf{GSch}_{/S}}(G, \mathbb{G}_{m,S})$ and $G^D(S)$. The R-algebra homomorphisms $f\colon R[x, x^{-1}] \to A$ are given by the elements $b \in A^*$, via the correspondence $b := f(x)$. The condition on $b \in A^*$ that the corresponding map f is a homomorphism of Hopf algebras is precisely that $\tilde{m}(b) = b \otimes b$. Hence we find a natural bijection $\mathrm{Hom}_{\mathsf{GSch}_S}(G, \mathbb{G}_{m,S}) \xrightarrow{\sim} A^{\mathrm{gl}}$, and one readily verifies this to be an isomorphism of groups.

Every R-module homomorphism $A^D \to R$ is of the form $\mathrm{ev}_b\colon \lambda \mapsto \lambda(b)$ for some $b \in A$. Conversely, if $b \in A$ then one verifies that

$$\mathrm{ev}_b(1) = 1 \quad \Longleftrightarrow \quad \tilde{e}(b) = 1$$

and

$$\mathrm{ev}_b \text{ is a ring homomorphism} \quad \Longleftrightarrow \quad \tilde{m}(b) = b \otimes b\,.$$

This gives a bijection $G^D(S) \xrightarrow{\sim} A^{\mathrm{gl}}$, and again one easily verifies this to be an isomorphism of groups. □

CDualDef **(3.23) Definition.** Let $\pi\colon G \to S$ be a commutative S-group scheme which is finite and locally free over S. Then we call G^D the *Cartier dual* of G. Similarly, if $f\colon G_1 \to G_2$ is a homomorphism between commutative, finite locally free S-group schemes then we obtain an induced homomorphism $f^D\colon G_2^D \to G_1^D$, called the Cartier dual of f.

CDExa **(3.24) Examples.** 1. Take $G = (\mathbb{Z}/n\mathbb{Z})_S$. Then it is clear from the functorial description of the Cartier dual that $G^D = \mu_{n,S}$. Hence $(\mathbb{Z}/n\mathbb{Z})$ and μ_n are Cartier dual to each other. Note that $(\mathbb{Z}/n\mathbb{Z})_S$ and $\mu_{n,S}$ may well be isomorphic. For instance, if $S = \mathrm{Spec}(k)$ is the spectrum of a field and if $\zeta \in k$ is a primitive nth root of 1 then we obtain an isomorphism $(\mathbb{Z}/n\mathbb{Z})_k \xrightarrow{\sim} \mu_{n,k}$ sending $\bar{1}$ to ζ. In particular, if $k = \overline{k}$ and $\mathrm{char}(k) \nmid n$ then $(\mathbb{Z}/n\mathbb{Z})_k \cong \mu_{n,k}$. By contrast, if $\mathrm{char}(k) = p > 0$ and p divides n then $(\mathbb{Z}/n\mathbb{Z})_k$ and $\mu_{n,k}$ are *not* isomorphic.

2. Let S be a scheme of characteristic $p > 0$. We claim that $\alpha_{p,S}$ is its own Cartier dual. Of course this can be shown at the level of Hopf algebras, but the functorial interpretation is perhaps more instructive. As Cartier duality is compatible with base-change it suffices to do the case $S = \mathrm{Spec}(\mathbb{F}_p)$.

Recall that if R is a ring of characteristic p then $\alpha_p(R) = \{r \in R \mid r^p = 0\}$ with its natural structure of an additive group. If we want to make a homomorphism $\alpha_p \to \mathbb{G}_m$ then the most obvious guess is to look for an "exponential". Indeed, if $r \in \alpha_p(R)$ then

$$\exp(r) = 1 + r + \frac{r^2}{2!} + \cdots + \frac{r^{p-1}}{(p-1)!}$$

is a well-defined element of R^*, and $r \mapsto \exp(r)$ defines a homomorphism $\alpha_p(R) \to \mathbb{G}_m(R)$. Now remark that α_p (like $\mathbb{G}_a$) is not just a group scheme but has a natural structure of a functor in rings. The self-duality $\alpha_p \xrightarrow{\sim} \alpha_p^D = \mathit{Hom}_{\mathsf{ShGr}_{/\mathbb{F}_p}}(\alpha_p, \mathbb{G}_m)$ is obtained by sending a point $\xi \in \alpha_p(T)$ (where T is an $\mathbb{F}_p$-scheme) to the homomorphism of group schemes $\alpha_{p,T} \to \mathbb{G}_{m,T}$ given (on points with values in T-schemes) by $x \mapsto \exp(\xi \cdot x)$.

3. After the previous example, one might guess that α_{p^n} is self-dual for all n. This is not the case. Instead, $(\alpha_{p^n})^D$ can be described as the kernel of Frobenius on the group scheme W_n of Witt vectors of length n. See Oort [3], § 10. For a special case of this, see also Exercise ??.

§4. *The component group of a group scheme.*

If X is a topological space then $\pi_0(X)$ denotes the set of connected components of X. The purpose of this section is to discuss a scheme-theoretic analogue of this for schemes that are

locally of finite type over a field k. To avoid confusion we shall use the notation π_0 in the topological context and ϖ_0 for the scheme-theoretic analogue.

If X/k is locally of finite type then $\varpi_0(X)$ will be an étale k-scheme, and $X \mapsto \varpi_0(X)$ is a covariant functor. Furthermore, if G is a k-group scheme, locally of finite type over k, then $\varpi_0(G)$ inherits a natural structure of a group scheme; it is called the component group (scheme) of G.

We start with some generalities on étale group schemes. Let us recall here that, according to our conventions, an étale morphism of schemes $f\colon X \to Y$ is only required to be locally of finite type; see ??.

FEtGrSch **(3.25)** *Étale group schemes over a field.* Let k be a field. Choose a separable algebraic closure k_s and write $\Gamma_k := \mathrm{Gal}(k_s/k)$. Then Γ_k is a pro-finite group, (see Appendix ??) and Galois theory tells us that $L \mapsto \mathrm{Gal}(k_s/L)$ gives a bijection between the field extensions of k inside k_s and the closed subgroups of Γ_k. Finite extensions of k correspond to open subgroups of Γ_k. A reference is Neukirch [1], Sect. 4.1.

By a Γ_k-set we mean a set Y equipped with a continuous left action of Γ_k; the continuity assumption here means that all Γ_k-orbits in Y are finite.

Let $S := \mathrm{Spec}(k)$. If X is a connected étale scheme over S, then X is of the form $X = \mathrm{Spec}(L)$, with L a finite separable field extension of k. An arbitrary étale S-scheme can be written as a disjoint union of its connected components, and is therefore of the form $X = \amalg_{\alpha\in I} \mathrm{Spec}(L_\alpha)$, where I is some index set and where $k \subset L_\alpha$ is a finite separable extension of fields. Hence the description of étale S-schemes is a matter of Galois theory. More precisely, if $\mathsf{Et}_{/k}$ denotes the category of étale k-schemes there is an equivalence of categories

$$\mathsf{Et}_{/k} \xrightarrow{\text{eq}} \big(\Gamma_k\text{-sets}\big)\,.$$

associating to $X \in \mathsf{Et}_{/k}$ the set $X(k_s)$ with its natural Γ_k-action. To obtain a quasi-inverse, write a Γ_k-set Y as a union of orbits, say $Y = \amalg_{\alpha\in I}(\Gamma_k \cdot y_\alpha)$, let $k \subset L_\alpha$ be the finite field extension (inside k_s) corresponding to the open subgroup $\mathrm{Stab}(y_\alpha) \subset \Gamma_k$, and associate to Y the S-scheme $\amalg_{\alpha\in I} \mathrm{Spec}(L_\alpha)$. Up to isomorphism of S-schemes this does not depend on the chosen base points of the Γ_k-orbits, and it gives a quasi-inverse to the functor $X \mapsto X(k_s)$.

This equivalence of categories induces an equivalence between the corresponding categories of group objects. This gives the following result.

FEtGSProp **(3.26) Proposition.** *Let $k \subset k_s$ and $\Gamma_k = \mathrm{Gal}(k_s/k)$ be as above. Associating to an étale k-group scheme G the group $G(k_s)$ with its natural Γ_k-action gives an equivalence of categories*

$$\begin{pmatrix}\text{étale}\\ k\text{-group schemes}\end{pmatrix} \xrightarrow{\text{eq}} \big(\Gamma_k\text{-groups}\big)\,,$$

where by a Γ_k-group we mean an (abstract) group equipped with a continuous left action of Γ_k by group automorphisms.

The proposition tells us that every étale k-group scheme G is a k-form of a constant group scheme. More precisely, consider the (abstract) group $M = G(k_s)$. Then we can form the constant group scheme M_k over k, and the proposition tells us that $G \otimes k_s \cong M_k \otimes k_s$. If G is finite étale over k then we can even find a finite separable field extension $k \subset K$ such that $G_K \cong M_K$. So we can think of étale group schemes as "twisted constant group schemes".

For instance, if $\mathrm{char}(k)$ is prime to n then μ_n is a finite étale group scheme, and $\mu_n(k_s)$ is (non-canonically) isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The action of Γ_k on $\mu_n(k_s)$ is given by a homomorphism $\chi\colon \Gamma_k \to (\mathbb{Z}/n\mathbb{Z})^*$; here the rule is that if $\zeta \in {k_s}^*$ is an n-th root of unity and $\sigma \in \Gamma_k$ then ${}^\sigma\zeta = \zeta^{\chi(\sigma)}$.

Now we turn to the scheme $\varpi_0(X)$ of connected components of X.

pi0XProp **(3.27) Proposition.** *Let X be a scheme, locally of finite type over a field k. Then there is an étale k-scheme $\varpi_0(X)$ and a morphism $q\colon X \to \varpi_0(X)$ over k such that q is universal for k-morphisms from X to an étale k-scheme. (By this we mean: for any k-morphism $h\colon X \to Y$ with Y/k étale, there is a unique k-morphism $g\colon \varpi_0(X) \to Y$ such that $h = g \circ q$.) The morphism q is faithfully flat, and its fibres are precisely the connected components of X.*

Before we give the proof, let us make the last assertion more precise. If P is a point of $\varpi_0(X)$ then $\{P\}$ is a connected component of $\varpi_0(X)$, as the topological space of an étale scheme is discrete. The claim is then that $q^{-1}(P)$, as an open subscheme of X, is a connected component of X, for all points $P \in \bigl|\varpi_0(X)\bigr|$.

Proof. Consider the set $\pi_0^{\mathrm{geom}}(X) := \pi_0\bigl(|X \otimes_k k_s|\bigr)$ with its natural action of Γ_k. First we show that the action of Γ_k is continuous. Let $\mathscr{C} \subset X_{k_s}$ be a connected component. Let $\mathscr{D} \subset X$ be the connected component containing the image of $\mathscr{C}$ under the natural morphism $X_{k_s} \to X$. Then $\mathscr{C}$ is one of the connected components of $\mathscr{D} \otimes_k k_s$. But $\mathscr{D}$, being connected and locally of finite type over k, has only finitely many geometric components; see EGA IV, Prop. (4.5.15). Hence indeed the Γ_k-orbit of $\mathscr{C}$ inside $\pi_0^{\mathrm{geom}}(X)$ is finite.

Define

$$\varpi_0^{\mathrm{geom}}(X) := \coprod_{\alpha \in \pi_0^{\mathrm{geom}}(X)} \mathrm{Spec}(k_s)^{(\alpha)}\,,$$

the disjoint union of copies of $\mathrm{Spec}(k_s)$, one copy for each element of $\pi_0^{\mathrm{geom}}(X)$. Consider the morphism $q^{\mathrm{geom}}\colon X_{k_s} \to \varpi_0^{\mathrm{geom}}(X)$ that on each connected component $X^{(\alpha)} \subset X_{k_s}$ is given by the structural morphism $X^{(\alpha)} \to \mathrm{Spec}(k_s)^{(\alpha)}$. (So a point $P \in X_{k_s}$ is sent to the copy of $\mathrm{Spec}(k_s)$ labelled by the component of X_{k_s} that contains P.) Because the Γ_k-action on the set $\pi_0^{\mathrm{geom}}(X)$ is continuous, there is an étale k-scheme $\varpi_0(X)$ such that we have an isomorphism $\beta\colon \varpi_0(X)\bigl(k_s\bigr) \xrightarrow{\sim} \pi_0^{\mathrm{geom}}(X)$ of sets with Galois action. Up to isomorphism of k-schemes, this scheme is unique, and we have a unique isomorphism $\varpi_0(X) \otimes_k k_s \xrightarrow{\sim} \varpi_0^{\mathrm{geom}}(X)$ that gives the identity on k_s-valued points. (Here we fix the identification β.) Then q^{geom} can be viewed as a morphism

$$q^{\mathrm{geom}}\colon X \otimes_k k_s \to \varpi_0(X) \otimes_k k_s\,,$$

which is Γ_k-equivariant. By Galois descent this defines a morphism $q\colon X \to \varpi_0(X)$ over k. (See also Exercise (3.9).)

Next we show that the fibres of q are the connected components of X. Over k_s this is clear from the construction. Over k it suffices to show that distinct connected components of X are mapped to distinct points of $\varpi_0(X)$. But the connected components of X correspond to the Γ_k-orbits in $\pi_0^{\mathrm{geom}}(X)$, so the claim follows from the result over k_s.

We claim that the morphism $q\colon X \to \varpi_0(X)$ has the desired universal property. To see this, suppose $h\colon X \to Y$ is a k-morphism with Y/k étale. Then $Y \otimes_k k_s$ is a disjoint union of copies of $\mathrm{Spec}(k_s)$. It readily follows from our construction of $\varpi_0(X)$ and q that there is a unique morphism $g^{\mathrm{geom}}\colon \varpi_0(X) \otimes_k k_s \to Y \otimes_k k_s$ such that $h^{\mathrm{geom}}\colon X_{k_s} \to Y_{k_s}$ factors as

$h^{\mathrm{geom}} = g^{\mathrm{geom}} \circ q^{\mathrm{geom}}$. Moreover, g^{geom} is easily seen to be Galois-equivariant; hence we get the desired morphism $g\colon \varpi_0(X) \to Y$ with $h = g \circ q$.

Finally we have to show that q is faithfully flat. But this can be checked after making a base change to k_s, and over k_s it is clear from the construction. □

pi0XComm **(3.28)** In the situation of the proposition, we refer to $\varpi_0(X)$ as the scheme of connected components of X. If $f\colon X \to Y$ is a morphism of schemes that are locally of finite type over k then we write $\varpi_0(f)\colon \varpi_0(X) \to \varpi_0(Y)$ for the unique morphism such that $q_Y \circ f = \varpi_0(f) \circ q_X\colon X \to \varpi_0(Y)$.

pi0GrSch **(3.29)** Let G be a k-group scheme, locally of finite type. The connected components of G_{k_s} are geometrically connected; see EGA IV, Prop. (4.5.21). Therefore $\pi_0^{\mathrm{geom}}(G) := \pi_0\big(|G_{k_s}|\big)$ is equal to $\pi_0\big(|G_{\overline{k}}|\big)$. The natural map $q^{\mathrm{geom}}\colon G(\overline{k}) \to \pi_0^{\mathrm{geom}}(G)$ is surjective and has $G^0(\overline{k})$ as its kernel. As $G^0(\overline{k})$ is normal in $G(\overline{k})$, the set $\pi_0^{\mathrm{geom}}(G)$ inherits a group structure such that q^{geom} is a homomorphism. It is clear from the construction that $\mathrm{Aut}(\overline{k}/k)$ acts on $\pi_0^{\mathrm{geom}}(G)$ through group automorphisms. On the other hand, this action factors through $\mathrm{Aut}(\overline{k}/k) \twoheadrightarrow \mathrm{Gal}(k_s/k) =: \Gamma_k$; hence we find that Γ_k acts on $\pi_0^{\mathrm{geom}}(G)$ through group automorphisms.

We can view $\varpi_0^{\mathrm{geom}}(G)$ as the constant group scheme associated to the abstract group $\pi_0^{\mathrm{geom}}(G)$, and because Γ_k acts on $\pi_0^{\mathrm{geom}}(G)$ through group automorphisms, the étale scheme $\varpi_0(G)$ over k inherits the structure of a k-group scheme. It is clear from the constructions that $q^{\mathrm{geom}}\colon G_{k_s} \to \varpi_0^{\mathrm{geom}}(G)$ is a Γ_k-equivariant homomorphism of group schemes. It follows that $q\colon G \to \varpi_0(G)$ is a homomorphism of k-group schemes.

The conclusion of this discussion is that $\varpi_0(G)$ has a natural structure of an étale group scheme over k, and that $q\colon G \to \varpi_0(G)$ is a homomorphism. We refer to $\varpi_0(G)$ as the component group scheme of G.

Another way to show that $\varpi_0(G)$, for G a k-group scheme, inherits the structure of a group scheme is to use the fact that $\varpi_0(G \times_k G) \cong \varpi_0(G) \times_k \varpi_0(G)$; see Exercise 3.10. The group law on $\varpi_0(G)$ is the map

$$\varpi_0(m)\colon \varpi_0(G \times_k G) \cong \varpi_0(G) \times_k \varpi_0(G) \longrightarrow \varpi_0(G)$$

induced by the group law $m\colon G \times_k G \to G$.

Exercises.

Ex:SGrSch **(3.1)** Show that the following definition is equivalent to the one given in (3.7): If G is a group scheme over a basis S then a subgroup scheme of G is a subscheme $H \subset G$ such that (a) the identity section $e\colon S \to G$ factors through H; (b) if $j\colon H \hookrightarrow G$ is the inclusion morphism then the composition $i \circ j\colon H \hookrightarrow G \to G$ factors through H; (c) the composition $m \circ (j \times j)\colon H \times_S H \to G \times_S G \to G$ factors through H.

Ex:Gred **(3.2)**

(i) Let G be a group scheme over a perfect field k. Prove that the reduced underlying scheme $G_{\mathrm{red}} \hookrightarrow G$ is a closed subgroup scheme. [*Hint:* you will need the fact that $G_{\mathrm{red}} \times_k G_{\mathrm{red}}$ is again a reduced scheme; see EGA IV, § 4.6. This is where we need the assumption that k is perfect.]

(ii) Show, by means of an example, that G_{red} is in general not normal in G.

(iii) Let k be a field of characteristic p. Let $a \in k$, and set $G := \operatorname{Spec}\big(k[x]/(x^{p^2} + ax^p)\big)$. Show that G is a subgroup scheme of $\mathbb{G}_{a,k} = \operatorname{Spec}\big(k[x]\big)$.

(iv) Assume that k is not perfect and that $a \in k \setminus k^p$. Show that $|G|$, the topological space underlying G, consists of p closed points, say $|G| = \{Q_1, Q_2, \dots, Q_p\}$, where $Q_1 = e$ is the origin. Show that G is reduced at the points Q_i for $i = 2, \dots, p$ but not geometrically reduced. Finally show that the reduced underlying subscheme $G_{\mathrm{red}} \hookrightarrow G$ is not a subgroup scheme.

Ex:comcoi **(3.3)** Prove the relations (1) and (2) in (3.9). Also prove relation (6) in the proof of Theorem (3.20).

Ex:Te(m) **(3.4)** Let G be a group scheme over a field k. Write $T_{G,e} = \operatorname{Ker}\big(G(k[\varepsilon]) \to G(k)\big)$ for the tangent space of G at the identity element. Show that the map $T_e(m)\colon T_{G,e} \times T_{G,e} \to T_{G,e}$ induced by the group law $m\colon G \times_k G \to G$ on tangent spaces (the "derivative of m at e") is given by $T_e(m)(a,b) = a + b$. Generalize this to group schemes over an arbitrary base.

Ex:Frobetale **(3.5)** Let k be a field.

(i) If $f\colon G_1 \to G_2$ is a homomorphism of k-group schemes, show that

$$T_{\operatorname{Ker}(f),e} \cong \operatorname{Ker}\big(T_e(f)\colon T_{G_1,e} \to T_{G_2,e}\big)\,.$$

(ii) If $\operatorname{char}(k) = p > 0$, write $G[F] \subset G$ for the kernel of the relative Frobenius homomorphism $F_{G/k}\colon G \to G^{(p)}$. Show that $T_{G[F],e} \cong T_{G,e}$.

(iii) If G is a finite k-group scheme and $\operatorname{char}(k) = p$, show that G is étale over k if and only if $F_{G/k}$ is an isomorphism. [*Hint:* in the "only if" direction, reduce to the case that $k = \overline{k}$.]

Ex:LinGS **(3.6)** Let $S = \operatorname{Spec}(R)$ be an affine base scheme. Let $G = \operatorname{Spec}(A)$ be an affine S-group scheme such that A is free of finite rank as an R-module. Choose an R-basis $e_1, \dots, e_d$ for A, and define elements $a_{ij} \in A$ by $\tilde{m}(e_j) = \sum_{i=1}^{d} e_i \otimes a_{ij}$. Let $R[T_{ij}, U]/(\det \cdot U - 1)$ be the affine algebra of $\mathrm{GL}_{d,R}$, where $\det \in k[T_{ij}]$ is the determinant of the matrix $\big(T_{ij}\big)$. Show that there is a well-defined homomorphism of R-algebras

$$\varphi\colon R[T_{ij}, U]/(\det \cdot U - 1) \longrightarrow A$$

with $T_{ij} \mapsto a_{ij}$. Show that the corresponding morphism $G \to \mathrm{GL}_{d,R}$ is a homomorphism and gives an isomorphism of G with a closed subgroup scheme of $\mathrm{GL}_{d,R}$. [*Hint:* write $M_{d,R}$ for the ring scheme over R of $d \times d$ matrices. First show that we get a morphism $f\colon G \to M_{d,R}$ such that $f(g_1 g_2) = f(g_1) f(g_2)$ for all g_1, $g_2 \in G$. Next show that $f(e_G)$ is the identity matrix, and conclude that f factors through the open subscheme $\mathrm{GL}_{d,R} \subset M_{d,R}$. Finally show that φ is surjective. Use the relations between $\tilde{m}$, $\tilde{e}$ and $\tilde{\imath}$.]

Ex:[p]Augm **(3.7)** Let k be a field of characteristic p. Consider the group variety $G := \mathrm{GL}_{d,k}$. Let $A = \operatorname{Spec}\big(k[T_{ij}, U]/(\det \cdot U - 1)\big)$ be its affine algebra. Recall that we write $[n]_G\colon G \to G$ for the morphism given on points by $g \mapsto g^n$.

(i) Let $I \subset A$ be the augmentation ideal. Let $[p]\colon A \to A$ be the homomorphism of k-algebras corresponding to $[p]_G$. Show that $[p](I) \subseteq I^p$.

(ii) Let $H = \operatorname{Spec}(B)$ be a finite k-group scheme. Let $J \subset B$ be the augmentation ideal. Show that $[p](J) \subseteq J^p$. [*Hint:* use the previous exercise.] For an application of this result, see Exercise (4.4).

Ex:CDHopf **(3.8)** Let $\pi\colon G \to S$ be an affine S-group scheme. Set $A := \pi_* O_G$, so that $G \cong \mathrm{Spec}(A)$ as an S-scheme. Let $A^D := \mathit{Hom}_{O_S}(A, O_S)$. Show that with the definitions given in (3.21), A^D is a sheaf of co-commutative O_S-Hopf algebras.

Ex:GalDesc **(3.9)** Let k be a field, $k \subset k_s$ a separable algebraic closure, and write $\Gamma := \mathrm{Gal}(k_s/k)$. Let X be a scheme, locally of finite type over k, and let Y be an étale k-scheme. Note that Γ naturally acts on the schemes X_{k_s} and Y_{k_s}. If $\varphi\colon X_{k_s} \to Y_{k_s}$ is a Γ-equivariant morphism of schemes over k_s, show that φ is defined over k, i.e., there is a (unique) morphism $f\colon X \to Y$ over k such that $f_{k_s} = \varphi$. [*Hint:* First reduce to the case that X is affine and that X and Y are connected. Then work on rings.]

Ex:pi0XxY **(3.10)** Let X and Y be two schemes that are locally of finite type over a field k. Let $q_X\colon X \to \varpi_0(X)$ and $q_Y\colon Y \to \varpi_0(Y)$ be the morphisms as in Prop. (3.27). By the universal property of $\varpi_0(X \times_k Y)$, there is a unique morphism

$$\rho\colon \varpi_0(X \times_k Y) \to \varpi_0(X) \times_k \varpi_0(Y)$$

such that $\rho \circ q_{(X\times Y)} = (q_X \circ \mathrm{pr}_X, q_Y \circ \mathrm{pr}_Y)$. Show that ρ is an isomorphism. In particular, conclude that if $k \subset K$ is a field extension then $\varpi_0(X_K)$ is naturally isomorphic to $\varpi_0(X)_K$. [*Hint:* Reduce to the case $k = k_s$. Use that if C and D are connected schemes over k_s then $C \times_{k_s} D$ is again connected. See EGA IV, Cor. (4.5.8), taking into account loc. cit., Prop. (4.5.21).]

Notes. Proposition (3.17) is taken from SGA 3, Exp. $\mathrm{VI_A}$. The example following Proposition (3.12) is taken from ibid., Exp. $\mathrm{VI_B}$, §5. A different proof of Prop. (3.27) can be found in the book of Demazure and Gabriel [1].

When we work with group schemes the question naturally arises if constructions from group theory can also be carried out in the context of group schemes. For instance, we have seen that if $f\colon G \to G'$ is a homomorphism then we can form the kernel group scheme, $\mathrm{Ker}(f)$. In this example the geometry and the group theory go hand in hand: there is an obvious scheme-theoretic candidate for the kernel, namely the inverse image of the identity section of G', and this candidate also represents the kernel as a functor.

The present chapter is devoted to the formation of quotients, which is more delicate. (Nog aanvullen)

The reader who wants to go on as quickly as possible with the general theory of abelian varieties, may skip most of this chapter. The only results that are directly relevant for the next chapters are the formation of quotients modulo finite group schemes, Thm. (4.16), Example (4.40), and the material in § 4.

§1. *Categorical quotients.*

GrActionDef **(4.1) Definition.** (i) Let G be a group scheme over a basis S. A *(left) action of G on an S-scheme X* is given by a morphism $\rho\colon G \times_S X \to X$ such that the composition

$$X \xrightarrow{\sim} S \times_S X \xrightarrow{e_G \times \mathrm{id}_X} G \times_S X \xrightarrow{\rho} X$$

is the identity on X, and such that the diagram

$$\begin{array}{ccc} G \times_S G \times_S X & \xrightarrow{\mathrm{id}_G \times \rho} & G \times_S X \\ {\scriptstyle m \times \mathrm{id}_X}\downarrow & & \downarrow{\scriptstyle \rho} \\ G \times_S X & \xrightarrow{\rho} & X \end{array} \qquad (1)$$

Quot:rhoDiag

is commutative. In other words: for every S-scheme T, the morphism ρ induces a left action of the group $G(T)$ on the set $X(T)$. We usually denote this action on points by $(g, x) \mapsto g \cdot x$.

(ii) Given an action ρ as in (i), we define the "graph morphism"

$$\Psi = \Psi_\rho := (\rho, \mathrm{pr}_2)\colon G \times_S X \longrightarrow X \times_S X\,;$$

on points this is given by $(g, x) \mapsto (g \cdot x, x)$. The action ρ is said to be *free*, or *set-theoretically free* if Ψ is a monomorphism of schemes, and is said to be *strictly free*, or *scheme-theoretically free*, if Ψ is an immersion.

(iii) If T is an S-scheme and $x \in X(T)$ then the *stabilizer of x*, notation G_x, is the subgroup scheme of G_T that represents the functor $T' \mapsto \{g \in G(T') \mid g \cdot x = x\}$ on T-schemes T'. (See also (4.2), (iii) below.)

GrActRem **(4.2) Remarks.** (i) In some literature the same terminology is used in a slightly different meaning (cf. GIT, for example).

(ii) The condition that an action ρ is free means precisely that for all T and all $x \in X(T)$ the stabilizer G_x is trivial.

(iii) With notations as in the definition, we have a diagram with cartesian squares

$$\begin{array}{ccccc} G_x & \hookrightarrow & G_T = G \times_S T & \xrightarrow{\mathrm{id}_G \times x} & G \times_S X \\ \downarrow & & \downarrow{\scriptstyle a_x} & & \downarrow{\scriptstyle \Psi} \\ T & \xrightarrow{(x,\mathrm{id}_T)} & X_T = X \times_S T & \xrightarrow{\mathrm{id}_X \times x} & X \times_S X \end{array} ,$$

where the morphism a_x is given by $a_x = (\rho \circ (\mathrm{id}_G \times x), \mathrm{pr}_2)$; on points: $a_x(g) = g \cdot x$. That the functor $T' \mapsto \{g \in G(T') \mid g \cdot x = x\}$ is indeed representable by a subgroup scheme $G_x \subset G_T$ is seen from this diagram, arguing as in (3.13).

GrActExa **(4.3) Examples.** If G is a group scheme over S and $H \subset G$ is a subgroup scheme then the group law gives an action of H on G. The graph morphism $\Psi\colon H \times_S G \to G \times_S G$ is the restriction to $H \times_S G$ of the universal right translation $\tau\colon G \times_S G \to G \times_S G$. Since τ is an isomorphism, the action is strictly free.

More generally, if $f\colon G \to G'$ is a homomorphism of group schemes then we get a natural action of G on G', given on points by $(g, g') \mapsto f(g) \cdot g'$. The action is free if and only if $\mathrm{Ker}(f)$ is trivial, but if this holds the action need not be strictly free. For instance, with $S = \mathrm{Spec}(\mathbb{Q})$ as a base scheme, take $G = \mathbb{Z}_S$ to be the constant group scheme defined by the (abstract) group $\mathbb{Z}$, and take $G' = \mathbb{G}_{a,S}$. We have a natural homomorphism $f\colon \mathbb{Z}_S \to \mathbb{G}_{a,S}$ which, for $\mathbb{Q}$-schemes T, is given on points by the natural inclusion $\mathbb{Z} \hookrightarrow \Gamma(T, O_T)$. This homomorphism f is injective, hence it gives a free action of $\mathbb{Z}_S$ on $\mathbb{G}_{a,S}$. The graph morphism can be described as the morphism

$$\Psi\colon \coprod_{n \in \mathbb{Z}} \mathbb{A}^1 \longrightarrow \mathbb{A}^2$$

that maps the nth copy of $\mathbb{A}^1$ to the line $L \subset \mathbb{A}^2$ given by $x - y = n$. But this Ψ is not an immersion (the image is not a subscheme of $\mathbb{A}^2$), so the action is not strictly free.

Quot1stExa **(4.4)** The central issue of this chapter is the following question. *Given a group scheme G acting on a scheme X, does there exist a good notion of a quotient space $G\backslash X$?* As particular instances of this question we have: *given a homomorphism of group schemes $f\colon G \to G'$, can we form a cokernel of f?*, and *if $N \subset G$ is a normal subgroup scheme, can we define a quotient group scheme G/N?*

Let us first look at an elementary example. Take an integer $N \geqslant 2$, and consider the endomorphism $f\colon \mathbb{G}_m \to \mathbb{G}_m$ over $S = \mathrm{Spec}(\mathbb{Z})$ given on points by $q \mapsto q^N$. The kernel of f is μ_N, by definition of the latter. As a morphism of schemes, f is faithfully flat, and if k is any algebraically closed field then f is surjective on k-valued points. Therefore we would expect that the cokernel of f is trivial, i.e., $\mathrm{Coker}(f) = S$. But clearly, the "cokernel functor" $C\colon T \mapsto \mathbb{G}_m(T)/f(\mathbb{G}_m(T))$ is non-trivial. E.g., $C(\mathbb{Q})$ is an infinite group. Moreover, from the fact that $C(\mathbb{Q}) \neq \{1\}$ but $C(\overline{\mathbb{Q}}) = \{1\}$ it follows that C is not representable by a scheme. So, in contrast with (3.13) where we defined kernels, the geometric and the functorial point of view do not give to the same notion of a cokernel.

The first notion of a quotient that we shall define is that of a categorical quotient. Though we are mainly interested in working with schemes, it is useful to extend the discussion to a more general setting.

CatQuotDef **(4.5) Definition.** Let C be a category with finite products. Let G be a group object in C. Let X be an object of C. Throughout, we simply write $X(T)$ for $h_X(T) = \mathrm{Hom}_C(T, X)$.

(i) A *(left) action* of G on X is a morphism $\rho\colon G \times X \to X$ that induces, for every object T, a (left) action of the group $G(T)$ on the set $X(T)$.

(ii) Let an action of G on X be given. A morphism $q\colon X \to Y$ in C is said to be *G-invariant* if $q \circ \rho = q \circ \mathrm{pr}_X\colon G \times X \to Y$. By the Yoneda lemma this is equivalent to the requirement that for every $T \in C$, if x_1, $x_2 \in X(T)$ are two points in the same $G(T)$-orbit then $q(x_1) = q(x_2)$ in $Y(T)$.

(iii) Let $f, g\colon W \rightrightarrows X$ be two morphisms in C. We say that a morphism $h\colon X \to Y$ is a *difference cokernel* of the pair (f, g) if $h \circ f = h \circ g$ and if h is universal for this property; by this we mean that for any other morphism $h'\colon X \to Y'$ with $h' \circ f = h' \circ g$ there is a unique $\alpha\colon Y \to Y'$ such that $h' = \alpha \circ h$.

(iv) Let $\rho\colon G \times X \to X$ be a left action. A morphism $q\colon X \to Y$ is called a *categorical quotient* of X by G if q is a difference cokernel for the pair $(\rho, \mathrm{pr}_X)\colon G \times X \rightrightarrows X$. In other words, q is a categorical quotient if q is G-invariant and if every G-invariant morphism $q'\colon X \to Y'$ factors as $q' = \alpha \circ q$ for a unique $\alpha\colon Y \to Y'$. The morphism $q\colon X \to Y$ is called a *universal categorical quotient* of X by G if for every object S of C the morphism $q_S\colon X_S \to Y_S$ is a categorical quotient of X_S by G_S in the category $C_{/S}$.

In practice the morphism q is often not mentioned, and we simply say that an object Y is the categorical quotient of X by G. Note that if a categorical quotient $q\colon X \to Y$ exists then it is unique up to unique isomorphism.

Quo1ExaBis **(4.6) Examples.** As in (4.4), let $S = \mathrm{Spec}(\mathbb{Z})$ and let $G = \mathbb{G}_{m,S}$ act on $X = \mathbb{G}_{m,S}$ by $\rho(g, x) = g^N \cdot x$. If $k = \overline{k}$ then $X(k)$ consists of a single orbit under $G(k)$; this readily implies that $X \to S$ is a categorical quotient of X by G. In fact, if we work a little harder we find that $X \to S$ is even a universal categorical quotient; see Exercise (4.1).

As a second example, let $k = \overline{k}$ and consider the action of $G = \mathbb{G}_{m,k}$ on $X = \mathbb{A}^1_k$ given on points by $\rho(g, x) = g \cdot x$. There are two orbits in $X(k)$, one given by the origin $0 \in X(k)$, the other consisting of all points $x \neq 0$. Suppose we have a G-invariant morphism $q\colon X \to Y$ for some k-scheme Y. It maps $X(k) \setminus \{0\}$ to a point $y \in Y(k)$. Because $X(k) \setminus \{0\}$ is Zariski dense in X we find that q is the constant map with value y. This proves that the structural morphism $X \to \mathrm{Spec}(k)$ is a categorical quotient of X by G. We conclude that it is not possible to construct a quotient scheme Y such that the two orbits $\{0\}$ and $\mathbb{A}^1 \setminus \{0\}$ are mapped to different points of Y.

Quot/YRem **(4.7) Remark.** Let G be an S-group scheme acting on an S-scheme X. Suppose there exists a categorical quotient $q\colon X \to Y$ in $\mathsf{Sch}_{/S}$. To study q we can take Y to be our base scheme. More precisely, $G_Y := G \times_S Y$ acts on X over Y and q is also a categorical quotient of X by G_Y in the category $\mathsf{Sch}_{/Y}$. Taking Y to be the base scheme does not affect the (strict) freeness of the action. To see this, note that the graph morphism $\Psi\colon G \times_S X \to X \times_S X$ factors through the subscheme $X \times_Y X \hookrightarrow X \times_S X$ and that the resulting morphism

$$G_Y \times_Y X = G \times_S X \to X \times_Y X$$

is none other than the graph morphism of G_Y acting on X over Y. Hence the action of G on X over S is (strictly) free if and only if the action of G_Y on X over Y is (strictly) free.

§2. *Geometric quotients, and quotients by finite group schemes.*

We first give, in its simplest form, a result about the existence of quotients under finite groups. This result will be generalized in (4.16) below. Here we consider an action of an abstract group Γ on a scheme X; this means that for every element $\gamma \in \Gamma$ we have a morphism $\rho(\gamma)\colon X \to X$, satisfying the usual axioms for a group action. Such an action is the same as an action of the constant group scheme Γ on X; hence we are in a special case of the situation considered in (4.1).

QuotFinGr **(4.8) Proposition.** *Let Γ be a finite (abstract) group acting on an affine scheme $X = \mathrm{Spec}(A)$. Let $B := A^\Gamma \subseteq A$ be the subring of Γ-invariant elements, and set $Y := \mathrm{Spec}(B)$.*

(i) *The natural morphism $q\colon X \to Y$ induces a homeomorphism $\Gamma\backslash|X| \xrightarrow{\sim} |Y|$, i.e., it identifies the topological space $|Y|$ with the quotient of $|X|$ under the acion of Γ.*

(ii) *The map $q^\sharp\colon O_Y \to q_*O_X$ induces an isomorphism $O_Y \xrightarrow{\sim} (q_*O_X)^\Gamma$, where the latter denotes the sheaf of Γ-invariant sections of q_*O_X.*

(iii) *The ring A is integral over B; the morphism $q\colon X \to Y$ is quasi-finite, closed and surjective.*

Proof. Write $\Gamma = \{\gamma_1, \dots, \gamma_r\}$. Define the map $N\colon A \to A^\Gamma = B$ by

$$N(a) = \gamma_1(a) \cdots \gamma_r(a)\,.$$

If $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals of A which lie in the same Γ-orbit then $\mathfrak{p} \cap A^\Gamma = \mathfrak{p}' \cap A^\Gamma$. Conversely, if $\mathfrak{p} \cap A^\Gamma = \mathfrak{p}' \cap A^\Gamma$ then $N(x) \in \mathfrak{p}'$ for every $x \in \mathfrak{p}$, so $\mathfrak{p} \subset \gamma_1(\mathfrak{p}') \cup \cdots \cup \gamma_r(\mathfrak{p}')$. This implies (see Atiyah-Macdonald [1], Prop. 1.11) that $\mathfrak{p} \subseteq \gamma_i(\mathfrak{p}')$ for some i, and by symmetry we conclude that $\mathfrak{p}$ and $\mathfrak{p}'$ lie in the same Γ-orbit. Hence $\Gamma\backslash|X| \xrightarrow{\sim} |Y|$ as sets, and q is quasi-finite.

For $a \in A$, let $\chi_a(T) := \big(T - \gamma_1(a)\big)\big(T - \gamma_2(a)\big) \cdots \big(T - \gamma_r(a)\big) \in A[T]$. Then it is clear that $\chi_a(T)$ is a monic polynomial in $B[T]$ and that $\chi_a(a) = 0$. This shows that A is integral over B. That the map q is closed and surjective then follows from Atiyah-Macdonald [1], Thm. 5.10; see also (4.21) below.

Finally we remark that for every $f \in A^\Gamma$ we have a natural isomorphism $(A^\Gamma)_f \xrightarrow{\sim} (A_f)^\Gamma$. As the special open subsets $D(f) := Y \setminus Z(f)$ form a basis for the topology on Y, property (ii) follows. □

QuotFinRem **(4.9) Remarks.** (i) The morphism $q\colon X \to Y$ need not be finite. It may happen that A is noetherian but that $B := A^\Gamma$ is not, and that A is not finitely generated as a B-module. Examples of this kind can be found in Nagata [1], ??. However, if either the action on Γ on X is free, or X is of finite type over a locally noetherian base scheme S and Γ acts by automorphisms of X over S, then q is a finite morphism. See (4.16) below.

(ii) It is not hard to show that $q\colon X \to Y$ is a categorical quotient of X by G. (See also Proposition (4.13) below.) More generally, if $X \to S$ is a morphism such that Γ acts by automorphisms of X over S then also Y has a natural structure of an S-scheme, and q is a categorical quotient in $\mathsf{Sch}_{/S}$. In general, q is not a universal categorical quotient. As an example, let k be a field of characteristic p, take $S = \mathrm{Spec}\,\big(k[\varepsilon]\big)$ and $X = \mathbb{A}^1_S = \mathrm{Spec}(A)$, with $A = k[x, \varepsilon]$. We let the group $\Gamma := \mathbb{Z}/p\mathbb{Z}$ act on X (over S); on rings we give the action of $n \bmod p$ by $x \mapsto x + n\varepsilon$ and $\varepsilon \mapsto \varepsilon$. The ring A^Γ of invariants is generated as a k-algebra by ε, $x\varepsilon, \dots, x^{p-1}\varepsilon$ and x^p. But on the special fibre $\mathbb{A}^1_k$ the action is trivial. As

$$A^\Gamma \otimes_{k[\varepsilon]} k = k[\varepsilon, x\varepsilon, \dots, x^{p-1}\varepsilon, x^p] \otimes_{k[\varepsilon]} k = k[x^p]$$

is a proper subring of

$$\big(A \otimes_{k[\varepsilon]} k\big)^{\Gamma} = k[x]\,,$$

we see that $Y := \operatorname{Spec}(A^{\Gamma})$ is not a universal categorical quotient of X in $\mathsf{Sch}_{/S}$.

GeomQuot **(4.10)** Suppose given an action of a group scheme G on a scheme X, over some basis S, say. We should like to decide if there exists a categorical quotient of X by G in $\mathsf{Sch}_{/S}$, and if yes then we should like to construct this quotient. Properties (a) and (b) in the above proposition point to a general construction. Namely, if $|X|$ is the topological space underlying X then we could try to form a quotient of $|X|$ modulo the action of G and equip this space with the sheaf of G-invariant functions on X.

Another way to phrase this is the following. The category of schemes is a full subcategory of the category LRS of locally ringed spaces, which in turn is a subcategory (not full) of the category RS of all ringed spaces. If G is an S-group scheme acting on an S-scheme X then we shall show that there exists a categorical quotient $(G\backslash X)_{\mathrm{rs}}$ in the category $\mathsf{RS}_{/S}$. It is constructed exactly as just described: form the quotient "$G\backslash|X|$" and equip this with the sheaf "$(q_*O_X)^G$", where $q\colon |X| \to G\backslash|X|$ is the natural map. Then the question is whether $(G\backslash X)_{\mathrm{rs}}$ is a scheme and, if so, if this scheme is a "good" scheme-theoretic quotient of X modulo G.

Before we give more details, let us note that in general $(G\backslash X)_{\mathrm{rs}}$ cannot be viewed as a categorical quotient in the sense of Definition (4.5). Namely, because $\mathsf{Sch}_{/S}$ is not a full subcategory of $\mathsf{RS}_{/S}$, products in the two categories may be different. Hence if G is an S-group scheme then it is not clear if the ringed space $\big(|G|, O_G\big)$ inherits the structure of a group object in $\mathsf{RS}_{/S}$. The assertion that $(G\backslash X)_{\mathrm{rs}}$ is a quotient of X by G will therefore be interpret as saying that the morphism q is a difference cokernel of the pair of morphisms $(\rho, \mathrm{pr}_X)\colon G \times_S X \rightrightarrows X$ in $\mathsf{RS}_{/S}$.

GQuotLem **(4.11) Lemma.** *Let $\rho\colon G \times_S X \to X$ be an action of an S-group scheme G on an S-scheme X. Consider the continuous maps*

$$|\mathrm{pr}_X|\colon |G \times_S X| \longrightarrow |X| \qquad \text{and} \qquad |\rho|\colon |G \times_S X| \longrightarrow |X|\,.$$

Given P, $Q \in |X|$, write $P \sim Q$ if there exists a point $R \in |G \times_S X|$ with $|\mathrm{pr}_X|(R) = P$ and $|\rho|(R) = Q$. Then $\sim$ is an equivalence relation on $|X|$.

Proof. See Exercise (4.2).

We refer to the equivalence classes under $\sim$ as the *G-equivalence classes in $|X|$*.

GXrsDef **(4.12) Definition.** Let $\rho\colon G \times_S X \to X$ be an action of an S-group scheme G on an S-scheme X. Let $|X|/\!\sim$ be the set of G-equivalence classes in $|X|$, equipped with the quotient topology. Write $q\colon |X| \to |X|/\!\sim$ for the canonical map. Let $U = q^{-1}(V)$ for some open subset $V \subset |X|/\!\sim$. If $f \in q_*O_X(V) = O_X(U)$ then we can form the elements $\mathrm{pr}_X^\sharp(f)$ and $\rho^\sharp(f)$ in $O_{G\times_S X}(G \times_S U)$. We say that f is G-invariant if $\mathrm{pr}_X^\sharp(f) = \rho^\sharp(f)$. The G-invariant functions f form a subsheaf of rings $(q_*O_X)^G \subset q_*O_X$.

We define

$$(G\backslash X)_{\mathrm{rs}} := \big(|X|/\!\sim, (q_*O_X)^G\big)\,,$$

and write $q\colon X \to (G\backslash X)_{\mathrm{rs}}$ for the natural morphism of ringed spaces.

If $(G\backslash X)_{\mathrm{rs}}$ is a scheme and q is a morphism of schemes then we say that it is a *geometric quotient* of X by G. If moreover for every S-scheme T we have that $(G\backslash X)_{\mathrm{rs}} \times_S T \cong (G_T\backslash X_T)_{\mathrm{rs}}$ then we say that $(G\backslash X)_{\mathrm{rs}}$ is a *universal geometric quotient*.

The phrase "if a geometric quotient of X by G exists" is used as a synonym for "if $(G\backslash X)_{\mathrm{rs}}$ is a scheme and $q\colon X \to (G\backslash X)_{\mathrm{rs}}$ is a morphism of schemes".

The stalks of the sheaf $(q_*O_X)^G$ may not be local rings; for an example see ??. This is the reason why we work in the category of ringed spaces rather than the category of locally ringed spaces. Further we note that the formation of $(G\backslash X)_{\mathrm{rs}}$ does not, in general, commute with base change; see (ii) of (4.9). However, if $U \subset S$ is a Zariski open subset then $(G_U\backslash X_U)_{\mathrm{rs}}$ is canonically isomorphic to the restriction of $(G\backslash X)_{\mathrm{rs}}$ to U.

GXrsProp **(4.13) Proposition.** *In the situation of* (4.12), $q\colon X \to (G\backslash X)_{\mathrm{rs}}$ *is a difference cokernel of the pair of morphisms* $(\rho, \mathrm{pr}_X)\colon G \times_S X \rightrightarrows X$ *in the category* $\mathsf{RS}_{/S}$. *By consequence, if a geometric quotient of* X *by* G *exists then it is also a categorical quotient in* $\mathsf{Sch}_{/S}$.

Proof. The first assertion is an immediate consequence of how we constructed $(G\backslash X)_{\mathrm{rs}}$. If $(G\backslash X)_{\mathrm{rs}}$ is a geometric quotient then it is also a difference cokernel of (ρ, pr_X) in the category $\mathsf{Sch}_{/S}$ because the latter is a subcategory of $\mathsf{RS}_{/S}$. This gives the second assertion. □

TrDetExa **(4.14) Example.** Let k be a field, and consider the k-scheme $\mathrm{M}_{2,k}$ $(=\mathbb{A}^4_k)$ of 2×2-matrices over k. The linear algebraic group $\mathrm{GL}_{2,k}$ acts on $\mathrm{M}_{2,k}$ by conjugation: if $g \in \mathrm{GL}_2(T)$ for some k-scheme T then g acts on $\mathrm{M}_2(T)$ by $A \mapsto g \cdot A \cdot g^{-1}$. Write $\rho\colon \mathrm{GL}_{2,k} \times \mathrm{M}_{2,k} \to \mathrm{M}_{2,k}$ for the morphism giving this $\mathrm{GL}_{2,k}$-action.

The trace and determinant give morphisms of schemes trace: $\mathrm{M}_{2,k} \to \mathbb{A}^1_k$ and det: $\mathrm{M}_{2,k} \to \mathbb{A}^1_k$. Now consider the morphism

$$p = (\mathrm{trace}, \det)\colon \mathrm{M}_{2,k} \to \mathbb{A}^2_k\,.$$

Clearly p is a GL_2-invariant morphism, i.e., $p \circ \mathrm{pr}_2\colon \mathrm{GL}_{2,k} \times \mathrm{M}_{2,k} \to \mathrm{M}_{2,k} \to \mathbb{A}^2_k$ is the same as $p \circ \rho$. It can be shown that the pair $(\mathbb{A}^2_k, p)$ is a (universal) categorical quotient of $\mathrm{M}_{2,k}$ by $\mathrm{GL}_{2,k}$, see GIT, Chap. 1, § 2 and Appendix 1C.

On the other hand, it is quite easy to see that $\mathbb{A}^2_k$ is not a geometric quotient. Indeed, if this were the case then on underlying topological spaces the map p should identify $\mathbb{A}^2_k$ as the set of $\mathrm{GL}_{2,k}$-orbits in $\mathrm{M}_{2,k}$. But the trace and the determinant are not able to distinguish a matrix

$$J_\lambda := \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

from its semi-simple part

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

To give another explanation of what is going on, let us look at $\overline{k}$-valued points, where $\overline{k}$ is an algebraic closure of k. The theory of Jordan canonical forms tells us that the $\mathrm{GL}_2(\overline{k})$-orbits in $\mathrm{M}_2(\overline{k})$ are represented by the diagonal matrices $\mathrm{diag}(\lambda_1, \lambda_2)$ together with the matrices J_λ. For $\tau, \delta \in \overline{k}$, write $N(\tau, \delta) \subset \mathrm{M}_{2,\overline{k}}$ for the 2-dimensional subvariety given by the conditions trace $= \tau$ and $\det = \delta$. By direct computation one readily verifies that (i) the orbit of a diagonal matrix $A = \mathrm{diag}(\lambda, \lambda)$ is the single closed point A; (ii) the orbit of a diagonal matrix $\mathrm{diag}(\lambda_1, \lambda_2)$ with $\lambda_1 \neq \lambda_2$ equals $N(\lambda_1 + \lambda_2, \lambda_1\lambda_2)$; (iii) the orbit of a matrix J_λ equals $N(2\lambda, \lambda^2) \setminus \{\mathrm{diag}(\lambda, \lambda)\}$; in particular, this orbit is not closed in $\mathrm{M}_{2,\overline{k}}$.

From the observation that there are non-closed orbits in $\mathrm{M}_{2,\overline{k}}$, it immediately follows that there does not exist a geometric quotient. (Indeed, the orbits in $\mathrm{M}_2(\overline{k})$ would be the pre-images of the $\overline{k}$-valued points of the geometric quotient. Cf. the second example in (4.6).) This

suggests that the points in a subvariety of the form $N(2\lambda, \lambda^2) \subset \mathrm{M}_{2,k}$ are the "bad" points for the given action of GL_2. Indeed, it can be shown that on the open complement $U \subset \mathrm{M}_{2,k}$ given by the condition $4\det - \mathrm{trace}^2 \neq 0$, the map $p = (\mathrm{trace}, \det)\colon U \to D(4y - x^2) \subset \mathbb{A}^2$ (taking coordinates x, y on $\mathbb{A}^2$ and writing $D(f)$ for the locus where a function f does not vanish) makes $D(4y - x^2) \subset \mathbb{A}^2_k$ a geometric quotient of U.

The notion of a geometric quotient plays a central role in geometric invariant theory. There, as in the above simple example, one studies which points, or which orbits under a given group action are so "unstable" that they obstruct the formation of a good quotient. (Which are the "bad" points may depend on further data, such as the choice of an ample line bundle on the scheme in question.) We refer the reader to the book GIT.

We now turn to the promised generalization of Proposition (4.8). First we need a lemma.

NormLem **(4.15) Lemma.** *Let $\varphi\colon A \to C$ be a homomorphism of commutative rings that makes C a projective A-module of rank $r > 0$. Let $\mathrm{Norm}_{C/A}\colon C \to A$ be the norm map. Let $\psi\colon \mathrm{Spec}(C) \to \mathrm{Spec}(A)$ be the morphism of affine schemes given by φ. If $Z \subset \mathrm{Spec}(C)$ is the zero locus of $f \in C$ then $\psi(Z) \subset \mathrm{Spec}(A)$ is the zero locus of $\mathrm{Norm}_{C/A}(f)$.*

Proof. The assumptions imply that φ is injective. As C is integral over A the map ψ is surjective; see also (4.21) below. Let $\mathfrak{p} \in \mathrm{Spec}(A)$; write $\psi^{-1}\{\mathfrak{p}\} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$. By definition, $N := \mathrm{Norm}_{C/A}(f)$ is the determinant of the endomorphism $\lambda_f\colon c \mapsto fc$ of C as a module over A.

Write $W \subset \mathrm{Spec}(A)$ for the zero locus of N. Write $a_{\mathfrak{p}}$ for the image of an element $a \in A$ in $A_{\mathfrak{p}}$; similar notation for elements of C. Then we have

$$\begin{aligned}
\mathfrak{p} \notin W &\iff N_{\mathfrak{p}} \in A^*_{\mathfrak{p}} \\
&\iff \lambda_{f,\mathfrak{p}}\colon C_{\mathfrak{p}} \to C_{\mathfrak{p}} \text{ is an isomorphism} \\
&\iff f_{\mathfrak{p}} \in C^*_{\mathfrak{p}} \\
&\iff f \notin \mathfrak{q}_i \text{ for all } i = 1, \dots, n \\
&\iff \mathfrak{q}_i \notin Z \text{ for all } i = 1, \dots, n\,,
\end{aligned}$$

which proves the lemma. □

QuotFinGS **(4.16) Theorem.** (Quotients by finite group schemes.) *Let G be a finite locally free S-group scheme acting on an S-scheme X. Assume that for every closed point $P \in |X|$ the G-equivalence class of P is contained in an affine open subset.*

(i) *The quotient $Y := (G\backslash X)_{\mathrm{rs}}$ is an S-scheme, which therefore is a geometric quotient of X by G. The canonical morphism $q\colon X \to Y$ is quasi-finite, integral, closed and surjective. If S is locally noetherian and X is of finite type over S then q is a finite morphism and Y is of finite type over S, too.*

(ii) *The formation of the quotient Y is compatible with* flat *base change (terminology: Y is a uniform quotient). In other words, let $h\colon S' \to S$ be a flat morphism. Let a prime $'$ denote a base change via h, e.g., $X' := X \times_S S'$. Then $Y' \cong (G'\backslash X')_{\mathrm{rs}}$.*

(iii) *If G acts freely then $q\colon X \to Y$ is finite locally free and the morphism*

$$G \times_S X \longrightarrow X \times_Y X$$

induced by $\Psi = (\rho, \mathrm{pr}_X)$ is an isomorphism. Moreover, Y is in this case a universal geometric quotient: for any morphism $h\colon S' \to S$, indicating base change via h by a prime $'$, we have $Y' \cong (G'\backslash X')_{\mathrm{rs}}$.

QFGSRem **(4.17) Remarks.** (i) The condition that every G-equivalence class is contained in an affine open subset is satisfied if X is quasi-projective over S. Indeed, given a ring R, a positive integer N, and a finite set V of closed points of $\mathbb{P}^N_R$, we can find an affine open subscheme $U \subset \mathbb{P}^N_R$ such that $V \subset U$.

(ii) In the situation of the theorem we find that a free action is automatically strictly free. Indeed, by (iii) the graph morphism Ψ gives an isomorphism of $G \times_S X$ with the subscheme $X \times_Y X \subset X \times_S X$; hence Ψ is an immersion.

We break up the proof of the theorem into a couple of steps, (4.18)–(4.26).

QFGSStep1 **(4.18)** *Reduction to the case that S is affine.* Suppose $S = \cup_\alpha U_\alpha$ is a covering of S by Zariski open subsets. As remarked earlier, the restriction of $(G\backslash X)_{\mathrm{rs}}$ to $U = U_\alpha$ is naturally isomorphic to $(G_U\backslash X_U)_{\mathrm{rs}}$. If we can prove the theorem over each of the open sets U_α then the result as stated easily follows by gluing. In the rest of the proof we may therefore assume that $S = \mathrm{Spec}(Q)$ is affine and that the affine algebra R of G is free of some rank r as a Q-module.

QFGSStep2 **(4.19)** *Reduction to the case that X is affine.* If $P \in |X|$, let us write $G(P)$ for its G-equivalence class; note that this is a finite set. Note further that

$$G(P) = \rho\big(\mathrm{pr}_X^{-1}\{P\}\big) = \mathrm{pr}_X\big(\rho^{-1}\{P\}\big)\,,$$

by definition of G-equivalence. (Strictly speaking we should write $|\rho|$ and $|\mathrm{pr}_X|$.)

Say that a subset $V \subset |X|$ is G-stable if it contains $G(P)$ whenever it contains P. If V is open then there is a maximal open subset $V' \subseteq V$ which is G-stable. Namely, if $Z := |X| \setminus V$ then $Z' := \mathrm{pr}_X\big(\rho^{-1}\{Z\}\big)$ is closed (since $\mathrm{pr}_X\colon G \times_S X \to X$ is proper), and $V' := |X| \setminus Z'$ has the required property.

We claim that X can be covered by G-stable affine open subsets. It suffices to show that every closed point $P \in X$ has a G-stable affine open neighbourhood. By assumption there exists an affine open $V \subset X$ with $G(P) \subset V$. Then also $G(P) \subset V'$. As $G(P)$ is finite there exists an $f \in \Gamma(V, O_V)$ such that, writing $D(f) \subset V$ for the open subset where f does not vanish, $G(P) \subset D(f) \subseteq V'$. In total this gives

$$G(P) \subset D(f)' \subseteq D(f) \subseteq V' \subseteq V\,.$$

Our claim is proven if we can show that $D(f)'$ is affine. Write f' for the image of f in $\Gamma(V', O_{V'})$, so that $Z := V' \setminus D(f)$ is the zero locus of f'. As V' is G-stable we have $\rho^{-1}(V') = G \times_S V'$, which gives an element $\rho^\sharp(f') \in \Gamma(G \times_S V', O_{G\times_S V'})$. The zero locus of $\rho^\sharp(f')$ is of course just $\rho^{-1}(Z) \subset G \times_S V'$. As G is finite locally free, the morphism pr_X makes $\Gamma\big(G \times_S V', O_{G\times_S V'}\big)$ into a projective module of finite rank over $\Gamma\big(V', O_{V'}\big)$. This gives us a norm map

$$\mathrm{Norm}\colon \Gamma\big(G \times_S V', O_{G\times_S V'}\big) \longrightarrow \Gamma\big(V', O_{V'}\big)\,.$$

Let $F := \mathrm{Norm}\big(\rho^\sharp(f')\big)$. By Lemma (4.15), the zero locus of F is the image of $\rho^{-1}(Z)$ under the projection to V'. But the complement of this locus in V' is precisely $D(f)'$. Hence if F' is the image of F in $\Gamma\big(D(f), O_{D(f)}\big)$ then $D(f)'$ is the open subset of $D(f)$ where F' does not vanish. As this subset is affine open, our claim is proven.

Except for the last assertion of (i), the proof of the theorem now reduces to the case that X is affine. Namely, by the previous we can cover X by G-stable affine open subsets, and if the

theorem is true for each of these then by gluing we obtain the result for X. The last assertion of (i) will be dealt with in (4.23).

QFGSStep3 **(4.20)** From now on we assume that $X = \mathrm{Spec}(A) \to S = \mathrm{Spec}(Q)$. Further we assume that $G = \mathrm{Spec}(R)$ for some Q-Hopf algebra R which is free of rank r as a module over Q. Much of what we are going to do is a direct generalization of the arguments in (4.8); that proof may therefore serve as a guide for the arguments to follow.

The action of G on X is given by a Q-algebra homomorphism $\sigma\colon A \to R \otimes_Q A$. Write $j\colon A \to R \otimes_Q A$ for the map given by $a \mapsto 1 \otimes a$. (In other words, we write σ for $\rho^\sharp$ and j for $\mathrm{pr}_X^\sharp$.) Define a subring $B := A^G \subset A$ of G-invariants by

$$B := \{a \in A \mid \sigma(a) = j(a)\}\,.$$

We are going to prove that $Y := \mathrm{Spec}(B)$ is the geometric quotient of X under the given action of G.

As a first step, let us show that A is integral over B. For $a \in A$, multiplication by $\sigma(a)$ is an endomorphism of $R \otimes_Q A$, and we can form its characteristic polynomial

$$\chi(t) = t^r + c_{r-1}t^{r-1} + \cdots + c_1 t + c_0 \in A[t]\,.$$

We have cartesian squares

$$\begin{array}{ccc} R \otimes_Q A & \xrightarrow{\tilde m \otimes \mathrm{id}_A} & R \otimes_Q R \otimes_Q A \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle j_{2,3}} \\ A & \xrightarrow{\ j\ } & R \otimes_Q A \end{array} \qquad \text{and} \qquad \begin{array}{ccc} R \otimes_Q A & \xrightarrow{\mathrm{id}_R \otimes \sigma} & R \otimes_Q R \otimes_Q A \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle j_{2,3}} \\ A & \xrightarrow{\ \sigma\ } & R \otimes_Q A\,, \end{array} \tag{2}$$

Quot:CartDiags

where the map $j_{2,3}$ is given by $r \otimes a \mapsto 1 \otimes r \otimes a$. We view $R \otimes_Q R \otimes_Q A$ as a module over $R \otimes_Q A$ via $j_{2,3}$. It follows from the left-hand diagram that $j\big(\chi(t)\big)$, the polynomial obtained from $\chi(t)$ by applying j to its coefficients, is the characteristic polynomial of $\tilde m \otimes \mathrm{id}_A\big(\sigma(a)\big)$. The right-hand diagram tells us that $\sigma\big(\chi(t)\big)$ is the characteristic polynomial of $\mathrm{id}_R \otimes \sigma\big(\sigma(a)\big)$. But the commutativity of diagram (1) in Definition (4.1) gives the identity $\tilde m \otimes \mathrm{id}_A\big(\sigma(a)\big) = \mathrm{id}_R \otimes \sigma\big(\sigma(a)\big)$. Hence $j\big(\chi(t)\big) = \sigma\big(\chi(t)\big)$, which means that $\chi(t)$ is a polynomial with coefficients c_i in the ring B of G-invariants.

The Cayley-Hamilton theorem tells us that

$$\sigma(a)^r + j(c_{r-1})\sigma(a)^{r-1} + \cdots + j(c_1)\sigma(a) + j(c_0) = 0\,.$$

As $j(c_i) = \sigma(c_i)$ for all i we can rewrite this as

$$\sigma\big(\chi(a)\big) = \sigma(a)^r + \sigma(c_{r-1})\sigma(a)^{r-1} + \cdots + \sigma(c_1)\sigma(a) + \sigma(c_0) = 0\,. \tag{3}$$

Quot:CayHam

But σ is an injective map, because we have the relation $(\tilde e \otimes \mathrm{id}_A) \circ \sigma = \mathrm{id}_A$, which translates the fact that the identity element of G acts as the identity on X. Hence (3) implies that $\chi(a) = 0$. This proves that A is integral over B.

QFGSStep4 **(4.21)** The fact that A is integral over B has the following consequences.

(i) If $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ are prime ideals of A with $\mathfrak{p}_1 \cap B = \mathfrak{p}_2 \cap B$ then $\mathfrak{p}_1 = \mathfrak{p}_2$. Geometrically this means that all fibres of $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ have dimension 0.

(ii) The natural map $q\colon X = \mathrm{Spec}(A) \to Y = \mathrm{Spec}(B)$ is surjective.

(iii) The map q is closed, i.e., if $C \subset X$ is closed then $q(C) \subset Y$ is closed too.

Properties (i) and (ii) can be found in many textbooks on commutative algebra, see for instance Atiyah-Macdonald [1], Cor. 5.9 and Thm. 5.10. For (iii), suppose $C \subset X$ is the closed subset defined by an ideal $\mathfrak{a} \subset A$. We may identify C with $\mathrm{Spec}(A/\mathfrak{a})$. The composite map $C = \mathrm{Spec}(A/\mathfrak{a}) \hookrightarrow \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ factors through the closed subset $\mathrm{Spec}(B/\mathfrak{b}) \subset \mathrm{Spec}(B)$, where $\mathfrak{b} = \mathfrak{a} \cap B$. Note that $A/\mathfrak{a}$ is again integral over its subring $B/\mathfrak{b}$. Applying (ii) with A and B replaced by $A/\mathfrak{a}$ and $B/\mathfrak{b}$, we find that $C = \mathrm{Spec}(A/\mathfrak{a}) \to \mathrm{Spec}(B/\mathfrak{b})$ is surjective. Hence $q(C)$ is the closed subset of B defined by $\mathfrak{b}$.

Define a map $N\colon A \to B$ by

$$N(a) = \mathrm{Norm}_{R\otimes_Q A/A}\big(\sigma(a)\big)\,.$$

Note that $N(a) = (-1)^n c_0$, where c_0 is the constant coefficient of the characteristic polynomial $\chi(t)$ considered in (4.20); hence $N(a)$ is indeed an element of B. The relation $\chi(a) = 0$ gives

$$N(a) = (-1)^{n+1} \cdot a \cdot \big(a^{n-1} + c_{n-1}a^{n-2} + \cdots + c_1\big)\,.$$

In particular, if $a \in \mathfrak{a}$ for some ideal $\mathfrak{a} \subset A$ then $N(a) \in \mathfrak{a} \cap B$.

QFGSStep5 **(4.22)** Recall that $Y := \mathrm{Spec}(B)$. We are going to prove that $Y = (G\backslash X)_{\mathrm{rs}}$. Note that the natural map $|X| \to |Y|$ is surjective, by (ii) in (4.21).

By definition, two prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ of A are in the same G-equivalence class if there exists a prime ideal $\mathfrak{Q}$ of $R \otimes_Q A$ with $\sigma^{-1}(\mathfrak{Q}) = \mathfrak{p}$ and $j^{-1}(\mathfrak{Q}) = \mathfrak{p}'$. If such a prime ideal $\mathfrak{Q}$ exists then it is immediate that $\mathfrak{p} \cap B = \mathfrak{p}' \cap B$, so G-equivalent points of X are mapped to the same point of Y.

Conversely, suppose $\mathfrak{p} \cap B = \mathfrak{p}' \cap B$. There are finitely many prime ideals $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n$ of $R\otimes_Q A$ with the property that $j^{-1}(\mathfrak{Q}_i) = \mathfrak{p}'$. (The morphism $\mathrm{pr}_X\colon G\times_S X \to X$ is finite because G is finite.) Set $\mathfrak{q}_i = \sigma^{-1}(\mathfrak{Q}_i)$. Note that $\mathfrak{q}_i \cap B = \mathfrak{p} \cap B$. Our goal is to prove that $\mathfrak{p} = \mathfrak{q}_i$ for some i. By property (i) above it suffices to show that $\mathfrak{p} \subseteq \mathfrak{q}_i$ for some i. Suppose this is not the case. Then there exists an element $a \in \mathfrak{p}$ that is not contained in $\mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n$. (Use Atiyah-Macdonald [1], Prop. 1.11, and cf. the proof of Prop. (4.8) above.) Lemma (4.15), applied with $f = \sigma(a) \in R\otimes_Q A$, tells us that the prime ideals of A containing $N(a)$ are all of the form $j^{-1}(\mathfrak{r})$ with $\mathfrak{r}$ a prime ideal of $R \otimes_Q A$ that contains $\sigma(a)$. But $a \in \mathfrak{p}$, hence $N(a) \in \mathfrak{p} \cap B = \mathfrak{p}' \cap B$. Hence one of the prime ideals $\mathfrak{Q}_i$ contains $\sigma(a)$, contradicting our choice of a.

We have now proven that the map $X \to Y$ identifies $|Y|$ with the set $|X|/\!\sim$ of G-equivalence classes in X. Further, by (iii) in (4.21) the quotient map $|X| \to |Y|$ is closed, so the topology on $|Y|$ is the quotient topology. If $V = D_Y(f) \subset Y$ is the fundamental open subset given by $f \in B$ then $q^{-1}(V) = D_X(f)$, and we find

$$O_Y(V) = B_f = (A^G)_f \xrightarrow{\sim} (A_f)^G = \big(O_X(q^{-1}(V))\big)^G = \big((q_*O_X)(V)\big)^G\,.$$

As the fundamental open subsets form a basis for the topology on Y, it follows that $q^\sharp\colon O_Y \to q_*O_X$ induces an isomorphism $O_Y \xrightarrow{\sim} (q_*O_X)^G$.

QFGSStep7 **(4.23)** Let us now prove the last assertion of part (i) of the theorem. As before we may assume that $S = \mathrm{Spec}(Q)$ is affine. Let $q\colon X \to Y := (G\backslash X)_{\mathrm{rs}}$ be the quotient morphism, which we have already shown to exist. Let $U = \mathrm{Spec}(A)$ be a G-stable affine open subset of X, and let

$B = A^G$. By construction, $q(U) = \mathrm{Spec}(B)$ is an open subset of Y, and $q^{-1}\big(q(U)\big) = U$. If X is locally of finite type over S then A is a finitely generated Q-algebra, a fortiori also of finite type as a B-algebra. But A is also integral over B. It follows that A is finitely generated as a B-module (see e.g. Atiyah-Macdonald [1], Cor. 5.2). Hence q is a finite morphism.

If S is locally noetherian then we may assume, arguing as in (4.18), that Q is a noetherian ring. Choose generators $a_1, \ldots, a_n$ for A as a Q-algebra. We have seen that for each i we can find a monic polynomial $f_i \in B[T]$ with $f_i(a_i) = 0$. Let $B' \subset B$ be the Q-subalgebra generated by the coefficients of the polynomials f_i. Then A is integral over B', and by the same argument as above it follows that A is finitely generated as a B'-module. Because B' is finitely generated over Q it is a noetherian ring. But then $B \subset A$ is also finitely generated as a B'-module, hence finitely generated as a Q-algebra. This shows that Y is locally of finite type over S.

So far we have used only that X is locally of finite type over S. Assume, in addition, that the morphism $f\colon X \to S$ is quasi-compact. Let $g\colon Y \to S$ be the structural morphism of Y. It remains to be shown that g is quasi-compact. But this is clear, for if $V \subset S$ is a quasi-compact open subset then $g^{-1}(V) = q\big(f^{-1}(V)\big)$, which is quasi-compact because $f^{-1}(V)$ is.

QFGSStep7A **(4.24)** Proof of (ii) of the theorem. Let $S' \to S$ be a flat morphism. We want to show that $Y' := Y \times_S S'$ is a geometric quotient of X' by G'. Arguing as in (4.18) one reduces to the case that $S' \to S$ is given by a flat homomorphism of rings $Q \to Q'$. Note that every G'-equivalence class in X' is again contained in an affine open subset. As in (4.19) one further reduces to the case that X, X', Y and Y' are all affine. With notations as above we have $Y = \mathrm{Spec}(B)$, where $B = \mathrm{Ker}(j - \sigma)$. We want to show, writing a prime $'$ for extension of scalars to Q', that $B \otimes_Q Q' = \mathrm{Ker}(j' - \sigma'\colon A' \otimes_{Q'} R' \to A' \otimes_{Q'} A')$. But this is obvious from the assumption that $Q \to Q'$ is flat.

QFGSStep8 **(4.25)** We now turn to part (iii) of the theorem. As before, everything reduces to the situation where S, G, X and Y are all affine, with algebras Q, R, A and $B = A^G$, respectively, and that R is free of rank r as a module over Q. We view $R \otimes_Q A$ as an A-module via j. Let

$$\varphi\colon A \otimes_B A \to R \otimes_Q A$$

be the homomorphism given by $\varphi(a_1 \otimes a_2) = \sigma(a_1) \cdot j(a_2) = \sigma(a_1) \cdot (1 \otimes a_2)$.

Assume that G acts freely on X. This means that the morphism $\Psi\colon G \times_S X \to X \times_S X$ is a monomorphism in the category of schemes. The corresponding map on rings is given by $\Psi^\sharp = \varphi \circ q$, where $q\colon A \otimes_Q A \twoheadrightarrow A \otimes_B A$ is the natural map. Since a morphism of affine schemes is a monomorphism if and only if the corresponding map on rings is surjective, it follows that φ is surjective.

Let $\mathfrak{q}$ be a prime ideal of B and write $A_\mathfrak{q} = (B - \mathfrak{q})^{-1}A \cong A \otimes_B B_\mathfrak{q}$. Note that $A_\mathfrak{q}$ is a semi-local ring, because $X \to Y$ is quasi-finite. Let $\mathfrak{r} \subset A_\mathfrak{q}$ be its radical. We claim that $A_\mathfrak{q}$ is free of rank $r = \mathrm{rank}(G)$ as a module over $B_\mathfrak{q}$. If this holds for all $\mathfrak{q}$ then A is a projective B-module of rank r; use Bourbaki [2], Chap. II, § 5, Thm. 2. Furthermore, φ is then a surjective map between projective A-modules of the same rank and is therefore an isomorphism.

We first prove that $A_\mathfrak{q}$ is $B_\mathfrak{q}$-free of rank r in the case where the residue field k of $B_\mathfrak{q}$ is infinite. Consider the $B_\mathfrak{q}$-submodule

$$N := \{\sigma(a) \mid a \in A_\mathfrak{q}\} \subset M := R \otimes_Q A_\mathfrak{q}\,.$$

Because $\varphi_\mathfrak{q}\colon A_\mathfrak{q} \otimes_{B_\mathfrak{q}} A_\mathfrak{q} \to R \otimes_Q A_\mathfrak{q}$ is surjective, N spans M as an $A_\mathfrak{q}$-module. Therefore $N/\mathfrak{r}N$ spans $M/\mathfrak{r}M \cong (A_\mathfrak{q}/\mathfrak{r})^r$ as a module over $A_\mathfrak{q}/\mathfrak{r}$, which is a product of fields. Using that

k is an infinite subfield of $A_{\mathfrak{q}}/\mathfrak{r}$ it follows that $N/\mathfrak{r}N$ contains a basis of $M/\mathfrak{r}M$ over $A_{\mathfrak{q}}/\mathfrak{r}$; see Exercise (4.3). Applying the Nakayama lemma, it follows that N contains a basis of M over $A_{\mathfrak{q}}$, i.e., we have elements $a_1, \dots a_r \in A_{\mathfrak{q}}$ such that the elements $\varphi_{\mathfrak{q}}(a_i \otimes 1) = \sigma(a_i)$ form an $A_{\mathfrak{q}}$-basis of $R \otimes_Q A_{\mathfrak{q}}$. Hence for every $a \in A_{\mathfrak{q}}$ there are unique coordinates $x_1, \dots, x_r \in A_{\mathfrak{q}}$ such that

Quot:QFGSfinal
$$\begin{aligned} \sigma(a) &= x_1 \cdot \sigma(a_1) + \cdots + x_r \cdot \sigma(a_r) \\ &= (1 \otimes x_1) \cdot \sigma(a_1) + \cdots + (1 \otimes x_r) \cdot \sigma(a_r)\,. \end{aligned} \tag{4}$$

We view $R'' := R \otimes_Q R \otimes_Q A_{\mathfrak{q}}$ as a module over $R \otimes_Q A_{\mathfrak{q}}$ via the homomorphism $j_{2,3}$ given by $r \otimes a \mapsto 1 \otimes r \otimes a$. The diagrams (2) tell us that the elements

$$\gamma_i := (\tilde{m} \otimes \mathrm{id}_A)\big(\sigma(a_i)\big) = (\mathrm{id}_R \otimes \sigma)\big(\sigma(a_i)\big)$$

form an $R \otimes_Q A_{\mathfrak{q}}$-basis of R''. Applying $\tilde{m} \otimes \mathrm{id}_A$ and $\mathrm{id}_R \otimes \sigma$ to (4) gives

$$\begin{array}{rcl} (\tilde{m} \otimes \mathrm{id}_A)\big(\sigma(a)\big) & = & (1 \otimes 1 \otimes x_1) \cdot \gamma_1 + \cdots + (1 \otimes 1 \otimes x_r) \cdot \gamma_r \\ \| & & \\ (\mathrm{id}_R \otimes \sigma)\big(\sigma(a)\big) & = & \big(1 \otimes \sigma(x_1)\big) \cdot \gamma_1 + \cdots + \big(1 \otimes \sigma(x_r)\big) \cdot \gamma_r\,. \end{array}$$

Hence the coordinates x_i lie in B, and (4) becomes $\sigma(a) = \sigma(x_1 a_1 + \cdots + x_r a_r)$. But we have seen in (4.20) that σ is injective, hence $a = x_1 a_1 + \cdots + x_r a_r$. This proves that the elements $a_1, \dots, a_r$ span $A_{\mathfrak{q}}$ as a $B_{\mathfrak{q}}$-module. On the other hand, since the map $a \mapsto \sigma(a)$ is $B_{\mathfrak{q}}$-linear, the elements $a_1, \dots, a_r$ are linearly independent over $B_{\mathfrak{q}}$. Hence $A_{\mathfrak{q}}$ is free of rank r over $B_{\mathfrak{q}}$.

Finally we consider the case that $B_{\mathfrak{q}}$ has a finite residue field. By what was explained in Remark (4.7) we may assume that $S = Y$. Because $B \to B_{\mathfrak{q}}$ is flat we may, by (ii) of the theorem, further reduce to the case where $B = B_{\mathfrak{q}}$. Let $h\colon B \to B'$ be a faithfully flat homomorphism, where B' is a local ring with infinite residue field; for instance we could take B' to be a strict henselization of $B = B_{\mathfrak{q}}$. In order to show that $A = A_{\mathfrak{q}}$ is free of rank r over B, it suffices to show that $A' := A \otimes_B B'$ is free of rank r over B', see EGA IV, 2.5.2. But, again by (ii), $\mathrm{Spec}(B')$ is the quotient of $\mathrm{Spec}(A')$ under the G-action obtained by base-change. Hence we are reduced to the case treated above.

QFGSStep9 **(4.26)** As the final step in the proof we show that if G acts freely, Y is a universal geometric quotient. Consider a morphism $h\colon S' \to S$. Let us indicate base change via h by a $'$, so $X' := X \times_S S'$, etc. Then G' acts again freely on X', and it is easy to see that every G'-equivalence class of closed points in $|X'|$ is contained in an affine open subset. (Since this statement only involves the fibres of X' we may assume that S' is affine, in which case the morphism $X' \to X$ is affine.) Hence there exists a geometric quotient, say $q_Z\colon X' \to Z$. As Z is a categorical quotient of X' by G', the morphism $q'\colon X' \to Y'$ factors as $q' = f \circ q_Z$ with $f\colon Z \to Y'$. We want to show that f is an isomorphism.

As before we may assume that G is free of rank r over S. Then X' is free of rank r over Z but at the same time it is free of the same rank r over Y'. But then Z has to be locally free of rank 1 over Y', so $f\colon Z \xrightarrow{\sim} Y'$. This completes the proof of Theorem (4.16). □

§3. *FPPF quotients.*

Consider an action of an S-group scheme G on an S-scheme X. In general there is not a simple procedure to construct a "good" quotient of X by G in the category $\mathsf{Sch}_{/S}$. Of course we have the notion of a categorical quotient, but this is only a "best possible approximation in the given category", and its definition gives no clues about whether there exists a categorical quotient and, if so, how to describe it.

Most approaches to the formation of quotients follow the same pattern:

(a) replace the category $\mathsf{Sch}_{/S}$ of S-schemes by some "bigger" category, in which the formation of quotients is easier;

(b) form the quotient $Y := G\backslash X$ in this bigger category;

(c) study under which assumptions the quotient Y is (representable by) a scheme.

Thus, for instance, in our discussion of geometric quotients the "bigger" category that we used was the category of ringed spaces over S.

The approach usually taken in the theory of group schemes is explained with great clarity in Raynaud [2]. The idea is that one chooses a Grothendieck topology on the category of S-schemes and that all objects in question are viewed as sheaves on the resulting site. The quotient spaces that we are interested in exist as sheaves—this usually involves a sheafification—and their construction has good functorial properties. Then it remains to be investigated under what conditions the quotient sheaf is representable by a scheme. For the choice of the topology, a couple of remarks have to be taken into account. First, we want our original objects, schemes, to be sheaves rather than presheaves; this means that the topology should be no finer than the canonical topology (see Appendix ??). On the other hand, the finer the topology, the weaker the condition that a sheaf is representable. Finally the topology has to be accessible by the methods of algebraic geometry. In practice one usually works with the étale topology, the fppf topology or the fpqc topology. We shall mostly work with the fppf topology. See (4.36) below for further discussion.

From a modern perspective, perhaps the most natural choice for the "bigger category" in which to work, is the category of algebraic stacks. An excellent reference for the foundations of this theory is the book by Laumon and Moret-Bailly [1]. For general results about the formation of quotients as algebraic spaces we recommend the papers by Keel and Mori [1] and Kollár [1]. However, at this stage in our book we shall not assume any knowledge of algebraic spaces or stacks (though algebraic spaces will be briefly mentioned in our discussion of Picard functors in Chap. 6).

Finally let us remark that we shall almost exclusively deal with quotients modulo a group action, and not with more general equivalence relations or groupoids. It should be noted that even if one is interested only in group quotients, the proofs often involve more general groupoids.

FPPFTop **(4.27)** We shall use some notions that are explained in more detail in Appendix ??.

Let S be a scheme. We write $(S)_{\mathrm{FPPF}}$ for the big fppf site of S, i.e., the category $\mathsf{Sch}_{/S}$ of S-schemes equipped with the fppf topology. We write $\mathrm{FPPF}(S)$ for the category of sheaves on $(S)_{\mathrm{FPPF}}$.

The fppf topology is coarser than the canonical topology; this means that for every S-scheme X the presheaf $h_X = \mathrm{Hom}_S(-, X)$ is a sheaf on $(S)_{\mathrm{FPPF}}$. As explained in A?? this is essentially a reformulation of results in descent theory. Via $X \mapsto h_X$ we can identify $\mathsf{Sch}_{/S}$ with a full subcategory of $\mathrm{FPPF}(S)$. We shall usually simply write X for h_X.

Denote by $\mathsf{ShGr}_{/S}$ and $\mathsf{ShAb}_{/S}$ the categories of sheaves of groups, respectively sheaves of abelian groups, on $(S)_{\mathrm{FPPF}}$. The category $\mathsf{ShAb}_{/S}$ is abelian; $\mathsf{ShGr}_{/S}$ is not abelian (excluding $S = \emptyset$) but we can still speak about exact sequences. Unless specified otherwise, we shall from

now on view the category of S-group schemes as a full subcategory of $\mathsf{ShGr}_{/S}$. For example, we shall say that a sequence of S-group schemes

$$G' \xrightarrow{\varphi} G \xrightarrow{\psi} G''$$

is exact if it is exact as a sequence in $\mathsf{ShGr}_{/S}$, i.e., if $\mathrm{Ker}(\psi)$ represents the fppf sheaf associated to the presheaf $T \mapsto \mathrm{Im}\big(\varphi(T)\colon G'(T) \to G(T)\big)$.

FPPFQDef **(4.28) Definition.** Let G be an S-group scheme acting, by $\rho\colon G \times_S X \to X$, on an S-scheme X. We write $(G\backslash X)_{\mathrm{fppf}}$, or simply $G\backslash X$, for the fppf sheaf associated to the presheaf

$$T \mapsto G(T)\backslash X(T)\,.$$

If $G\backslash X$ is representable by a scheme Y then we refer to Y (or to the quotient morphism $q\colon X \to Y$) as the *fppf quotient of X by G*.

We often say that "an fppf quotient exists" if $(G\backslash X)_{\mathrm{fppf}}$ is representable by a scheme. Note that the sheaf $G\backslash X$ is a categorical quotient of X by G in $\mathrm{FPPF}(S)$, so we are indeed forming the quotient in a "bigger" category. Note further that if $(G\backslash X)_{\mathrm{fppf}}$ is representable by a scheme Y then by the Yoneda lemma we have a morphism of schemes $q\colon X \to Y$.

As we are mainly interested in the formation of quotients of a group scheme by a subgroup scheme, we shall mostly restrict our discussion of fppf quotients to the case that the action is free.

FPPFExa **(4.29) Example.** Consider the situation as in (iii) of Theorem (4.16). So, G is finite locally free over S, acting freely on X, and every orbit is contained in an affine open set. Let $q_Y\colon X \to Y$ be the universal geometric quotient, as we have proven to exist. We claim that Y is also an fppf quotient. To see this, write $Z := (G\backslash X)_{\mathrm{fppf}}$ and write $q_Z\colon X \to Z$ for the quotient map. As Z is a categorical quotient in $\mathrm{FPPF}(S)$, the morphism q_Y, viewed as a morphism of fppf sheaves, factors as $q_Y = r \circ q_Z$ for some $r\colon Z \to Y$. To prove that r is an isomorphism it suffices to show that it is both a monomorphism and an epimorphism.

By (iii) of (4.16), the morphism q_Y is fppf. By A?? this implies it is an epimorphism of sheaves. But then r is an epimorphism too. On the other hand, suppose T is an S-scheme and suppose a, $b \in Z(T)$ map to the same point in $Y(T)$. There exists an fppf covering $T' \to T$ such that a and b come from points a', $b' \in X(T')$. But we know that $\Psi = (\rho, \mathrm{pr}_X)\colon G \times_S X \to X \times_Y X$ is an isomorphism, so there is a point $c \in G \times_S X(T')$ with $\rho(c) = a'$ and $\mathrm{pr}_X(c) = b'$. By construction of $Z := (G\backslash X)_{\mathrm{fppf}}$ this implies that $a = b$. Hence r is a monomorphism.

FPPFFunct **(4.30)** The formation of fppf quotients is compatible with base change. To explain this in more detail, suppose $j\colon S' \to S$ is a morphism of schemes. Then j gives rise to an inverse image functor $j^*\colon \mathrm{FPPF}(S) \to \mathrm{FPPF}(S')$ which is exact. Concretely, if $f\colon T \to S'$ is an S'-scheme then $j \circ f\colon T \to S$ is an S-scheme, and if F is an fppf sheaf on S then we have $j^*F(f\colon T \to S') = F(j \circ f\colon T \to S)$. In particular, on representable sheaves j^* is simply given by base-change: $j^*X = X \times_S S'$. Writing $X' = X \times_S S'$ and $G' = G \times_S S'$, we conclude that $j^*(G\backslash X) = (G'\backslash X')$ as sheaves on $(S')_{\mathrm{FPPF}}$. Hence if $q\colon X \to Y$ is an fppf quotient over S then $Y' := Y \times_S S'$ is an fppf quotient of X' by G'. Put differently: *An fppf quotient, if it exists, is automatically a* universal *fppf quotient.*

QuotProp **(4.31) Proposition.** *Let G be an S-group scheme acting freely on an S-scheme X. Suppose the fppf sheaf $(G\backslash X)_{\mathrm{fppf}}$ is representable by a scheme Y. Write $q\colon X \to Y$ for the canonical morphism. Then q is an fppf covering and the morphism $\Psi\colon G \times_S X \to X \times_Y X$ is an isomorphism. This gives a commutative diagram with cartesian squares*

$$\begin{array}{ccccc} G \times_S X & \xrightarrow{\sim} & X \times_Y X & \xrightarrow{\mathrm{pr}_1} & X \\ {\scriptstyle \mathrm{pr}_2}\downarrow & & {\scriptstyle \mathrm{pr}_2}\downarrow & & \downarrow{\scriptstyle q} \\ X & = & X & \xrightarrow{q} & Y \end{array} .$$

In particular, X is a G-torsor over Y in the fppf topology which becomes trivial over the covering $q\colon X \to Y$.

Proof. By construction, the projection $X \to Y$ is an epimorphism of fppf sheaves. This implies that it is an fppf covering; see A??. Further, $\Psi\colon G \times_S X \to X \times_Y X$ is an isomorphism of fppf sheaves, again by construction of $Y = G\backslash X$. By the Yoneda lemma (3.3), Ψ is then also an isomorphism of schemes. □

FPPFLoc **(4.32)** In the situation of the proposition, a necessary condition for $(G\backslash X)_{\mathrm{fppf}}$ to be representable by a scheme is that the action of G on X is *strictly* free. Indeed, this is immediate from the fact that $X \times_Y X$ is a subscheme of $X \times_S X$. But the good news contained in (4.31) is that if an fppf quotient exists, it has very good functorial properties. Let us explain this in some more detail.

We say that a property P of morphisms of schemes is *fppf local on the target* if the following two conditions hold:

(a) given a cartesian diagram

$$\begin{array}{ccc} X' & \xrightarrow{h} & X \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ S' & \underset{g}{\longrightarrow} & S \end{array}$$

we have $P(f) \Rightarrow P(f')$ (we say: "P is stable under base change");

(b) if furthermore $g\colon S' \to S$ is an fppf covering then $P(f) \Leftrightarrow P(f')$.

Many properties that play a role in algebraic geometry are fppf local on the target. More precisely, it follows from the results in EGA IV, § 2 that this holds for the property P of a morphism of schemes of being flat, smooth, unramified, étale, (locally) of finite type or finite presentation, (quasi-) separated, (quasi-) finite, (quasi-) affine, or integral.

FPPFLocCor **(4.33) Corollary.** *Let P be a property of morphisms of schemes which is local on the target for the fppf topology. If $q\colon X \to Y$ is an fppf quotient of X under the free action of an S-group scheme G, then*

$$\begin{array}{c} q\colon X \to Y \\ \text{has property } P \end{array} \iff \begin{array}{c} \mathrm{pr}_2\colon G \times_S X \to X \\ \text{has property } P \end{array} \impliedby \begin{array}{c} \pi\colon G \to S \\ \text{has property } P \end{array}$$

where moreover the last implication is an equivalence if $X \to S$ is an fppf covering.

Proof. Clear, as $q\colon X \to Y$ is an fppf covering and $G \times_S X \xrightarrow{\sim} X \times_Y X$. □

In the applications we shall see that this is a most useful result. After all, it tells us that an fppf quotient morphism $q\colon X \to Y$ inherits many properties from the structural morphism

$\pi\colon G \to S$. To study π we can use the techniques discussed in Chapter 3. To give but one example, suppose $S = \mathrm{Spec}(k)$ is the spectrum of a field and that G and X are of finite type over k. As before we assume that G acts freely on X. Then the conclusion is that an fppf quotient morphism $q\colon X \to Y$ is smooth if and only if G is a smooth k-group scheme. By (3.17) it suffices to test this at the origin of G, and if moreover $\mathrm{char}(k) = 0$ then by (3.20) G is automatically smooth over k.

QuotCompar **(4.34)** At this point, let us take a little step back and compare the various notions of a quotient that we have encountered.

Consider a base scheme S, an S-group scheme G acting on an S-scheme X, and suppose $q\colon X \to Y$ is a morphism of S-schemes. Then q realizes Y as

—*a categorical quotient of X by G* if q is universal for G-equivariant morphisms from X to an S-scheme with trivial G-action;

—*a geometric quotient of X by G* if $|Y| = |X|/\sim$ and $O_Y = (q_*O_X)^G$, i.e., Y represents the quotient of X by G formed in the category of ringed spaces;

—*an fppf quotient of X by G* if Y represents the fppf sheaf associated to the presheaf $T \mapsto G(T)\backslash X(T)$, i.e., Y represents the quotient of X by G formed in the category of fppf sheaves.

Further we have defined what it means for Y to be a universal categorical or geometric quotient. As remarked earlier, an fppf quotient is automatically universal.

The following result is due to Raynaud [1] and gives a comparison between fppf and geometric quotients.

GEOM/FPPF **(4.35) Theorem.** *Let G be an S-group scheme acting on an S-scheme X.*

(i) *Suppose there exists an fppf quotient Y of X by G. Then Y is also a geometric quotient.*

(ii) *Assume that X is locally of finite type over S, and that G is flat and locally of finite presentation over S. Assume further that the action of G on X is strictly free. If there exists a geometric quotient Y of X by G then Y is also an fppf quotient. In particular, the quotient morphism $q\colon X \to Y$ is an fppf morphism and Y is a universal geometric quotient.*

Proof. For the proof of (ii) we refer to Anantharaman [1], Appendix I. Let us prove (i). Suppose that $q\colon X \to Y$ is an fppf quotient. Write $r\colon X \to Z := (G\backslash X)_{\mathrm{rs}}$ for the quotient of X by G in the category of ringed spaces over S. Since r is a categorical quotient in $\mathsf{RS}_{/S}$ we have a unique morphism of ringed spaces $s\colon Z \to Y$ such that $q = s \circ r$. Our goal is to prove that s is an isomorphism. First note that q, being an fppf covering, is open and surjective. Since also r is surjective, this implies that the map s is open and surjective.

Next we show that s is injective. Suppose A and B are points of $|X|$ that map to the same point C in $|Y|$. We have to show that $\rho^{-1}\{A\} \cap \mathrm{pr}_X^{-1}\{B\}$ is non-empty, for then A and B map to the same point of Z, and the injectivity of s follows. Choose a field extension $\kappa(C) \subset K$ and K-valued points $a \in X(K)$ and $b \in X(K)$ with support in A and B, respectively, such that $q(a) = q(b)$. By construction of the fppf quotient, there exists a K-algebra L of finite type and an L-valued point $d \in G \times_S X(L)$ with $\rho(d) = a$ and $\mathrm{pr}_X(d) = b$. But then the image of $d\colon \mathrm{Spec}(L) \to G \times_S X$ is contained in $\rho^{-1}\{A\} \cap \mathrm{pr}_X^{-1}\{B\}$.

Finally, let U an open part of Y. There is a natural bijection between $\Gamma(U, O_Y)$ and the morphisms $U \to \mathbb{A}^1_S$ over S. Write $V := q^{-1}(U)$ and $W := \rho^{-1}(V) = \mathrm{pr}_X^{-1}(V)$. By the Yoneda lemma the morphisms $U \to \mathbb{A}^1_S$ as schemes are the same as the morphisms as fppf sheaves. By construction of the fppf quotient we therefore find that $\Gamma(U, O_Y)$ is in bijection with the set of

morphisms $f\colon V \to \mathbb{A}^1_S$ over S such that $f\circ\rho = f\circ \mathrm{pr}_X\colon W \to \mathbb{A}^1_S$. Writing $f := q\circ\rho = q\circ\mathrm{pr}_X$, this shows that O_Y is the kernel of $q_*O_X \rightrightarrows f_*O_{G\times_S X}$, which, by definition, is the subsheaf of G-invariant sections in q_*O_X. This proves that s is an isomorphism of ringed spaces, so that Y is also a geometric quotient of X by G. □

To summarize, we have the following relations between the various notions:*

$$\begin{array}{ccccc} \text{fppf quotient} & \Longrightarrow & \begin{array}{c}\text{universal}\\ \text{geometric quotient}\end{array} & \Longrightarrow & \begin{array}{c}\text{universal}\\ \text{categorical quotient}\end{array} \\ & \nwarrow & \Downarrow & & \Downarrow \\ & & \text{geometric quotient} & \Longrightarrow & \text{categorical quotient} \end{array}$$

where the implication "geometric ⇒ fppf" is valid under the assumptions as in (ii) of the theorem.

TopChoice **(4.36)** The sheaf-theoretic approach that we are discussing here of course also makes sense for other Grothendieck topologies on $\mathsf{Sch}_{/S}$, such as the étale topology. Thus, for instance, suppose $q\colon X \to Y$ is an fppf quotient of X by the action of an S-group scheme G. One may ask if q is also an étale quotient. But for this to be the case, q has to be an epimorphism of étale sheaves, which means that étale-locally on Y it admits a section. If this is not the case then q will not be a quotient morphism for the étale topology.

To give a simple geometric example, suppose $q\colon X \to Y$ is a finite morpism of complete non-singular curves over a field such that the extension $k(Y) \subset k(X)$ on function fields is Galois with group G. Then q is an fppf quotient of X by G, but it is an étale quotient only if there is no ramification, i.e., if q is étale.

Conversely, if étale-locally on Y the morphism q has a section then q is an epimorphism of étale sheaves and one shows without difficulty that q is an étale quotient of X by G. (Note that q is assumed to be an fppf quotient morphism, so we already know it is faithfully flat, and in particular also surjective.) But as the simple example just given demonstrates, for a general theory of quotients we obtain better results if we use a finer topology, such as the fppf topology.

QuotGr **(4.37)** Working with sheaves of groups has the advantage that many familiar results from ordinary group theory readily generalize. For instance, if H is a normal subgroup scheme of G then the fppf quotient sheaf G/H is naturally a sheaf of groups, and the canonical map $q\colon G \to G/H$ is a homomorphism. Hence if G/H is representable then it is a group scheme and the sequence $0 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 0$ is exact. In this case, if $f\colon G \to G'$ is a homomorphism of S-group schemes such that $f_{|H}$ is trivial then f factors uniquely as $f = f'\circ q$, where $f'\colon G/H \to G'$ is again a homomorphism of group schemes.

To conclude our general discussion of fppf quotients, let us now state two existence results. For some finer results see Raynaud [1] and [2], SGA 3, Exp. V and VI, and Anantharaman [1].

QuotExist1 **(4.38) Theorem.** *Let G be a proper and flat group scheme of finite type over a locally noetherian basis S. Let $\rho\colon G\times_S X \to X$ define a strictly free action of G on a quasi-projective S-scheme X. Then the fppf quotient $G\backslash X$ is representable by a scheme.*

A proof of this result can be found in SGA 3, Exp. V, § 7.

* schuine pijl moet gestreepte pijl worden

QuotExist2 **(4.39) Theorem.** *Let G be a flat group scheme of finite type over a locally noetherian base scheme S. Let $H \subset G$ be a closed subgroup scheme which is flat over S. Suppose that we are in one of the following cases:*

(a) $\dim(S) \leqslant 1$;

(b) *G is quasi-projective over S and H is proper over S;*

(c) *H is finite locally free over S such that every fibre $H_s \subset G_s$ is contained in an affine open subset of G.*

Then the fppf quotient sheaf G/H is representable by an S-scheme. If H is normal in G then G/H has the structure of an S-group scheme such that the natural map $q\colon G \to G/H$ is a homomorphism.

For the proof of this result in case (a) see Anantharaman [1], § 4. In case (b) the assertion follows from (4.38), and case (c) is an application of Thm. (4.16); cf. Example (4.29).

AVQuotExa **(4.40) Example.** Let X be an abelian variety over a field k. If $H \subset X$ is a closed subgroup scheme then by Thm. (4.38) there exists an fppf quotient $q\colon X \to Y := X/H$. By Thm. (4.35) q is also a geometric quotient, and from this it readily follows that Y is again an abelian variety.

§4. *Finite group schemes over a field.*

Now that we have some further techniques at our disposal, let us return to the study of group schemes. As an application of the above, we sketch the proof of a useful general result.

CGSAbCat **(4.41) Theorem.** *If k is a field then the category of commutative group schemes of finite type over k is abelian.*

Proof (sketch). Write $\boldsymbol{C}$ for the category of commutative group schemes of finite type over k. We view $\boldsymbol{C}$ as a full subcategory of the category $\mathsf{ShAb}_{/k}$ of fppf sheaves of abelian groups on $\mathrm{Spec}(k)$, which is an abelian category. Clearly $\boldsymbol{C}$ is an additive subcategory, and by (3.13) it is stable under the formation of kernels.

Let $f\colon G_1 \to G_2$ be a morphism in $\boldsymbol{C}$. In the category $\mathsf{ShAb}_{/k}$ we can form the quotients $q_1\colon G_1 \to G_1/\mathrm{Ker}(f)$ and $q_2\colon G_2 \to G_2/G_1$, and we have an isomorphism $\alpha\colon G_1/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Ker}(q_2)$. First one shows that the quotient morphism q_1 exists as a homomorphism of group schemes; see also (4.39) below. Let $\bar{G}_1 := G_1/\mathrm{Ker}(f)$, and let $\bar{f}\colon \bar{G}_1 \to G_2$ be the homomorphism induced by f. Note that $\bar{f}$ is a monomorphism. Now one proves that the quotient sheaf $G_2/\bar{G}_1$ is also representable by a k-scheme of finite type; for the details of this see SGA 3, Exp VI_A, Thm. 3.2. But the natural map of sheaves $G_2/G_1 \to G_2/\bar{G}_1$ is an isomorphism, so it follows that G_2/G_1 is a group scheme. In particular, $\boldsymbol{C}$ is stable under the formation of cokernels, and since $\boldsymbol{C}$ is a full subcategory of $\mathsf{ShAb}_{/k}$ we have an isomorphism $\alpha\colon G_1/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Ker}(q_2)$ in $\boldsymbol{C}$. □

We now focus on finite group schemes.

LocEtTerm **(4.42) Definition.** Let G be a finite group scheme over a field k. We say that G is

— *étale* if the structural morphism $G \to \mathrm{Spec}(k)$ is étale;

— *local* if G is connected.

Next suppose that G is commutative. Recall that we write G^D for the Cartier dual of G. We say that G is

— *étale-étale* if G and G^D are both étale;
— *étale-local* if G is étale and G^D is local;
— *local-étale* if G is local and G^D is étale;
— *local-local* if G and G^D are both local.

Let us note that if $k \subset K$ is a field extension and if G is étale (resp. local) then G_K is étale (resp. local), too. For étaleness this is clear; for the property of being local this is just Prop. (3.17), part (i).

LocEtExa **(4.43) Examples.** If $\mathrm{char}(k) = 0$ then it follows from Thm. (3.20) that every finite commutative k-group scheme is étale-étale. If $\mathrm{char}(k) = p > 0$ then all four types occur:

type:	étale-étale	étale-local	local-étale	local-local
example:	$(\mathbb{Z}/m\mathbb{Z})$ with $p \nmid m$	$(\mathbb{Z}/p^n\mathbb{Z})$	μ_{p^n}	α_{p^n}

LocEtLem **(4.44) Lemma.** *Let G_1 and G_2 be finite group schemes over a field k, with G_1 étale and G_2 local. Then the only homomorphisms $G_1 \to G_2$ and $G_2 \to G_1$ are the trivial ones.*

Proof. Without loss of generality we may assume that $k = \overline{k}$. Then $G_{2,\mathrm{red}} \subset G_2$ is a connected étale subgroup scheme; hence $G_{2,\mathrm{red}} \cong \mathrm{Spec}(k)$. Now note that any homomorphism $G_1 \to G_2$ factors through $G_{2,\mathrm{red}}$. Similarly, any homomorphism $G_2 \to G_1$ factors through $G_1^0 \cong \mathrm{Spec}(k)$. □

Note that the assertion about homomorphisms from an étale to a local group scheme does not generalize to arbitrary base schemes. For instance, if we take $S = \mathrm{Spec}\big(k[\varepsilon]\big)$ as a base scheme then the group $\mathrm{Hom}_S\big((\mathbb{Z}/p\mathbb{Z}), \mu_p\big)$ is isomorphic to the additive group k, letting $a \in k$ correspond to the homomorphism $(\mathbb{Z}/p\mathbb{Z})_S \to \mu_{p,S}$ given on points by $(n \bmod p) \mapsto (1 + a\varepsilon)^n$.

LocEtDec **(4.45) Proposition.** *Let G be a finite group scheme over a field k. Then G is an extension of an étale k-group scheme $G_{\text{ét}} = \varpi_0(G)$ by the local group scheme G^0; so we have an exact sequence*

Quot:GOGet
$$1 \longrightarrow G^0 \longrightarrow G \longrightarrow G_{\text{ét}} \longrightarrow 1\,. \tag{5}$$

If k is perfect then this sequence splits (i.e., we have a homomorphic section $G \leftarrow G_{\text{ét}}$) and G is isomorphic to a semi-direct product $G^0 \rtimes G_{\text{ét}}$. In particular, if k is perfect and G is commutative then $G \cong G^0 \times G_{\text{ét}}$.

Note that the étale quotient $G_{\text{ét}}$ is nothing but the group scheme $\varpi_0(G)$ of connected components introduced in (3.28). In the present context it is customary to think of $G_{\text{ét}}$ as a "building block" for G, and it is more customary to use a notation like $G_{\text{ét}}$.

Proof. Define $G_{\text{ét}} := \varpi_0(G)$, and consider the homomorphism $q\colon G \to G_{\text{ét}}$ as in Prop. (3.27). As shown there, q is faithfully flat, and the kernel of q is precisely the identity component G^0. Hence we have the exact sequence (5).

Let us now assume that k is perfect. Then $G_{\mathrm{red}} \subset G$ is a closed subgroup scheme (Exercise 3.2) which by (ii) of Prop. (3.17) is étale over k. We claim that the composition $G_{\mathrm{red}} \hookrightarrow G \twoheadrightarrow G_{\text{ét}}$ is an isomorphism. To see this we may assume that $k = \overline{k}$. But then G, as a scheme, is a finite disjoint union of copies of G^0. If there are n components then G_{red} and $G_{\text{ét}}$ are both isomorphic to the disjoint union of n copies of $\mathrm{Spec}(k)$, and it is clear that $G_{\mathrm{red}} \to G_{\text{ét}}$ is an isomorphism of group schemes. The inverse of this isomorphism gives a splitting of (5). □

Combining this with Lemma (4.44) we find that the category $\boldsymbol{C}$ of finite commutative group schemes over a perfect field k decomposes as a product of categories:

$$\boldsymbol{C} = \boldsymbol{C}_{\text{ét,ét}} \times \boldsymbol{C}_{\text{ét,loc}} \times \boldsymbol{C}_{\text{loc,ét}} \times \boldsymbol{C}_{\text{loc,loc}}\,.$$

As remarked above, $\boldsymbol{C} = \boldsymbol{C}_{\text{ét,ét}}$ if $\operatorname{char}(k) = 0$.

RanksExSeq **(4.46) Lemma.** *Let S be a connected base scheme. If $0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0$ is an exact sequence of finite locally free S-group schemes then* $\operatorname{rank}(G_2) = \operatorname{rank}(G_1) \cdot \operatorname{rank}(G_3)$.

Proof. Immediate from the fact that G_2 is a G_1-torsor over G_3 for the fppf topology, as this implies that O_{G_2} is locally free as an O_{G_3}-module, of rank equal to $\operatorname{rank}(G_1/S)$. □

pPowRank **(4.47) Proposition.** *Let k be a field of characteristic $p > 0$. Let G be a finite* connected *k-group scheme. Then the rank of G is a power of p.*

Proof. Let $F_{G/k}\colon G \to G^{(p)}$ be the relative Frobenius homomorphism. Write $G[F] := \operatorname{Ker}(F_{G/k})$. The strategy of the proof is to use the short exact sequence $1 \longrightarrow G[F] \longrightarrow G \longrightarrow G/G[F] \longrightarrow 1$ and induction on the rank of G. The main point is then to show that the affine algebra of $G[F]$ is of the form $k[X_1, \ldots, X_d]/(X_1^p, \ldots, X_d^p)$ with $d = \dim_k(T_{G,e})$. To prove this we use certain differential operators.

Write $G = \operatorname{Spec}(A)$, and let $I \subset A$ be the augmentation ideal. We have an isomorphism $I/I^2 \xrightarrow{\sim} \Omega_{A/k} \otimes_A k$, sending the class of $\xi \in I$ to $d\xi \otimes 1$. Further, (3.15) tells us that $\Omega_{A/k} \cong (\Omega_{A/k} \otimes_A k) \otimes_k A$. In total we find

$$\operatorname{Der}_k(A) = \operatorname{Hom}_A(\Omega_{A/k}, A) \cong \operatorname{Hom}_k(I/I^2, A)\,,$$

where the derivation $D_\varphi\colon A \to A$ corresponding to $\varphi\colon I/I^2 \to A$ satisfies $D_\varphi(\xi) = \varphi(\xi) \bmod I$ for all $\xi \in I$.

Choose elements $x_1, \ldots, x_d \in I$ whose classes form a k-basis for I/I^2. By the previous remarks, there exist k-derivations $D_i\colon A \to A$ such that $D_i(x_j) = \delta_{i,j} \bmod I$ for all i and j. We claim that for all non-negative numbers $m_1, \ldots, m_d$ and $n_1, \ldots, n_d$ with $m_1 + \cdots + m_d = n_1 + \cdots + n_d$ we have

Quot:DerForm
$$D_d^{m_d} D_{d-1}^{m_{d-1}} \cdots D_1^{m_1}\bigl(x_1^{n_1} \cdots x_d^{n_d}\bigr) \equiv \begin{cases} n_1!\, n_2! \cdots n_d! \bmod I, & \text{if } m_i = n_i \text{ for all } i; \\ 0 \bmod I, & \text{otherwise.} \end{cases} \tag{6}$$

To see this, note that for every $D \in \operatorname{Der}_k(A)$ the product rule implies that $D(I^r) \subseteq I^{r-1}$. With this remark, (6) follows by induction on the number $m_1 + \cdots + m_d$.

By Nakayama's lemma the x_i generate I, so we have

$$A \cong k[X_1, \ldots, X_d]/(f_1, \ldots, f_q)$$

via $x_i \leftrightarrow X_i$. Let $J = (f_1, \ldots, f_q) \subset A$. We claim that $J \subseteq (X_1^p, \ldots, X_d^p)$. To see this, suppose we have a polynomial relation between the x_i such that there are no terms x_i^a with $a \geqslant p$. Write this relation as

$$0 = h_0 + h_1(x_1, \ldots, x_d) + \cdots + h_r(x_1, \ldots, x_d)\,,$$

where h_j is a homogeneous polynomial of degree j. Let j be the smallest integer such that $h_j \neq 0$. Suppose $x_1^{n_1} \cdots x_d^{n_d}$ (with $n_1 + \cdots + n_d = j$) is a monomial occurring with non-zero

coefficient. Applying the differential operator $D_d^{n_d} D_{d-1}^{n_{d-1}} \cdots D_1^{n_1}$ and using (6) we obtain the relation $n_1! n_2! \cdots n_d! \in I$. This contradicts the fact that k is a field of characteristic p and that all n_i are $< p$. Hence $J \subseteq (X_1^p, \ldots, X_d^p)$, as claimed.

Let $F_{G/k}\colon G \to G^{(p)}$ be the relative Frobenius homomorphism. On rings it is given by

$$k[X_1, \ldots, X_d]/(f_1^{(p)}, \ldots, f_q^{(p)}) \longrightarrow k[X_1, \ldots, X_d]/(f_1, \ldots, f_q)\,, \qquad X_i \mapsto X_i^p\,.$$

As the zero section of $G^{(p)}$ is given by sending all X_i to 0 we find that the affine algebra of $G[F] := \mathrm{Ker}(F_{G/k})$ is

$$A_{G[F]} = k[X_1, \ldots, X_d]/(X_1^p, \ldots, X_d^p, f_1, \ldots, f_q) = k[X_1, \ldots, X_d]/(X_1^p, \ldots, X_d^p)\,.$$

In particular, $G[F]$ has rank p^d. Further, $\mathrm{rank}(G) = \mathrm{rank}\big(G[F]\big) \cdot \mathrm{rank}\big(G/G[F]\big) = p^d \cdot \mathrm{rank}\big(G/G[F]\big)$ by Lemma (4.46). As $G = G^0$ we have $d > 0$ if $G \neq \{1\}$; now the proposition follows by induction on $\mathrm{rank}(G)$. □

EtEtCor **(4.48) Corollary.** *If $\mathrm{char}(k) = p$ then a finite commutative k-group scheme is étale-étale if and only if $p \nmid \mathrm{rank}(G)$.*

Proof. In the "if" direction this is a direct consequence of the proposition combined with (4.45) and Lemma (4.46). Conversely, suppose G is étale-étale. We may assume that $k = \overline{k}$, in which case G is a constant group scheme. If $p \mid \mathrm{rank}(G)$ then G has a direct factor $(\mathbb{Z}/p^n\mathbb{Z})$. But then G^D has a factor μ_{p^n} and is therefore not étale. □

Exercises.

Ex:GmGm **(4.1)** Let S be a base scheme. Fix an integer $N \geqslant 2$. Take $G = X = \mathbb{G}_{m,S}$, and let $g \in G$ act on X as multiplication by g^N.

(i) Let T be an S-scheme. Let x_1 and x_2 be T-valued points of X; they correspond to elements $\gamma_1,\ \gamma_2 \in \Gamma(T, O_T)^*$. Let $c := \gamma_1/\gamma_2$, and define a scheme T', affine over T, by $T' := \mathrm{Spec}\,\big(O_T[t]/(t^N - c)\big)$. Show that the images of x_1 and x_2 in $X(T')$ lie in the same orbit under $G(T')$.

(ii) Show that $T' \to T$ is an epimorphism of schemes over S. (By definition this means that for every S-scheme Z the induced map $Z(T) \to Z(T')$ is injective.)

(iii) Suppose that $q\colon X \to Y$ is a G-invariant morphism of S-schemes. Show that for every S-scheme T the image of $q(T)\colon X(T) \to Y(T)$ consists of a single point. Conclude that $X \to S$ is a universal categorical quotient of X by G.

(iv) Show that the endomorphism $\mathbb{G}_m \to \mathbb{G}_m$ given by $g \mapsto g^N$ is faithfully flat and of finite presentation. Use this to show that the fppf sheaf $G\backslash X$ is represented by the scheme S.

Ex:GeqClass **(4.2)** Let $\rho\colon G \times_S X \to X$ be an action of an S-group scheme G on an S-scheme X. Define the relation $P \sim Q$ on $|X|$ as in (4.11). The goal of this exercise is to show that $\sim$ is an equivalence relation.

(i) Let $\Psi = \Psi_\rho$ be the graph morphism, as defined in (4.1). Write

$$\widetilde{\Psi}\colon |G \times_S X| \to |X| \times_{|S|} |X|$$

for the composition of the map $|\Psi|\colon |G \times_S X| \to |X \times_S X|$ and the canonical (surjective) map $|X \times_S X| \to |X| \times_{|S|} |X|$. Show that $P \sim Q$ precisely if $(P, Q) \in \mathrm{Im}\widetilde{\Psi}$.

(ii) Write $e(S) \subset G$ for the image of the identity section. Show that the projection $e(S) \times_S X \to X$ is an isomorphism. Conclude that $\sim$ is reflexive.

(iii) Let $s\colon X \times_S X \longrightarrow X \times_S X$ be the morphism reversing the factors. Find a morphism $f\colon G \times_S X \to G \times_S X$ such that $s \circ \Psi = \Psi \circ f$. Conclude that $\sim$ is symmetric.

(iv) Show that $\sim$ is transitive. [*Hint:* use that the natural map

$$\Big|(G \times_S X) \underset{\rho, X, \mathrm{pr}_X}{\times} (G \times_S X)\Big| \longrightarrow |G \times_S X| \underset{|\rho|, |X|, |\mathrm{pr}_X|}{\times} |G \times_S X|$$

is surjective.]

Ex:AlgExQFGS **(4.3)** Let k be an infinite field. Let Λ be a k-algebra which is a product of fields. Suppose M is a free Λ-module of finite rank. Let $N \subset M$ be a k-submodule such that N spans M as a Λ-module. Show that N contains a Λ-basis for M. Show by means of an example that the condition that k is infinite is essential.

Ex:KilledbyRk **(4.4)** Let $\pi\colon G \to S$ be a locally free group scheme of rank r over a reduced, irreducible base scheme S. The goal of this exercise is to show that G is annihilated by its rank, i.e., the morphism $[r]_G\colon G \to G$ given on points by $g \mapsto g^r$ equals the zero morphism $[0]_G = e \circ \pi\colon G \to S \to G$.

(i) Suppose S is the spectrum of a field k. Reduce the problem to the case that $G = G^0$. [*Hint:* Use (4.45) and Lemma (4.46). For étale group schemes reduce the problem to Lagrange's theorem in group theory.]

(ii) Suppose $S = \mathrm{Spec}(k)$ with $\mathrm{char}(k) = p$. Suppose further that $G = G^0 = \mathrm{Spec}(A)$. By (4.47) we have $\mathrm{rank}(G) = p^n$ for some n. If $I \subset A$ is the augmentation ideal, show that $I^{p^n} = (0)$. Now use the result of Exercise (3.7) to derive that $[p^n](I) = (0)$. Conclude that $[p^n]_G = [0]_G$.

(iii) Prove the stated result over an arbitrary reduced and irreducible basis. [*Hint:* use that the generic fibre of G is Zariski dense in G.]

[*Remark:* for *commutative* finite locally free group schemes the result holds without any restriction on the basis. This was proven by Deligne; see Tate-Oort [1]. It is an open problem if the result is also valid over arbitrary base schemes for non-commutative G.]

Ex:X/Glocalaty **(4.5)** Let S be a locally noetherian scheme. Let G be a finite locally free S-group scheme acting on an S-scheme X of finite type. Assume that for every closed point $P \in |X|$ the G-equivalence class of P is contained in an affine open subset. Write $q\colon X \to Y$ for the quotient morphism. If $x \in |X|$ then we write $\hat{O}_{X,x}$ for the completed local ring of X at the point x; likewise for other schemes.

(i) Let $y \in |Y|$. Show that the scheme $\hat{F}_y := \prod_{x \in q^{-1}(y)} \mathrm{Spec}(\hat{O}_{X,x})$ inherits a G-action, and that $\mathrm{Spec}(\hat{O}_{Y,y})$ is the quotient of $\hat{F}_y$ modulo G. [*Hint:* First reduce to the case that $S = Y$; then apply a flat base change.]

(ii) Suppose $S = \mathrm{Spec}(k)$ is the spectrum of a field. Let $x \in X(k)$ be a k-rational point with image $y \in Y(k)$ under q. Show that q induces an isomorphism $\hat{O}_{Y,y} \xrightarrow{\sim} (\hat{O}_{X,x})^{G_x}$.

Ex:FixedPts **(4.6)** Let $X \to S$ be a morphism of schemes. Let G be a finite group that acts on X over S.

(i) For $g \in G$, define a scheme X^g and a morphism $i_g\colon X^g \to X$ by the fibre product square

$$\begin{array}{ccc} X^g & \xrightarrow{i_g} & X \\ \downarrow & & \downarrow{\scriptstyle \Delta_X} \\ X & \xrightarrow[\psi_g]{} & X \times_S X \end{array}$$

where the morphism $\psi_g\colon X \to X \times_S X$ is given by $x \mapsto (g \cdot x, x)$. Show that i_g is an immersion and that it is a closed immersion if X/S is separated. fix

(ii) Define $X^G \hookrightarrow X$ as the scheme-theoretic intersection of the subschemes X^g, for $g \in G$. (In other words, if $G = \{g_1, \ldots, g_n\}$ then $X^G := X^{g_1} \times_X X^{g_2} \times_X \cdots \times_X X^{g_n}$.) Show that X^G is a subscheme of X, and that it is a closed subscheme if X/S is separated. Further show that for any S-scheme T we have $X^G(T) = X(T)^G$. The subscheme $X^G \hookrightarrow X$ is called the *fixed point subscheme* of the given action of G.

In this chapter we define the notion of an isogeny, and we discuss some basic examples, including the multiplication by an integer $n \neq 0$ and the relative Frobenius homomorphism in characteristic p. As applications we obtain results about the group of n-torsion points on an abelian variety. If the ground field has positive characteristic p this leads to the introduction of an invariant, the p-rank of the abelian variety.

§1. *Definition of an isogeny, and basic properties.*

FlatLem **(5.1) Lemma.** (i) *Let X and Y be irreducible noetherian schemes which are both regular and with $\dim(X) = \dim(Y)$. Let $f\colon X \to Y$ be a quasi-finite morphism. Then f is flat.*

(ii) *Let $f\colon X \to Y$ be a morphism of finite type between noetherian schemes, with Y reduced and irreducible. Then there is a non-empty open subset $U \subseteq Y$ such that either $f^{-1}(U) = \emptyset$ or the restricted morphism $f\colon f^{-1}(U) \to U$ is flat.*

A proof of (i) can be found in Altman-Kleiman [1], Chap. V, Cor. 3.6 or Matsumura [1], Thm. 23.1. For (ii) we refer to Mumford [2], Lecture 8.

IsogProp **(5.2) Proposition.** *Let $f\colon X \to Y$ be a homomorphism of abelian varieties. Then the following conditions are equivalent:*

(a) *f is surjective and $\dim(X) = \dim(Y)$;*

(b) *$\mathrm{Ker}(f)$ is a finite group scheme and $\dim(X) = \dim(Y)$;*

(c) *f is a finite, flat and surjective morphism.*

Proof. We shall use that if $h\colon Z_1 \to Z_2$ is a flat morphism of k-varieties and $F \subset Z_1$ is the fibre of h over a closed point of Z_2 then F is equidimensional and

Isogs:dim $$\dim(Z_1) = \dim(Z_2) + \dim(F)\,. \tag{1}$$

(This is a special case of HAG, Chap. III, Prop. 9.5.)

Let us first assume that (b) holds. As f is proper and all fibres are translates of $\mathrm{Ker}(f)$ it follows that f is finite. Hence $f(X)$ is closed in Y, of dimension equal to $\dim(X) = \dim(Y)$. Hence f is surjective. Further, by (i) of the lemma, f is flat. This shows that (a) and (c) hold.

Next suppose that (a) holds. By (ii) of the lemma, f is flat over a non-empty open subset $U \subseteq Y$. As all fibres of f are translates of $\mathrm{Ker}(f)$, (b) follows from (1). That (c) implies (b) again readily follows from (1). □

By making use of the results about quotients that were discussed in the previous chapter, we could do without Lemma (5.1). We leave such an alternative proof of the proposition to the reader.

IsogDef **(5.3) Definition.** A homomorphism $f\colon X \to Y$ of abelian varieties is called an *isogeny* if f satisfies the three equivalent conditions (a), (b) and (c) in (5.2). The *degree* of an isogeny f is the degree of the function field extension $[k(X)\colon k(Y)]$. (Note that we have a homomorphism $k(Y) \to k(X)$, since an isogeny is surjective.)

If $f\colon X \to Y$ is an isogeny then f induces an isomorphism $X/\mathrm{Ker}(f) \xrightarrow{\sim} Y$. Because all fibres of f are translates of $\mathrm{Ker}(f)$ the sheaf f_*O_X is a locally free O_Y-module of finite rank. Computing this rank at the generic point of Y, respectively the closed point $0 \in Y$, gives

$$\deg(f) = \mathrm{rank}_{O_Y}(f_*O_X) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)\,.$$

(Here $\mathrm{rank}\big(\mathrm{Ker}(f)\big)$ denotes the rank of the finite group scheme $\mathrm{Ker}(f)$.) If $f\colon X \to Y$ and $g\colon Y \to Z$ are isogenies then so is $g\circ f$, and $\deg(g\circ f) = \deg(g)\cdot\deg(f)$.

fghLem **(5.4) Lemma.** *Let $f\colon W \to X$ and $h\colon Y \to Z$ be isogenies of abelian varieties over k. If g_1, $g_2\colon X \to Y$ are homomorphisms such that $h\circ g_1\circ f = h\circ g_2\circ f$ then $g_1 = g_2$.*

Proof. We may assume that $k = \overline{k}$. Suppose $h\circ g_1\circ f = h\circ g_2\circ f$. Because f is faithfully flat, it is an epimorphism of schemes, so it follows that $h\circ g_1 = h\circ g_2$. Hence $g_1 - g_2$ maps X into the finite group scheme $\mathrm{Ker}(h)$. As X is connected and reduced, $g_1 - g_2$ factors through $\mathrm{Ker}(h)^0_{\mathrm{red}}$, which is trivial. □

PureInsep **(5.5)** We recall the notion of a purely inseparable morphism (French: morphisme radiciel). In EGA I$^{\mathrm{new}}$, Prop. 3.7.1 it is shown that the following conditions on a morphism of schemes $f\colon X \to Y$ are equivalent:

(a) f is universally injective; this means that for every $Y' \to Y$ the morphism $f'\colon X' \to Y'$ obtained from f by base change is injective;

(b) f is injective and for every $x \in X$ the residue field $k(x)$ is a purely inseparable extension of $k\big(f(x)\big)$;

(c) for every field K, the map $X(K) \to Y(K)$ induced by f is injective.

A morphism that satisfies these conditions is called a *purely inseparable morphism*.

SepIsogProp **(5.6) Proposition.** *Let $f\colon X \to Y$ be an isogeny.*

(i) *The following conditions are equivalent.*
- (a) *The function field $k(X)$ is a separable field extension of $k(Y)$;*
- (b) *f is an étale morphism;*
- (c) *$\mathrm{Ker}(f)$ is an étale group scheme.*

(ii) *The following conditions are equivalent.*
- (a) *The function field $k(X)$ is a purely inseparable field extension of $k(Y)$;*
- (b) *f is a purely inseparable morphism;*
- (c) *$\mathrm{Ker}(f)$ is a connected group scheme.*

Proof. (i) That (b) and (c) are equivalent is clear from (4.33). If f is étale then for every $x \in X$, writing $y = f(x) \in Y$, the residue field $k(x)$ is a finite separable extension of $k(y)$. If we apply this with x the generic point of X, we see that (b) implies (a).

Now assume that $k(X)$ is a finite separable extension of $k(Y)$. As f is a finite flat morphism, it is étale at a point $x \in X$ if and only if $(\Omega^1_{X/Y})_x = 0$. But $\Omega^1_{X/Y}$ is a coherent O_X-module, hence its support is closed, and it follows that the locus where f is étale is an open subset $U \subset X$. The assumption that $k(X)$ is finite separable over $k(Y)$ means that the generic point of X is in U, so U is non-empty. As f is proper it follows that there is an open subset $V \subset Y$ such that $f^{-1}(V)$ is étale over V. But V is the quotient of $f^{-1}(V)$ under $\mathrm{Ker}(f)$, so it follows from (4.33) that $\mathrm{Ker}(f)$ is étale.

(ii) We can factor f as a composition of two isogenies: $X \to X/\mathrm{Ker}(f)^0 \to Y$. The kernel of the second isogeny is $\mathrm{Ker}(f)/\mathrm{Ker}(f)^0$, which is étale. (See also Prop. (4.45).) Using (i) it follows that (a) implies (c).

That (b) implies (a) is immediate from property (b) in (5.5), applied to the generic point of X.

Finally suppose that $N := \mathrm{Ker}(f)$ is a connected group scheme. Let $k \subset K$ be a field extension. Let A be the affine algebra of N and write $A_K = A \otimes_k K$. If $y\colon \mathrm{Spec}(K) \to Y$ is a K-valued point then the scheme-theoretic fibre $f^{-1}(y) := X \times_{Y,y} \mathrm{Spec}(K)$ is isomorphic to $N_K = \mathrm{Spec}(A_K)$. As A_K has finite K-dimension it is an artinian ring. Any artinian ring is a product of artinian local rings; this corresponds to the decomposition of $f^{-1}(y)$ as a union of connected components. But we know from (i) of (3.17) that N_K is a connected scheme. Hence A_K is artinian local and $|f^{-1}(y)|$ consists of a single point. This shows that f satisfies condition (c) of (5.5) and is therefore purely inseparable. □

SepIsogDef **(5.7) Definition.** An isogeny $f\colon X \to Y$ is called *separable* if it satisfies the three equivalent conditions in (5.6)(i). It is called a *(purely) inseparable isogeny* if it satisfies the equivalent conditions of (5.6)(ii).

SepInsep **(5.8) Corollary.** *Every isogeny $f\colon X \to Y$ can be factorized as $f = h \circ g$, where $g\colon X \to Z$ is an inseparable isogeny and $h\colon Z \to Y$ is a separable isogeny. This factorization is unique up to isomorphism, in the sense that if $f = h' \circ g'\colon X \to Z' \to Y$ is a second such factorization then there is an isomorphism $\alpha\colon Z \xrightarrow{\sim} Z'$ with $g' = \alpha \circ g$ and $h = h' \circ \alpha$.*

Proof. Immediate from the above and Prop. (4.45). □

An important example of an isogeny is the multiplication $[n]_X\colon X \to X$ by an integer $n \neq 0$. We write $X[n] := \mathrm{Ker}([n]_X) \subset X$.

MultByn **(5.9) Proposition.** *For $n \neq 0$, the morphism $[n]_X$ is an isogeny. If $g = \dim(X)$, we have $\deg([n]_X) = n^{2g}$. If $(\mathrm{char}(k), n) = 1$ then $[n]_X$ is separable.*

Proof. Choose an ample and symmetric line bundle L on X. (Recall that L is said to be symmetric if $(-1)^*L \cong L$, and note that if L is ample then $L \otimes (-1)^*L$ is ample and symmetric.) By (2.12) we know that $n_X^*L \cong L^{\otimes n^2}$. The restiction of n_X^*L to $\mathrm{Ker}(f)$ is a trivial bundle which is ample. (Here we use that $n \neq 0$.) This implies that $\mathrm{Ker}(f)$ is finite, hence $[n]_X$ is an isogeny.

To compute the degree we use intersection theory on smooth varieties. Choose an ample symmetric divisor D. Then $\deg([n]_X) \cdot (D)^g = ([n]_X^*D)^g$. But $[n]_X^*D$ is linearly equivalent to $n^2 \cdot D$, so $([n]_X^*D)^g = n^{2g} \cdot (D)^g$, and we find that $\deg([n]_X) = n^{2g}$.

If $\mathrm{char}(k) = 0$ then the last assertion is trivial. If $\mathrm{char}(k) = p > 0$ with $p \nmid n$ then also $p \nmid n^{2g} = \mathrm{rank}(X[n])$, and the result follows from Cor. (4.48). Alternatively, as p does not divide $n^{2g} = \big[k(X_1) : k(X_2)\big]$, the field extension $k(X_2) \subset k(X_1)$ given by f is separable. □

Divisible **(5.10) Corollary.** *If X is an abelian variety over an algebraically closed field k then $X(k)$ is a divisible group. That is, for every $P \in X(k)$ and $n \in \mathbb{Z}\backslash\{0\}$ there exists a point $Q \in X(k)$ with $n \cdot Q = P$.*

Note that if the ground field k is only assumed to be separably closed then it is *not* true in general that $X(k)$ is a divisible group. See ?? for an example.

X[n]Struct **(5.11) Corollary.** *If* $(\mathrm{char}(k), n) = 1$ *then* $X[n](k_s) = X[n](\overline{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof. We know that $X[n]$ is an étale group scheme of rank n^{2g}. Hence $X[n](k_s) = X[n](\overline{k})$ is an abelian group of order n^{2g}, killed by n. Further, for every divisor d of n the subgroup of elements killed by d is just $X[d](k_s)$ and has order d^{2g}. It now readily follows from the structure theorem for finite abelian groups that we must have $X[n](k_s) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. □

fg=d=gf **(5.12) Proposition.** *If* $f\colon X \to Y$ *is an isogeny of degree* d *then there exists an isogeny* $g\colon Y \to X$ *with* $g \circ f = [d]_X$ *and* $f \circ g = [d]_Y$.

Proof. If $\deg(f) = d$ then $\mathrm{Ker}(f)$ is a finite group scheme of rank d and is therefore annihilated by multiplication by d; see Exercise (4.4). It follows that $[d]_X$ factors as

$$[d]_X = (X \xrightarrow{f} Y \xrightarrow{g} X)$$

for some isogeny $g\colon Y \to X$. Then $g \circ [d]_Y = [d]_X \circ g = (g \circ f) \circ g = g \circ (f \circ g)$, and by Lemma (5.4) it follows that $f \circ g = [d]_Y$. □

IsogEqRel **(5.13) Corollary.** *The relation*

$$X \sim_k Y \quad \stackrel{\text{def}}{=} \quad \text{there exists an isogeny } f\colon X \to Y$$

is an equivalence relation on the set of abelian varieties over k.

If there is no risk of confusion we shall use the notation $X \sim Y$ instead of $X \sim_k Y$. Note, however, that the ground field plays a role: if $k \subset K$ is a field extension then $X \sim_k Y$ implies that $X_K \sim_K Y_K$, but the converse does not hold in general.

If there exists an isogeny $f\colon X \to Y$ then we say that X and Y are *isogenous*. Again this notion is relative to a given ground field; if necessary we may specify that X and Y are isogenous over the given field k.

Isog/C **(5.14) Example.** Suppose we work over the field $\mathbb{C}$ of complex numbers. If X is an abelian variety over $\mathbb{C}$, the associated analytic manifold X^{an} is a complex torus; see also (1.11). So we can write $X^{\mathrm{an}} = V/L$, where V is a complex vector space and $L \subset V$ is a lattice. More intrinsically, V can be identified with the tangent space of X^{an} at the origin, and the projection map $V \to X$ is then the exponential map in the sense of Lie theory. We shall come back to this in more detail in Chapter ??.

Let X_1 and X_2 be complex abelian varieties; write $X_i^{\mathrm{an}} = V_i/L_i$. Let $f\colon X_1 \to X_2$ be a homomorphism. It follows from the previous remarks that the associated analytic map $f^{\mathrm{an}}\colon X_1^{\mathrm{an}} \to X_2^{\mathrm{an}}$ is given by a $\mathbb{C}$-linear map $\varphi\colon V_1 \to V_2$ such that $\varphi(L_1) \subseteq L_2$. Conversely, any such φ gives an analytic map $\bar{\varphi}\colon X_1^{\mathrm{an}} \to X_2^{\mathrm{an}}$, and it can be shown (using a result of Chow, see HAG, Appendix B, Thm. 2.2) that there exists a unique algebraic homomorphism $f\colon X_1 \to X_2$ with $\bar{\varphi} = f^{\mathrm{an}}$.

As an example, multiplication by n on X corresponds to $\varphi = n \cdot \mathrm{id}_V$, which obviously maps L into itself. We find that the group of n-torsion points $X[n](\mathbb{C})$ is isomorphic to $n^{-1}L/L \subset V/L$, and if $g = \dim(X)$ then indeed $n^{-1}L/L \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

As an application we find that $X_1 \sim X_2$ if and only if there exists a $\mathbb{C}$-linear isomorphism $\alpha\colon V_1 \xrightarrow{\sim} V_2$ such that $\alpha(L_1 \otimes \mathbb{Q}) = L_2 \otimes \mathbb{Q}$; in other words, there should exist positive integers m and n with $m \cdot L_2 \subseteq \alpha(L_1) \subseteq n^{-1} \cdot L_2$.

com
abe
Fro
Fro
iso
Ver

§2. *Frobenius and Verschiebung.*

As the next example of an isogeny, we look at Frobenius in characteristic $p > 0$.

FrobIsog **(5.15) Proposition.** *Let X be a g-dimensional abelian variety over a field k with $\mathrm{char}(k) = p > 0$. Then the relative Frobenius homomorphism $F_{X/k}\colon X \to X^{(p)}$ is a purely inseparable isogeny of degree p^g.*

Proof. Write $X[F] := \mathrm{Ker}(F_{X/k})$. On underlying topological spaces, the absolute Frobenius $\mathrm{Frob}_X\colon X \to X$ is the identity. It follows that the topological space underlying $X[F]$ is the singleton $\{e\}$. Let now $U = \mathrm{Spec}(A)$, with $A = k[x_1, \ldots, x_r]/(f_1, \ldots, f_n)$, be an affine open neigbourhood of e in X such that e corresponds to the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_r) \subset A$. Write $f_i^{(p)} \in k[x_1, \ldots, x_r]$ for the polynomial obtained from f_i by raising all coefficients to the pth power. Then $U^{(p)} = \mathrm{Spec}(A^{(p)})$, with $A^{(p)} = k[x_1, \ldots, x_r]/(f_1^{(p)}, \ldots, f_n^{(p)})$, and $F_{U/k}\colon U \to U^{(p)}$, the restriction of $F_{X/k}$ to U, is given on rings by

$$\begin{aligned} A = k[x_1, \ldots, x_r]/(f_1, \ldots, f_n) &\longleftarrow A^{(p)} = k[x_1, \ldots, x_r]/(f_1^{(p)}, \ldots, f_n^{(p)}) \\ x_i^p &\longleftarrow\!\shortmid\ x_i\,. \end{aligned}$$

It follows that $X[F] = \mathrm{Spec}(B)$, with $B = k[x_1, \ldots, x_r]/(x_1^p, \ldots, x_r^p, f_1, \ldots, f_n)$. In particular, $X[F]$ is finite, hence $F_{X/k}$ is an isogeny.

Write $\hat{A}$ for the $\mathfrak{m}$-adic completion of A. Without loss of generality we may assume that $x_1, \ldots, x_g$ form a basis of $\mathfrak{m}/\mathfrak{m}^2 = T_{X,e}^\vee$. The structure theory for complete regular local rings tells us that there is an isomorphism

$$k[\![t_1, \ldots, t_g]\!] \xrightarrow{\sim} \hat{A}$$

sending t_i to x_i. (See Bourbaki [2], Chap. VIII, § 5, n° 2.) Since $(x_1^p, \ldots, x_r^p) \subset \mathfrak{m}$, we find that

$$\begin{aligned} B = A/(x_1^p, \ldots, x_r^p)A &\cong \hat{A}/(x_1^p, \ldots, x_r^p)\hat{A} \\ &\cong \hat{A}/(x_1^p, \ldots, x_g^p)\hat{A} \\ &\cong k[\![t_1, \ldots, t_g]\!]/(t_1^p, \ldots, t_g^p) \\ &\cong k[t_1, \ldots, t_g]/(t_1^p, \ldots, t_g^p)\,. \end{aligned}$$

In particular this shows that $\deg(F_{X/k}) = \mathrm{rank}(X[F]) = p^g$ and that $X[F]$ is a connected group scheme. □

Our next goal is to define the *Verschiebung* isogeny for abelian varieties in characteristic p. In fact, under a suitable flatness assumption the Verschiebung can be defined for arbitrary commutative group schemes over a basis S with $\mathrm{char}(S) = p$; we shall give the construction in this generality. First we need some preparations.

VerschPrep **(5.16)** Let R be a ring with $\mathrm{char}(R) = p > 0$. Let A be an R-algebra. Write $T^p(A) := A \otimes_R \otimes_R \cdots \otimes_R A$ for the p-fold tensor product of A over R. The symmetric group $\mathfrak{S}_p$ on p letters naturally acts on $T^p(A)$ by ring automorphisms. Write $S^p(A) \subset T^p(A)$ for the subalgebra of $\mathfrak{S}_p$-invariants, i.e., the subalgebra of symmetric tensors. sym sym sym sym

Let $N\colon T^p(A) \to S^p(A)$ be the "symmetrizer" map, i.e., the map given by

$$N(a_1 \otimes \cdots \otimes a_p) = \sum_{\sigma \in \mathfrak{S}_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}\,.$$

If $s \in S^p(A)$ is a symmetric tensor and $t \in T^p(A)$ then $N(st) = sN(t)$. It follows that $J := N\big(T^p(A)\big)$ is an ideal of $S^p(A)$.

Write $U := \mathrm{Spec}(A) \to T := \mathrm{Spec}(R)$. Applying Thm. (4.8) we find that the quotient $S^p(U)$ of $U_T^p := U \times_T U \times_T \cdots \times_T U$ (p factors) under the natural action of $\mathfrak{S}_p$ exists and is given by $S^p(U) = \mathrm{Spec}\,\big(S^p(A)\big)$. The scheme $S^p(U)$ is called the p-th symmetric power of U over T. Note that $S^p(U/T)$ would be a better notation, as the base scheme is important in the construction. We trust, however, that the simpler notation $S^p(U)$ will not cause any confusion. Let $U^{[p/T]} \hookrightarrow S^p(U)$ be the closed subscheme defined by the ideal J. If $\eta\colon T^p(A) \to A$ is the multiplication map, given by $a_1 \otimes \cdots \otimes a_p \mapsto a_1 \cdots a_p$, then $\eta\big(N(a_1 \otimes \cdots \otimes a_p)\big) = p! \cdot (a_1 \cdots a_p) = 0$. This means that the morphism

$$U \xrightarrow{\Delta^p_{U/T}} U_T^p \longrightarrow S^p(U)$$

factors through $U^{[p/T]} \subset S^p(U)$. Write $F'_{U/T}\colon U \to U^{[p/T]}$ for the morphism thus obtained.

Write $A^{(p/R)} := A \otimes_{R,F} R$, where $F = \mathrm{Frob}_R\colon R \to R$ is the Frobenius homomorphism, given by $r \mapsto r^p$. We view $A^{(p/R)}$ as an R-algebra via $r \mapsto 1 \otimes r$; so for $a \in A$ and $r \in R$ we have the relations $r^p \cdot (a \otimes 1) = a \otimes r^p = (ra) \otimes 1$. By definition, $U^{(p/T)} = \mathrm{Spec}\,\big(A^{(p/R)}\big)$. Now observe that we have a well-defined map

$$\varphi_{A/R}\colon A^{(p/R)} \to S^p(A)/J$$

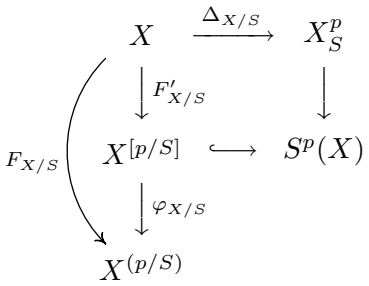
sending $a \otimes r \in A^{(p/R)}$ to $(ra \otimes a \otimes \cdots \otimes a) \bmod J$. Note that $(ra \otimes a \otimes \cdots \otimes a)$ is an element of $S^p(A)$ because all tensors are taken over the ring R. Also note that $\varphi_{A/R}$ is well-defined precisely because we use p-tensors. (Check this yourself!) Write $\varphi_{U/T}\colon U^{[p/T]} \to U^{(p/T)}$ for the morphism of schemes induced by $\varphi_{A/R}$. It is clear from the definitions that $F_{U/T} = \varphi_{U/T} \circ F'_{U/T}$.

We now globalize these constructions. For this, consider a base scheme S of characteristic p and an S-scheme $\pi\colon X \to S$. Define $S^p(X)$, the pth symmetric power of X over S, to be the quotient of X_S^p under the natural action of $\mathfrak{S}_p$. If $U \subset X$ and $T \subset S$ are affine open subsets with $\pi(U) \subseteq T$ then $S^p(U)$ is an affine open subset of $S^p(X)$. The closed subschemes $U^{[p/T]} \hookrightarrow S^p(U)$ glue to a locally closed subscheme $X^{[p/S]} \hookrightarrow S^p(X)$. Also, the morphisms $F'_{U/T}$ and $\varphi_{U/T}$ glue and give a factorization of the relative Frobenius morphism $F_{X/S}$ as

$$F_{X/S} = (X \xrightarrow{F'_{X/S}} X^{[p/S]} \xrightarrow{\varphi_{X/S}} X^{(p/S)})\,.$$

By construction, the composition of $F'_{X/S}$ and the inclusion $X^{[p/S]} \hookrightarrow S^p(X)$ is the same as the composition of the diagonal $\Delta^p_{X/S}\colon X \to X_S^p$ and the natural projection $X_S^p \to S^p(X)$. Summing

up, we have a commutative diagram



VerschLem **(5.17) Lemma.** (i) *The construction of $X^{[p/S]}$, as well as the formation of $F'_{X/S}$ and $\varphi_{X/S}$, is functorial in X and compatible with flat base change $T \to S$.*

(ii) *If X is flat over S then $\varphi_{X/S}\colon X^{[p/S]} \to X^{(p/S)}$ is an isomorphism of S-schemes.*

Proof. Part (i) of the lemma is a straightforward verification. For (ii), it suffices to treat the case that $X = U = \operatorname{Spec}(A)$ and $S = T = \operatorname{Spec}(R)$. Let M be an R-module. Just as before we can form the p-fold tensor product $T^p(M)$ of M over R and the submodule $S^p(M) \subset T^p(M)$ of symmetric tensors, and there is a symmetrizer map $N\colon T^p(M) \to S^p(M)$. We have a well-defined map

$$\varphi_{M/R}\colon M^{(p/R)} \longrightarrow S^p(M)/N\big(T^p(M)\big) \quad \text{given by} \quad m \otimes r \mapsto [rm \otimes m \otimes \cdots \otimes m]\,.$$

Suppose M is a free R-module with a basis $\{e_i\}_{i\in I}$. The tensors $e_{\underline{i}} := e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_p}$ with $\underline{i} = (i_1, \ldots, i_p) \in I^p$, form a basis of $T^p(M)$. Such a tensor $e_{\underline{i}}$ can be symmetrized in a minimal way. Namely, if $H \subset \mathfrak{S}_p$ is the stabilizer of $(i_1, \ldots, i_p)$ in the natural action of $\mathfrak{S}_p$ on I^p then for $\bar\sigma \in H\backslash\mathfrak{S}_p$ the element $e_{i_{\bar\sigma(1)}} \otimes e_{i_{\bar\sigma(2)}} \otimes \cdots \otimes e_{i_{\bar\sigma(p)}}$ is well-defined; now set

$$s_{\underline{i}} := \sum_{\bar\sigma \in H\backslash\mathfrak{S}_p} e_{i_{\bar\sigma(1)}} \otimes e_{i_{\bar\sigma(2)}} \otimes \cdots \otimes e_{i_{\bar\sigma(p)}}\,.$$

The symmetric tensors $s_{\underline{i}}$ obtained in this way span $S^p(M)$; note however that different sequences $\underline{i}$ may give the same tensor $s_{\underline{i}}$. If $i_1 = i_2 = \cdots = i_p$ then $N(e_{\underline{i}}) = p! \cdot s_{\underline{i}} = 0$; if not all i_j are equal then $N(e_{\underline{i}})$ is a unit times $s_{\underline{i}}$. (Recall that R is an $\mathbb{F}_p$-algebra.) We conclude that the tensors $e_i \otimes e_i \otimes \cdots \otimes e_i$ form a basis of $S^p(M)/N\big(T^p(M)\big)$, and it follows that $\varphi_{M/R}$ is an isomorphism if M is free over R.

Now we use a non-trivial result from commutative algebra. Namely, if M is flat over R then it can be written as a filtered direct limit, say $M = \varinjlim M_\alpha$, of free R-modules. For a proof see [??]. Since $\varinjlim$ is right exact and commutes with tensor products, $\varphi_{M/R}$ can be identified with $\varinjlim \varphi_{M_\alpha/R}$ and is therefore again an isomorphism. Applying this to $M = A$ the lemma follows. □

We now consider a commutative S-group scheme G. The morphism $m^{(p)}\colon G^p_S \to G$ given on sections by $(g_1, g_2, \ldots, g_p) \mapsto g_1 g_2 \cdots g_p$ factors through $S^p(G)$, say via $\bar m^{(p)}\colon S^p(G) \to G$. It follows that $[p]\colon G \to G$, which is equal to $m^{(p)} \circ \Delta^p_{G/S}$, factors as

Isogs:[p] $$[p] = \big(G \xrightarrow{F'_{G/S}} G^{[p/S]} \hookrightarrow S^p(G) \xrightarrow{\bar m^{(p)}} G\big)\,. \tag{2}$$

VerschDef **(5.18) Definition.** If G is a commutative flat group scheme over a basis S of characteristic p then we define the Verschiebung homomorphism

$$V_{G/S}\colon G^{(p/S)} \longrightarrow G$$

to be the composition

$$V_{G/S} = \big(G^{(p/S)} \xrightarrow{\varphi^{-1}_{G/S}} G^{[p/S]} \hookrightarrow S^p(G) \xrightarrow{\bar m^{(p)}} G\big)\,.$$

That $V_{G/S}$ is indeed a homomorphism of group schemes follows from (i) of the lemma.

VerschProp **(5.19) Proposition.** *Let S be a scheme with $\mathrm{char}(S) = p > 0$. Let G be a flat S-group scheme.*

(i) *We have $V_{G/S} \circ F_{G/S} = [p]_G\colon G \longrightarrow G$.*

(ii) *If G is finite locally free over S then the Verschiebung is Cartier dual to the Frobenius homomorphism; more precisely, we have $(V_{G/S})^D = F_{G^D/S}$ and $V_{G/S} = (F_{G^D/S})^D$.*

Proof. Statement (i) follows from the definitions; indeed, if we write $j\colon G^{[p/S]} \hookrightarrow S^p(G)$ for the inclusion morphism then

$$V_{G/S} \circ F_{G/S} = (\bar m^{(p)} \circ j \circ \varphi^{-1}_{G/S}) \circ (\varphi_{G/S} \circ F'_{G/S}) = \bar m^{(p)} \circ j \circ F'_{G/S} = [p]_G$$

by (2).

For (ii), suppose G is finite locally free over S. Without loss of generality we may assume that $S = \mathrm{Spec}(R)$ is affine, so that G is given by an R-algebra A. Possibly after further localization on S we may assume that A is free as a module over R, say with basis $\{e_1, \dots, e_n\}$. Recall from the proof of Lemma (5.17) that given a sequence $\underline{i} = (i_1, i_2, \dots, i_p) \in \{1, 2, \dots, n\}^p$, we can symmetrize the tensor $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_p}$ in a minimal way. The resulting collection of tensors

$$\{s_{\underline{i}}\}_{1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_p \leqslant n}$$

is a basis of $S^p(A)$. It follows from the proof of Lemma (5.17) that the Verschiebung $V_{G/S}$ is given on rings by the composition

$$A \xrightarrow{\bar m^{(p)}} S^p(A) \longrightarrow A^{(p/R)}\,,$$

where $\bar m^{(p)}$ is the homomorphism that corresponds to the morphism $\bar m^{(p)}\colon S^p(G) \to G$, and where the homomorphism $S^p(A) \to A^{(p/R)}$ is given by

$$s_{\underline{i}} \mapsto \begin{cases} 0, & \text{if } i_j < i_{j+1} \text{ for some } j; \\ e_i \otimes 1 & \text{if } \underline{i} = (i, i, \dots, i). \end{cases}\,.$$

Now we apply the functor $(\ )^D = \mathrm{Hom}_R(-, R)$. We have an isomorphism

$$\big(A^D\big)^{(p/R)} \xrightarrow{\sim} \big(A^{(p/R)}\big)^D$$

by sending $\varphi \otimes \rho \in A^D \otimes_{R,F} R$ to the map $a \otimes r \mapsto r\rho\varphi(a)^p$. Further there is a canonical isomorphism $\big(S^p(A)\big)^D \cong \mathrm{Sym}^p(A^D)$; here we note that by our general conventions in (??), $\mathrm{Sym}^p(A^D)$ is a *quotient* of the p-fold tensor product $T^p(A^D)$, whereas $S^p(A)$ is a *sub-algebra*

of $T^p(A)$. Using these identifications, and writing $\{\varepsilon_1, \dots, \varepsilon_n\}$ for the R-basis of A^D dual to $\{e_1, \dots, e_n\}$, the dual of the map $S^p(A) \to A^{(p/R)}$ is the map

$$\big(A^D\big)^{(p/R)} \longrightarrow \mathrm{Sym}^p(A^D) \quad \text{given by} \quad \varepsilon_i \otimes \rho \mapsto [\rho\varepsilon_i \otimes \varepsilon_i \otimes \cdots \otimes \varepsilon_i]\,.$$

Furthermore, by definition of the ring structure on A^D, the dual of the map $\bar{m}^{(p)}\colon A \to S^p(A)$ is the multiplication map $\mathrm{Sym}^p(A^D) \to A^D$ given by $[\varphi_1 \otimes \cdots \otimes \varphi_p] \mapsto \varphi_1 \cdots \varphi_p$. Combining this we see that the Cartier dual of $V_{G/S}$ is given on rings by the map

$$\big(A^D\big)^{(p/R)} \to A \quad \text{sending} \quad \varphi \otimes r \quad \text{to} \quad r \cdot \varphi^p\,.$$

This shows that $(V_{G/S})^D = F_{G^D/S}$. By Cartier duality then also $V_{G/S} = (F_{G^D/S})^D$. □

Now we apply this to abelian varieties.

VerschAV **(5.20) Proposition.** *Let X be an abelian variety over a field k with $\mathrm{char}(k) = p$. Then the Verschiebung homomorphism $V_{X/k}\colon X^{(p)} \to X$ is an isogeny of degree p^g. We have $V_{X/k} \circ F_{X/k} = [p]_X$ and $F_{X/k} \circ V_{X/k} = [p]_{X^{(p)}}$.*

Proof. Write $F = F_{X/k}$ and $V = V_{X/k}$. We have already seen that $V \circ F = [p]_X$. It follows that V satisfies (a) of Proposition (5.2); hence it is an isogeny. That V has degree p^g follows from the relation $p^{2g} = \deg\big([p]\big) = \deg(V) \cdot \deg(F) = \deg(V) \cdot p^g$. Finally, $F \circ V \circ F = F \circ [p] = [p] \circ F$, and because F is an epimorphism this implies that $F \circ V = [p]$. □

FVIterates **(5.21)** Let X be a k-scheme, where k is a field of characteristic p. For $m \geqslant 1$ we write $X^{(p^m)}$ for the base change of X over the mth power Frobenius homomorphism $\mathrm{Frob}_k^m\colon k \to k$. By a slight abuse of notation we write

$$F^m_{X/k} = F_{X^{(p^{m-1})}/k} \circ \cdots \circ F_{X^{(p)}/k} \circ F_{X/k}\colon X \to X^{(p)} \to X^{(p^2)} \to \cdots \to X^{(p^m)}$$

for the "mth power" of Frobenius, or "iterated Frobenius". Similarly, we can define an "mth iterated Verschiebung" $V^m_{X/k}\colon X^{(p^m)} \to X$ by

$$V^m_{X/k} = V_{X/k} \circ V_{X^{(p)}/k} \circ \cdots \circ V_{X^{(p^{m-1})}/k}\,.$$

By an easy induction on m we find that $[p^m]_X = V^m_{X/k} \circ F^m_{X/k}$ and $[p^m]_{X^{(p^m)}} = F^m_{X/k} \circ V^m_{X/k}$. Indeed, for $m = 1$ this is just Proposition (5.20), and to make the induction we note that

$$\begin{aligned} V^{m+1}_{X/k} \circ F^{m+1}_{X/k} &= V_{X/k} \circ V^m_{X^{(p)}/k} \circ F^m_{X^{(p)}/k} \circ F_{X/k} \\ &= V_{X/k} \circ [p^m]_{X^{(p)}} \circ F_{X/k} \\ &= [p^m]_X \circ V_{X/k} \circ F_{X/k} = [p^{m+1}]_X\,. \end{aligned}$$

(Likewise for the relation $[p^m]_{X^{(p^m)}} = F^m_{X/k} \circ V^m_{X/k}$.)

Let us now look what is the analogue of (5.11) in case $\mathrm{char}(k) \mid n$. In fact, since all $X[n](\overline{k})$ are finite abelian, it suffices to consider the case that $n = p^m$, where $p = \mathrm{char}(k) > 0$.

X[pm]Struct **(5.22) Proposition.** *Suppose $\mathrm{char}(k) = p > 0$. There is an integer $f = f(X)$, with $0 \leqslant f \leqslant g = \dim(X)$, such that $X[p^m](\overline{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^f$ for all $m \geqslant 0$. If Y is isogenous to X then $f(Y) = f(X)$.*

Proof. We can factor $p^m\colon X \to X$ as

$$[p^m]_X = \left(X \xrightarrow{F^m_{X/k}} X^{(p^m)} \xrightarrow{h_1} Y \xrightarrow{h_2} X \right),$$

where $h_1 \circ F^m_{X/k}$ is purely inseparable and h_2 is a separable isogeny. Looking at the degrees we find that $X[p^m](\overline{k})$ is an abelian group of rank $\deg(h_2) = p^{d(m)}$, where $d(m)$ is an integer with $0 \leqslant d(m) \leqslant gm$. Write $f = d(1)$, so that $X[p](\overline{k}) \cong (\mathbb{Z}/p\mathbb{Z})^f$. It follows from Corollary (5.10) that we have exact sequences of (abstract) groups

$$0 \longrightarrow X[p^{m-1}](\overline{k}) \longrightarrow X[p^m](\overline{k}) \xrightarrow{p^{m-1}} X[p](\overline{k}) \longrightarrow 0\,.$$

The claim that $X[p^m](\overline{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^f$ for all $m \geqslant 0$ follows by induction on m.

Finally, suppose $h\colon X \to Y$ is an isogeny, say of degree d. Then $X[p^m](\overline{k})$ maps to $Y[p^m](\overline{k})$, and the kernel has order at most d. Taking m large enough, it follows that $f(Y) \geqslant f(X)$. As $X \sim Y$ is a symmetric relation, we conclude that $f(X) = f(Y)$. □

pRankDef **(5.23) Definition.** The integer $f = f(X)$, which lies in the range $0 \leqslant f \leqslant g := \dim(X)$, is called the *p-rank* of X.

pRankCaution **(5.24) Caution.** Let X be an abelian variety of p-rank $f > 0$ over a non-perfect field k, and let $k \subset k_s \subset \overline{k}$ be respectively a separable closure and an algebraic closure of k. Then we have natural injective maps $X[p^m](k_s) \to X[p^m](\overline{k})$, but these are not, in general, isomorphisms. In other words, in order to see all p^{mf} distinct physical points of order p^m, in general we need an inseparable extension of the ground field.

At first sight this may seem to contradict the fact that an étale k-group scheme becomes constant over k_s. For instance, taking $m = 1$ we have a short exact sequence of k-group schemes

$$1 \longrightarrow X[p]_{\mathrm{loc}} \longrightarrow X[p] \longrightarrow X[p]_{\text{ét}} \longrightarrow 1\,,$$

(see Prop. (4.45)) and $X[p]_{\text{ét}} \otimes_k k_s$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^f$. However, in order to split the exact sequence, and hence to be able to lift the points of $X[p]_{\text{ét}}$ to points of $X[p]$, we in general need to pass to an inseparable extension. See also the examples in (5.26) and (5.27) below for a concrete illustration of this point.

prkEllC **(5.25) Remarks.** (i) The p-rank does not depend on the ground field. More precisely, if $k \subset K$ is a field extension and X is an abelian variety over k then $f(X) = f(X_K)$. To see this we may assume that k and K are both algebraically closed. By (4.45) the group scheme $X[p]$ is a product of its local and étale parts, i.e., $X[p] \cong X[p]_{\mathrm{loc}} \times X[p]_{\text{ét}}$. Over $k = \overline{k}$ the étale part becomes a constant group scheme, i.e., $X[p]_{\text{ét}} = \Gamma_k$ with $\Gamma = X[p](\overline{k})$. But after extension of scalars to K the local and étale parts of $X[p]$ remain local and étale, respectively; see ??. Therefore $X[p](K) = \Gamma_k(K) = \Gamma$, so indeed $f(X) = f(X_K)$.

(ii) Later we shall prove that the p-rank may take any value between 0 and $\dim(X)$: given a field k with $\mathrm{char}(k) = p > 0$ and integers $0 \leqslant f \leqslant g$, there exists an abelian variety X over k with $\dim(X) = g$ and $f(X) = f$. In fact, as clearly $f(X_1 \times X_2) = f(X_1) + f(X_2)$, it suffices to show that there exist elliptic curves X_0 and X_1 over k with $f(X_i) = i$.

(iii) An elliptic curve X is said to be *ordinary* if $f(X) = 1$ and *supersingular* if $f(X) = 0$. In the examples below we shall use this terminology. In Chapter ??, we shall define the notions

"ordinary" and "supersingular" for abelian varieties of arbitrary dimension. It should be noted that for $\dim(X) > 2$, "supersingular" is *not* equivalent to "p-rank $= 0$".

FEllCExa **(5.26) Example.** Let X be an elliptic curve over a field k with $\mathrm{char}(k) = 2$. Then X can be given by a Weierstrass equation

Isogs:Weier
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \tag{3}$$

such that the origin is the "point at infinity" $\infty = (0 : 1 : 0)$. A point $P \in X(k)$ with affine coordinates (ξ, η) is a 2-torsion point precisely if the tangent line at P passes through ∞. An easy calculation shows that this happens if and only if $a_1\xi + a_3 = 0$. We cannot have $a_1 = a_3$, because X then would be singular. We conclude:

$$f(X) = \begin{cases} 0 & \text{if } a_1 = 0; \\ 1 & \text{if } a_1 \neq 0. \end{cases}$$

It should be noted that if $a_1 = 0$ and $k = \overline{k}$ then there is a linear change of coordinates such that the equation for X becomes $y^2 + y = x^3$. So, up to isomorphism this is the only supersingular elliptic curve in characteristic 2 (over $k = \overline{k}$).

In the ordinary case, $a_1 \neq 0$, we find that the non-trivial point of order 2 in $X(\overline{k})$ is the point with affine coordinates $(a_3/a_1, \eta)$, where $\eta \in \overline{k}$ satisfies

$$\eta^2 = (a_3/a_1)^3 + a_2(a_3/a_1)^2 + a_4(a_3/a_1) + a_6\,.$$

In particular, we see illustrated here the point made in (5.24) that in general we need to pass to an inseparable extension of the ground field in order to have all p-torsion points rational.

FEllCExaB **(5.27) Example.** Let X be an elliptic curve given by a Weierstrass equation (3), this time over a field k with $\mathrm{char}(k) = 3$. Then $P \in X(k) \setminus \{0\}$ is a 3-torsion point if and only if P is a flex point, i.e., a point at which the tangent line $T_{X,P}$ intersects X with multiplicity 3. (As X is a nonsingular cubic curve the intersection multiplicity cannot be bigger.) Again this allows to compute the p-rank by hand. To simplify, let us assume that $a_1 = a_3 = 0$; this is achieved after a linear change of variables. Then $P = (\xi, \eta) \in X(k)$ is a flex point if and only if

Isogs:Flex
$$4a_2\eta^2 = 4a_2^2\xi^2 + 4a_2a_4\xi + a_4^2\,. \tag{4}$$

Combined with the equation for X this is equivalent to

Isogs:Flex2
$$4a_2\xi^3 + (4a_2a_6 - a_4^2) = 0\,. \tag{5}$$

As X is nonsingular we cannot have $a_2 = a_4 = 0$. Hence

$$X \text{ is ordinary} \iff^{\text{def}} X[3](\overline{k}) \cong \mathbb{Z}/3\mathbb{Z} \iff a_2 \neq 0\,.$$

Note that if $a_2 \neq 0$ then (5) has a unique solution for $\xi \in \overline{k}$, and if $\pm\eta$ are the corresponding solutions of (5.27.1) then $(\xi, \pm\eta)$ are the only two non-trivial 3-torsion points in $X(\overline{k})$. So indeed $X[3](\overline{k}) \cong \mathbb{Z}/3\mathbb{Z}$ and $f = 1$. Further note that solving (4) in general requires passing to an inseparable extension of k.

IsogExa **(5.28) Example.** Let k be a field of characteristic 2. Consider the elliptic curve $X \subset \mathbb{P}^2_k$ given by the homogeneous equation $x_1^2x_2 + x_1x_2^2 = x_0^3$, with $\infty = (0:1:0)$ as origin. As we have seen above, X is supersingular, which for an elliptic curve is the same as saying that X has p-rank zero.

Recall that the group scheme $\alpha_2 = \alpha_{2,k}$ is given by $\alpha_2 = \operatorname{Spec}\big(k[\varepsilon]/(\varepsilon^2)\big)$, with co-multiplication $\varepsilon \mapsto \varepsilon \otimes 1 + 1 \otimes \varepsilon$. We are going to give an action $\rho\colon \alpha_2 \times X \to X$ of α_2 on X. For this, write X as the union of two affine open subsets: $X = U_1 \cup U_2$, with

$$U_1 = X \setminus \{(0:1:0)\} = \operatorname{Spec}\big(k[x,y]/(x^3 - y^2 - y)\big)$$

and

$$U_2 = X \setminus \{(0:0:1)\} = \operatorname{Spec}\big(k[x,z]/(x^3 - z^2 - z)\big)\,.$$

Now we can give the action ρ on rings: let $\rho_1\colon \alpha_2 \times U_1 \to U_1$ be given by the homomorphism

$$k[x,y]/(x^3 - y^2 - y) \longrightarrow k[x,y,\varepsilon]/(x^3 - y^2 - y, \varepsilon^2) \qquad \text{with} \quad x \mapsto x + \varepsilon\,, \quad y \mapsto y + \varepsilon x^2\,,$$

and, similarly, let $\rho_2\colon \alpha_2 \times U_2 \to U_2$ be given on rings by $x \mapsto x + \varepsilon$ and $z \mapsto z + \varepsilon x^2$. It is not hard to verify that these homomorphisms are well-defined, that ρ_1 and ρ_2 agree on $U_1 \cap U_2$, and that the resulting morphism ρ is indeed a group scheme action. Note that the points $(0:1:0)$ and $(0:0:1)$ are α_2-stable when viewed as points in the underlying topological space $|X|$, but that they are *not* fixed points of the action. In fact, the action is strictly free.

On U_1 the functions $\xi := x^2$ and $\eta := y^2$ are α_2-invariant. They generate a subring of $O(U_1)$ of index 2; as the functions x and y themselves are clearly not invariant we conclude that

$$O(U_1)^{\alpha_2} \cong k[\xi,\eta]/(\xi^3 - \eta^2 - \eta) \longhookrightarrow O(U_1) = k[x,y]/(x^3 - y^2 - y)\,.$$

Similarly, the algebra of α_2-invariants in $O(U_2)$ is generated by x^2 and z^2. We find that the quotient $\alpha_2\backslash X$ is isomorphic to X itself, where the quotient map $X \to X$ is just the Frobenius endomorpism, given on points by $(x,y) \mapsto (x^2,y^2)$.

It can be shown that there is an isomorphism $X[F] \cong \alpha_2$ such that the action ρ described above becomes precisely the action of $X[F]$ on X by translations. As Exercise (??) shows, this does not immediately follow from the fact that the quotient map for the α_2-action is the Frobenius morphism. Note that from the given definition of the action ρ it is not clear that this is an action of a subgroup scheme by translations. We shall return to this later; see (??).

IsogsParam **(5.29) Example.** Let X be an elliptic curve over a field k with $\operatorname{char}(k) = p$, such that $X[F] \cong \alpha_{p,k}$. It is not hard to verify that $k \xrightarrow{\sim} \operatorname{End}_k(\alpha_{p,k})$, where the map sends $\lambda \in k$ to the endomorphism of $\alpha_{p,k} = \operatorname{Spec}\big(k[t]/(t^p)\big)$ given on rings by $t \mapsto \lambda \cdot t$. For $(\lambda,\mu) \in \mathbb{A}^2(k)$ we obtain an embedding $\varphi_{(\lambda,\mu)}\colon \alpha_{p,k} \hookrightarrow X \times X$ by taking the composition

$$\alpha_{p,k} \xrightarrow{(\lambda,\mu)} \alpha_{p,k} \times \alpha_{p,k} \cong X[F] \times X[F] \subset X \times X\,.$$

The image of $\varphi_{(\lambda,\mu)}$ only depends on $(\lambda:\mu) \in \mathbb{P}^1(k)$.

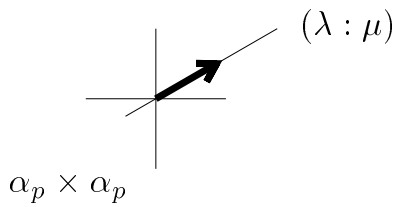


Figure ??.

We get a family of abelian surfaces over $\mathbb{P}^1$ by considering $Y_{(\lambda:\mu)} := (X \times X)/\varphi_{(\lambda,\mu)}(\alpha_p)$. It can be shown that given $(\lambda_0 : \mu_0) \in \mathbb{P}^1(k)$, there are only finitely many $(\lambda : \mu)$ with $Y_{(\lambda:\mu)} \cong Y_{(\lambda_0:\mu_0)}$. The conclusion is that we have a non-trivial "continuous" family of isogenies $X \times X \to Y_{(\lambda:\mu)}$. As we shall see later, such examples only exist in characteristic $p > 0$.

sup

tor

§3. *Density of torsion points.*

TorsionDense **(5.30) Theorem.** *Let X be an abelian variety over a field k and let p be a prime number. Then the collection of subschemes $X[p^m]$ for $m \geqslant 0$ is scheme-theoretically dense in X.*

Let $i_m\colon X[p^m] \hookrightarrow X$ be the inclusion homomorphism. By definition, saying that the collection of subschemes $X[p^m] \subset X$ is scheme-theoretically dense in X means that there does not exist a proper closed subscheme $Y \subsetneq X$ such that all i_m factor through Y. If $p \neq \mathrm{char}(k)$ we can express the density of the torsion points of p-power order in a more elementary way. Namely, in that case the following statements hold, as we shall see in the proof.

(1) *Topological density:* the union of the subspaces $\big|X[p^m]\big| \subset |X|$ is dense in $|X|$;
(2) *Function-theoretic density:* the homomorphism of sheaves $O_X \to \prod_{m\geqslant 0} O_{X[p^m]}$ that is induced by the homomorphisms i_m is injective.

Because X is reduced, properties (1) and (2) are equivalent, and (1) immediately implies that the collection of subschemes $X[p^n]$ is scheme-theoretically dense in X.

By contrast, if $p = \mathrm{char}(k)$ then (1) and (2) do not hold, in general. Indeed, if the p-rank of X is zero then the group schemes $X[p^m]$ are local, which means that the underlying topological space is reduced to the single point 0. So in this case we can only interprete the density statement scheme-theoretically.

Proof. We give separate proofs for the cases $p = \mathrm{char}(k)$ and $p \neq \mathrm{char}(k)$.

First assume that $p \neq \mathrm{char}(k)$. It suffices to prove the assertion for $k = \overline{k}$, which from now on we assume. In this case we know that $X[p^m]$ is étale and consists of p^{2gm} distinct closed points. Let $T \subset X(k)$ be the union of all $X[p^m](k)$, and let $Y \subset X$ be the smallest closed subscheme such that all i_m factor through Y. Note that Y is reduced; it is in fact just the reduced closed subscheme of X whose underlying space is the Zariski closure of T. We shall first prove that Y is a subgroup scheme of X.

If $x \in T$ then the translation $t_x\colon X \to X$ maps T into itself; hence $t_x(Y) \subseteq Y$. This holds for all $x \in T$, so it follows that for all $y \in Y(k)$ also the translation t_y maps T into itself, and hence $t_y(Y) \subset Y$. Because Y and $Y \times_k Y$ are reduced, this implies that under the group law $m\colon X \times X \to X$ we have $m(Y \times Y) \subset Y$. As further it is clear that also Y is mapped into itself under the inverse $\iota\colon X \to X$, we conclude that Y is indeed a subgroup scheme of X.

The identity component Y^0 is an abelian subvariety of X. Let N be the number of connected components of Y. Further, let $g = \dim(X)$ and $h = \dim(Y^0)$. By Prop. (5.9) we have $\#Y^0[p^m](k) = p^{2mh}$ for all $m \geqslant 0$, and it follows that $\#Y[p^m](k) \leqslant N \cdot p^{2mh}$. (If $W \subset Y$ is a connected component that contains a torsion point w with $p^m \cdot w = 0$ then translation by w gives an isomorphism $Y^0[p^m] \xrightarrow{\sim} W \cap X[p^m]$.) But by construction, Y contains all torsion points of X of p-power order; so $\#Y[p^m](k) = p^{2mg}$. Taking m very large we see that we must have $h = g$, which gives that $Y^0 = X$.

Next we deal with the case $p = \mathrm{char}(k)$. Let $F^m = F^m_{X/k}\colon X \to X^{(p^m)}$ be the mth power

of the Frobenius homomorphism, and let $X[F^m] \subset X$ be the kernel. Because $[p^m] = V^m \circ F^m$ (with $V^m = V^m_{X/k}$ the iterated Verschiebung; see (5.21)) we have $X[F^m] \subset X[p^m]$. So we are done if we can prove that the collection of group schemes $X[F^m]$ is scheme-theoretically dense in X. As in the proof of Prop. (5.15), let $U = \mathrm{Spec}(A)$ with $A = k[x_1, \ldots, x_r]/(f_1, \ldots, f_n)$ be an affine open neigbourhood of the origin e in X such that e corresponds to the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_r) \subset A$. Write $f_i^{(p^m)} \in k[x_1, \ldots, x_r]$ for the polynomial obtained from f_i by raising all coefficients to the power p^m, and write $A^{(p^m)} = k[x_1, \ldots, x_r]/(f_1^{(p^m)}, \ldots, f_n^{(p^m)})$. The restriction of F^m to U is given on rings by the homomorphism $A^{(p^m)} \to A$ that sends x_j to $x_j^{p^m}$. It follows that $X[F^m]$ is the closed subscheme of U defined by the ideal $(x_1^{p^m}, \ldots, x_r^{p^m}, f_1, \ldots, f_n) \subset A$.

Suppose $Y \subset X$ is a closed subscheme such that all inclusion homomorphisms $X[F^m] \hookrightarrow X$ factor through Y. Let $J \subset A$ be the ideal of $Y \cap U$. As in the proof of Prop. (5.15), let $\hat{A}$ be the $\mathfrak{m}$-adic completion of A and choose the coordinates x_i in such a way that $x_1, \ldots, x_g$ (with $g = \dim(X)$) form a basis of $\mathfrak{m}/\mathfrak{m}^2$. We then have an isomorphism $k[\![t_1, \ldots, t_g]\!] \xrightarrow{\sim} \hat{A}$ via $t_i \mapsto x_i$, and we shall identify $\hat{A}$ with $k[\![t_1, \ldots, t_g]\!]$ via this isomorphism. The assumption that $X[F^m]$ is a subscheme of Y means that $J\hat{A}$ is contained in the ideal $(t_1^{p^m}, \ldots, t_g^{p^m})$. The intersection of the ideals $(t_1^{p^m}, \ldots, t_g^{p^m}) \subset \hat{A}$ for all $m \geqslant 0$ is the zero ideal, so we conclude that $J\hat{A} = (0)$. But then the complete local ring $\hat{O}_{Y,e} = \hat{A}/J\hat{A}$ of Y at the origin has Krull dimension g, and consequently $Y = X$. □

We now prove the fact stated in Remark (2.14) that the results in (2.13) are true over an arbitrary, not necessarily perfect, ground field.

PfAVsubvarFact **(5.31) Proposition.** *Let X be an abelian variety over a field k. If $Y \hookrightarrow X$ is a closed subgroup scheme then the connected component $Y^0 \subset Y$ that contains the origin is an open and closed subgroup scheme of Y that is geometrically irreducible. The reduced underlying scheme $Y^0_{\mathrm{red}} \hookrightarrow X$ is an abelian subvariety of X.*

Proof. The assertion that Y^0 is open and closed in Y and is geometrically irreducible, was proven in Prop. (3.17). To prove that Y^0_{red} is an abelian subvariety of X we may assume, to simplify notation, that $Y = Y^0$. We are going to prove that Y_{red} is geometrically reduced. Before we give the argument, let us explain how the desired conclusion follows. If Y_{red} is geometrically reduced then we have, with $k \subset \overline{k}$ an algebraic closure, that $Y_{\mathrm{red},\overline{k}} = (Y_{\overline{k}})_{\mathrm{red}}$ is a closed subgroup scheme of $Y_{\overline{k}}$; see Exercise (3.2). But then also Y_{red} is a closed subgroup scheme of Y. Indeed, the assertion that Y_{red} is a subgroup scheme just means that the morphism $Y_{\mathrm{red}} \times Y_{\mathrm{red}} \to Y$ given on points by $(y_1, y_2) \mapsto y_1 - y_2$ factors through $Y_{\mathrm{red}} \subset Y$. If this holds after extension of scalars to $\overline{k}$ then it also holds over k. So the conclusion is that Y_{red} is a subgroup scheme of X that is geometrically integral; hence it is an abelian subvariety.

We now prove that Y_{red} is geometrically reduced. If $\mathrm{char}(k) = 0$ then $Y = Y_{\mathrm{red}}$ by Thm. (3.20) and we are done by Prop. (3.17). Assume then that $\mathrm{char}(k) = p > 0$. For all positive integers n with $p \nmid n$ the subgroup scheme $Y[n] \subset Y$ is étale; hence we have $Y[n] \subset Y_{\mathrm{red}} \subset Y$. This gives us a homomorphism of sheaves $h_n\colon O_{Y_{\mathrm{red}}} \to O_{Y[n]}$ on $|Y_{\mathrm{red}}| = |Y|$, and we define

$$h\colon O_{Y_{\mathrm{red}}} \to \prod_{p \nmid n} O_{Y[n]}$$

by $h(f) = \prod_n h_n(f)$. Further we know that $(Y_{\overline{k}})_{\mathrm{red}} \subset X_{\overline{k}}$ is an abelian subvariety. By Thm. (5.30) the collection of $Y[n]_{\overline{k}}$, for $n \geqslant 1$ with $p \nmid n$, is topologically dense in $|Y_{\overline{k}}| = |(Y_{\overline{k}})_{\mathrm{red}}|$. This implies that also the collection of all $Y[n]$ is topologically dense in $|Y| = |Y_{\mathrm{red}}|$, and because Y_{red} is reduced, the homomorphism h is injective.

Suppose that Y_{red} is not geometrically reduced. Then there is a finite, purely inseparable field extension $k \subset K$ such that $(Y_{\mathrm{red}})_K$ is not reduced. (See EGA IV, Prop. 4.6.1.) As $k \subset K$ is purely inseparable, we have $|(Y_{\mathrm{red}})_K| = |Y_{\mathrm{red}}|$ and $|Y[n]_K| = |Y[n]|$ for all n. The structure sheaves of $(Y_{\mathrm{red}})_K$ and $Y[n]_K$ are just $O_{Y_{\mathrm{red}}} \otimes_k K$ and $O_{Y[n]} \otimes_k K$, respectively, and the homomorphism

$$h \otimes \mathrm{id}\colon O_{Y_{\mathrm{red}}} \otimes_k K \to \big(\prod_{p\nmid n} O_{Y[n]}\big) \otimes_k K$$

can be identified with the map

$$h_K\colon O_{(Y_{\mathrm{red}})_K} \to \prod_{p\nmid n} O_{Y[n]_K}$$

induced by the inclusions $Y[n]_K \hookrightarrow (Y_{\mathrm{red}})_K$. By our assumptions, $(Y_{\mathrm{red}})_K$ is not reduced, whereas all $Y[n]_K$ are reduced schemes. Hence $h \otimes \mathrm{id} = h_K$ must have a non-trivial kernel. But then also h has a non-trivial kernel ($k \subset K$ being faithfully flat), which contradicts our earlier conclusion that it is injective. □

Exercises.

Ex:surjfflat **(5.1)** Let $f\colon X \to Y$ be a surjective homomorphism of abelian varieties. Show that f is flat.

Ex:SameQuot **(5.2)** Let $k = \mathbb{F}_p$. By definition, α_p is a subgroup scheme of $\mathbb{G}_a$, so that we get a natural action $\rho\colon \alpha_p \times \mathbb{G}_a \to \mathbb{G}_a$. Similarly, μ_p is a subgroup scheme of $\mathbb{G}_m$, which gives an action $\sigma\colon \mu_p \times \mathbb{G}_m \to \mathbb{G}_m$.

(i) Identify $\mathbb{G}_m$ with the open subscheme of $\mathbb{G}_a$ given by $x \neq 0$. Show that the action ρ restricts to a free action ρ' of α_p on $\mathbb{G}_m$, and that the Frobenius endomorphism $F\colon \mathbb{G}_m \to \mathbb{G}_m$, given on points by $x \mapsto x^p$, is a quotient morphism for ρ'.

(ii) Conclude that σ and ρ' give rise to the same quotient morphism, even though $\alpha_p \ncong \mu_p$.

§1. *Relative Picard functors.*

To place the notion of a dual abelian variety in its context, we start with a short discussion of relative Picard functors. Our goal is to sketch some general facts, without much discussion of proofs.

Given a scheme X we write

$$\mathrm{Pic}(X) = H^1(X, O_X^*) = \{\text{isomorphism classes of line bundles on } X\}\,,$$

which has a natural group structure. (If τ is either the Zariski, or the étale, or the fppf topology on $\mathsf{Sch}_{/X}$ then we can also write $\mathrm{Pic}(X) = H^1_\tau(X, \mathbb{G}_m)$, viewing the group scheme $\mathbb{G}_m = \mathbb{G}_{m,X}$ as a τ-sheaf on $\mathsf{Sch}_{/X}$; see Exercise ??.)

If C is a complete non-singular curve over an algebraically closed field k then its Jacobian $\mathrm{Jac}(C)$ is an abelian variety parametrizing the degree zero divisor classes on C or, what is the same, the degree zero line bundles on C. (We refer to Chapter 14 for further discussion of Jacobians.) Thus, for every $k \subset K$ the degree map gives a homomorphism $\mathrm{Pic}(C_K) \to \mathbb{Z}$, and we have an exact sequence

$$0 \longrightarrow \mathrm{Jac}(C)(K) \longrightarrow \mathrm{Pic}(C_K) \longrightarrow \mathbb{Z} \longrightarrow 0\,.$$

In view of the importance of the Jacobian in the theory of curves one may ask if, more generally, the line bundles on a variety X are parametrized by a scheme which is an extension of a discrete part by a connected group variety.

If we want to study this in the general setting of a scheme $f\colon X \to S$ over some basis S, we are led to consider the contravariant functor $P_{X/S}\colon (\mathsf{Sch}_{/S})^0 \to \mathsf{Ab}$ given by

$$P_{X/S}\colon T \mapsto \mathrm{Pic}(X_T) = H^1(X \times_S T, \mathbb{G}_m)\,.$$

However, one easily finds that this functor is not representable (unless $X = \emptyset$.). The reason for this is the following. Suppose $\{U_\alpha\}_{\alpha\in A}$ is a Zariski covering of S and L is a line bundle on X such that the restrictions $L_{|X\times_S U_\alpha}$ are trivial. Then it is not necessarily the case that L is trivial. This means that $P_{X/S}$ is not a sheaf for the Zariski topology on $\mathsf{Sch}_{/S}$, hence not representable. (See also Exercise (6.1).)

The previous arguments suggest that in order to arrive at a functor that could be representable we should first sheafify (or "localize") $P_{X/S}$ with respect to some topology.

RelPicDef **(6.1) Definition.** The *relative Picard functor* $\mathrm{Pic}_{X/S}\colon (\mathsf{Sch}_{/S})^0 \to \mathsf{Ab}$ is defined to be the fppf sheaf (on $(S)_{\mathrm{FPPF}}$) associated to the presheaf $P_{X/S}$. An S-scheme representing $\mathrm{Pic}_{X/S}$ (if such a scheme exists) is called the *relative Picard scheme* of X over S.

Concretely, if T is an S-scheme then we can describe an element of $\mathrm{Pic}_{X/S}(T)$ by giving an fppf covering $T' \to T$ and a line bundle L on $X_T \times_T T'$ such that the two pull-backs of L to $X_T \times_T (T' \times_T T')$ are isomorphic. Now suppose we have a second datum of this type, say an fppf

covering $U' \to T$ and a line bundle M on $X_T \times_T U'$ whose two pull-backs to $X_T \times_T (U' \times_T U')$ are isomorphic. Then $(T' \to T, L)$ and $(U' \to T, M)$ define the same element of $\mathrm{Pic}_{X/S}(T)$ if there is a common refinement of the coverings T' and U' over which the bundles L and M become isomorphic.

As usual, if $\mathrm{Pic}_{X/S}$ is representable then the representing scheme is unique up to S-isomorphism; this justifies calling it *the* Picard scheme.

RigLineB **(6.2)** Let us study $\mathrm{Pic}_{X/S}$ in some more detail in the situation that

$$(*) \quad \begin{cases} \text{the structure morphism } f\colon X \to S \text{ is quasi-compact and quasi-separated,} \\ f_*(O_{X\times_S T}) = O_T \text{ for all } S\text{-schemes } T, \\ f \text{ has a section } \varepsilon\colon S \to X. \end{cases}$$

For instance, this holds if S is the spectrum of a field k and X is a complete k-variety with $X(k) \neq \emptyset$ (see also Exercise ??); this is the case we shall mostly be interested in.

Rather than sheafifying $P_{X/S}$ we may also rigidify the objects we are trying to classify. This is done as follows. If L is a line bundle on X_T for some S-scheme T then, writing $\varepsilon_T\colon T \to X_T$ for the section induced by ε, by a *rigidification of L along ε_T* we mean an isomorphism $\alpha\colon O_T \xrightarrow{\sim} \varepsilon_T^* L$. (In the sequel we shall usually simply write ε for ε_T.)

Let (L_1, α_1) and (L_2, α_2) be line bundles on X_T with rigidification along ε. By a homomorphism $h\colon (L_1, \alpha_1) \to (L_2, \alpha_2)$ we mean a homomorphism of line bundles $h\colon L_1 \to L_2$ with the property that $(\varepsilon^* h) \circ \alpha_1 = \alpha_2$. In particular, an endomorphism of (L, α) is given by an element $h \in \Gamma(X_T, O_{X_T}) = \Gamma\big(T, f_*(O_{X_T})\big)$ with $\varepsilon^*(h) = 1$. By the assumption that $f_*(O_{X_T}) = O_T$ we therefore find that rigidified line bundles on X_T have no nontrivial automorphisms.

Now define the functor $P_{X/S,\varepsilon}\colon (\mathsf{Sch}_{/S})^0 \to \mathsf{Ab}$ by

$$P_{X/S,\varepsilon}\colon T \mapsto \left\{ \begin{matrix} \text{isomorphism classes of rigidified} \\ \text{line bundles } (L, \alpha) \text{ on } X \times_S T \end{matrix} \right\},$$

with group structure given by

$$\begin{aligned} &(L, \alpha) \cdot (M, \beta) = (L \otimes M, \gamma)\,, \\ &\gamma = \alpha \otimes \beta\colon O_T = O_T \underset{O_T}{\otimes} O_T \to \varepsilon^* L \underset{O_T}{\otimes} \varepsilon^* M = \varepsilon^*(L \otimes M)\,. \end{aligned}$$

If $h\colon T' \to T$ is a morphism of S-schemes and (L, α) is a rigidified line bundle on $X \times_S T$ then $P_{X/S,\varepsilon}(h)\colon P_{X/S,\varepsilon}(T) \to P_{X/S,\varepsilon}(T')$ sends (L, α) to (L', α'), where $L' = (\mathrm{id}_X \times h)^* L$ and where $\alpha'\colon O_{T'} \xrightarrow{\sim} \varepsilon_{T'}^* L' = h^*\big(\varepsilon_T^* L\big)$ is the pull-back of α under h.

Suppose $P_{X/S,\varepsilon}$ is representable by an S-scheme. On $X \times_S P_{X/S,\varepsilon}$ we then have a universal rigidified line bundle $(\mathscr{P}, \nu)$; it is called the *Poincaré bundle*. The universal property of $(\mathscr{P}, \nu)$ is the following: if (L, α) is a line bundle on $X \times_S T$ with rigidification along the section ε then there exists a unique morphism $g\colon T \to P_{X/S,\varepsilon}$ such that $(L, \alpha) \cong (\mathrm{id}_X \times g)^*(\mathscr{P}, \nu)$ as rigidified bundles on X_T.

Under the assumptions $(*)$ on f it is not so difficult to prove the following facts. (See for example BLR, § 8.1 for details.)

(i) For every S-scheme T there is a short exact sequence

DualAV1:exseq1
$$0 \longrightarrow \mathrm{Pic}(T) \xrightarrow{\mathrm{pr}_T^*} \mathrm{Pic}(X_T) \longrightarrow \mathrm{Pic}_{X/S}(T)\,. \tag{1}$$

This can be viewed as a short exact sequence obtained from a Leray spectral sequence. The existence of a section is not needed for this.

(ii) For every S-scheme T, we have an isomorphism

$$\mathrm{Pic}(X_T)/\mathrm{pr}_T^*\mathrm{Pic}(T) \xrightarrow{\sim} P_{X/S,\varepsilon}(T)$$

obtained by sending the class of a line bundle L on X_T to the bundle $L \otimes f^*\varepsilon^* L^{-1}$ with its canonical rigidification.

(iii) The functor $P_{X/S,\varepsilon}$ is an fppf sheaf. (Descent theory for line bundles.)

Combining these facts we find that $P_{X/S,\varepsilon} \cong \mathrm{Pic}_{X/S}$ and that these functors are given by

$$T \mapsto \frac{\mathrm{Pic}(X_T)}{\mathrm{pr}_T^*\mathrm{Pic}(T)} = \frac{\{\text{line bundles on } X_T\}}{\{\text{line bundles of the form } f^*L, \text{ with } L \text{ a line bundle on } T\}}\,.$$

In particular, the exact sequence (1) extends to an exact sequence

DualAV1:exseq2
$$0 \longrightarrow \mathrm{Pic}(T) \longrightarrow \mathrm{Pic}(X_T) \longrightarrow \mathrm{Pic}_{X/S}(T) \longrightarrow 0\,. \tag{2}$$

It also follows that $\mathrm{Pic}_{X/S}$ equals the Zariski sheaf associated to $P_{X/S}$.

PicRepr **(6.3)** Returning to the general case (i.e., no longer assuming that f satisfies the conditions $(*)$ in (6.2)), one finds that $\mathrm{Pic}_{X/S}$ cannot be expected to be representable unless we impose further conditions on X/S. (See Exercise ?? for an example.) The most important general results about representability all work under the assumption that $f\colon X \to S$ is proper, flat and of finite presentation. We quote some results:

(i) If f is flat and projective with geometrically integral fibres then $\mathrm{Pic}_{X/S}$ is representable by a scheme, locally of finite presentation and separated over S. (Grothendieck, FGA, Exp. 232.)

(ii) If f is flat and projective with geometrically reduced fibres, such that all irreducible components of the fibres of f are geometrically irreducible then $\mathrm{Pic}_{X/S}$ is representable by a scheme, locally of finite presentation (but not necessarily separated) over S. (Mumford, unpublished.)

(iii) If $S = \mathrm{Spec}(k)$ is the spectrum of a field and f is proper then $\mathrm{Pic}_{X/S}$ is representable by a scheme that is separated and locally of finite type over k. (Murre [1], using a theorem of Oort [1] to reduce to the case that X is reduced.)

If we further weaken the assumptions on f, e.g., if in (ii) we omit the condition that the irreducible components of the fibres are geometrically irreducible, then we may in general only hope for $\mathrm{Pic}_{X/S}$ to be representable by an algebraic space over S. Also if we only assume X/S to be proper, not necessarily projective, then in general $\mathrm{Pic}_{X/S}$ will be an algebraic space rather than a scheme. For instance, in Grothendieck's FGA, Exp. 236 we find the following criterion.

(iv) If $f\colon X \to S$ is proper and locally of finite presentation with geometrically integral fibres then $\mathrm{Pic}_{X/S}$ is a separated algebraic space over S.

We refer to ??, ?? for further discussion.

MaxTrivRem **(6.4) Remark.** Let X be a complete variety over a field k, let Y be a k-scheme and let L be a line bundle on $X \times Y$. The existence of maximal closed subscheme $Y_0 \hookrightarrow Y$ over which L is trivial, as claimed in Proposition (2.4), is an immediate consequence of the existence of $\mathrm{Pic}_{X/k}$. Namely, the line bundle L gives a morphism $Y \to \mathrm{Pic}_{X/k}$ and Y_0 is simply the fibre over the zero section of $\mathrm{Pic}_{X/k}$ under this morphism. (We use the exact sequence (1); as remarked earlier this does not require the existence of a rational point on X.)

Let us now turn to some basic properties of $\mathrm{Pic}_{X/S}$ in case it is representable. Note that $\mathrm{Pic}_{X/S}$ comes with the structure of an S-group scheme, so that the results and definitions of Chapter 3 apply.

LiePic **(6.5) Proposition.** *Assume that $f\colon X \to S$ is proper, flat and of finite presentation, with geometrically integral fibres. As discussed above, $\mathrm{Pic}_{X/S}$ is a separated algebraic space over S. (Those who wish to avoid algebraic spaces might add the hypothesis that f is projective, as in that case $\mathrm{Pic}_{X/S}$ is a scheme.)*

(i) Write $\mathscr{T}$ for the relative tangent sheaf of $\mathrm{Pic}_{X/S}$ over S. Then the sheaf $e^*\mathscr{T}$ ("the tangent space of $\mathrm{Pic}_{X/S}$ along the zero section") is canonically isomorphic to $R^1 f_* O_X$.

(ii) Assume moreover that f is smooth. Then every closed subscheme $Z \hookrightarrow \mathrm{Pic}_{X/S}$ which is of finite type over S is proper over S.

For a proof of this result we refer to BLR, Chap. 8.

LiePicCor **(6.6) Corollary.** *Let X be a proper variety over a field k.*

(i) *The tangent space of $\mathrm{Pic}_{X/S}$ at the identity element is isomorphic to $H^1(X, O_X)$. Further, $\mathrm{Pic}^0_{X/S}$ is smooth over k if and only if $\dim \mathrm{Pic}^0_{X/S} = \dim H^1(X, O_X)$, and this always holds if $\mathrm{char}(k) = 0$.*

(ii) *If X is smooth over k then all connected components of $\mathrm{Pic}_{X/k}$ are complete.*

Proof. This is immediate from (6.5) and the results discussed in Chapter 3 (notably (3.17) and (3.20)). As we did not prove (6.5), let us here give a direct explanation of why the tangent space of $\mathrm{Pic}_{X/S}$ at the identity element is isomorphic to $H^1(X, O_X)$, and why the components of $\mathrm{Pic}_{X/k}$ are complete.

Let $S = \mathrm{Spec}\big(k[\varepsilon]\big)$, where $k[\varepsilon]$ is the ring of dual numbers over k. Note that X and X_S have the same underlying topological space. On this space we have a short exact sequence of sheaves

$$0 \longrightarrow O_X \xrightarrow{h} O^*_{X_S} \xrightarrow{\mathrm{res}} O^*_X \longrightarrow 1$$

where h is given on sections by $f \mapsto \exp(\varepsilon f) = 1 + \varepsilon f$ and where res is the natural restriction map. On cohomology in degree zero this gives the exact sequence

$$0 \longrightarrow k \longrightarrow k[\varepsilon]^* \longrightarrow k^* \longrightarrow 1$$

where the maps are given by $f \mapsto 1 + \varepsilon f$ and $a + \varepsilon b \mapsto a$. On cohomology in degree 1 we then find an exact sequence

DualAV1:Lie
$$0 \longrightarrow H^1(X, O_X) \xrightarrow{h} \mathrm{Pic}(X_S) \xrightarrow{\mathrm{res}} \mathrm{Pic}(X)\,. \tag{3}$$

Concretely, if $\gamma \in H^1(X, O_X)$ is represented, on some open covering $\mathfrak{U} = \{U_\alpha\}_{\alpha \in A}$, by a Čech 1-cocyle $\{f_{\alpha\beta} \in O_X(U_\alpha \cap U_\beta)\}$ then $h(\gamma)$ is the class of the line bundle on X_S which is trivial on each U_α (now to be viewed as an open subset of X_S) and with transition functions $1 + \varepsilon f_{\alpha\beta}$.

Write T for the tangent space of $\mathrm{Pic}_{X/k}$ at the identity element. We can descibe T as the kernel of the restriction map $\mathrm{Pic}_{X/k}(S) \to \mathrm{Pic}_{X/k}(k)$; see Exercise 1.2. If $\gamma \in H^1(X, O_X)$ then $h(\gamma)$ restricts to the trivial class on X. Hence γ defines an element of T, and this gives a linear map $\xi\colon H^1(X, O_X) \to T$. As $\mathrm{Pic}(S) = \{1\}$ it follows from the exact sequences (1) and (3) that ξ is injective.

So far we have not used anything about X. To prove that ξ is also surjective it suffices to show that $\dim\big(H^1(X, O_X)\big) = \dim(T)$. Both numbers do not change if we extend the ground

field. Without loss of generality we may therefore assume that $X(k)$ is non-empty, so that assumptions $(*)$ in (6.2) are satisfied. Then the surjectivity of the map ξ follows from the exact sequence (2). This proves that $H^1(X, O_X) \xrightarrow{\sim} T$.

Next let us explain why the components of $\mathrm{Pic}_{X/S}$ are complete. We already know that $\mathrm{Pic}_{X/S}$ is a group scheme, locally of finite type over k. By Propositions (3.12) and (3.17), all connected components are separated and of finite type over k. To show that they are complete, we may extend the ground field; hence we can again assume that the assumptions $(*)$ in (6.2) are satisfied. In this situation we apply the valuative criterion for properness. Let R be a k-algebra which is a dvr. Let K be its fraction field, and suppose we have a K-valued point of $\mathrm{Pic}_{X/k}$, say represented by a line bundle L on X_K. We want to show that L extends to a line bundle on X_R. Since X/k is smooth, L is represented by a Weil divisor. But if $P \subset X_K$ is any prime divisor then the closure of P inside X_R is a prime divisor of X_R. It follows that L extends to a line bundle on X_R. □

PicNotRedRem **(6.7) Remark.** If $\mathrm{char}(k) = p > 0$ then $\mathrm{Pic}_{X/k}$ is in general not reduced, even if X is smooth and proper over k. An example illustrating this will be given in (7.31) below.

JacDef **(6.8)** Let C be a complete curve over a field k. Then $\mathrm{Pic}_{C/k}$ is a group scheme, locally of finite type over k; see (6.3). We claim that $\mathrm{Pic}_{C/k}$ is smooth over k. To see this we may extend the ground field and assume that $C(k) \neq \emptyset$, so that the assumptions $(*)$ in (6.2) are satisfied. Because $\mathrm{Pic}_{C/k}$ is locally of finite type over k, it suffices to show that any point of $\mathrm{Pic}_{C/k}$ with values in $R_0 := k[t]/(t^n)$ can be lifted to a point with values in $R := k[t]/(t^{n+1})$. But if we have a line bundle L_0 on $C \otimes_k R_0$ then the obstruction for extending L_0 to a line bundle on $C \otimes_k R$ lies in $H^2(C, O_C)$, which is zero because C is a curve.

In particular, we find that the identity component $\mathrm{Pic}^0_{C/k}$ is a group variety over k. If in addition we assume that C is smooth then by Cor. (6.6) $\mathrm{Pic}^0_{C/k}$ is complete, and is therefore an abelian variety. In this case we usually write $\mathrm{Jac}(C)$ for $\mathrm{Pic}^0_{C/k}$; it is called the *Jacobian* of C. Jacobians will be further discussed in Chapter 14. We remark that the term "Jacobian of C", for a complete and smooth curve C/k, usually refers to the abelian variety $\mathrm{Jac}(C) := \mathrm{Pic}^0_{C/k}$ together with its natural principal polarisation.

AlgEqDiv **(6.9) Remark.** Suppose X is a smooth proper variety over an algebraically closed field k. Recall that two divisors D_1 and D_2 are said to be algebraically equivalent (notation $D_1 \sim_{\mathrm{alg}} D_2$) if there exist (i) a smooth k-variety T, (ii) codimension 1 subvarieties $Z_1, \ldots, Z_n$ of $X \times_k T$ which are flat over T, and (iii) points $t_1, t_2 \in T(k)$, such that $D_1 - D_2 = \sum_{i=1}^n (Z_i)_{t_1} - (Z_i)_{t_2}$ as divisors on X; here $(Z_i)_t := Z_i \cap (X \times \{t\})$, viewed as a divisor on X. Translating this to line bundles we find that $D_1 \sim_{\mathrm{alg}} D_2$ precisely if the classes of $L_1 = O_X(D_1)$ and $L_2 = O_X(D_2)$ lie in the same connected component of $\mathrm{Pic}_{X/k}$. (Note that the components of the reduced scheme underlying $\mathrm{Pic}_{X/k}$ are smooth k-varieties.) The discrete group $\pi_0(\mathrm{Pic}_{X/k}) = \mathrm{Pic}_{X/k}/\mathrm{Pic}^0_{X/k}$ is therefore naturally isomorphic to the *Néron-Severi group* $\mathrm{NS}(X) := \mathrm{Div}(X)/\sim_{\mathrm{alg}}$. For a more precise treatment, see section (7.24).

§2. *Digression on graded bialgebras.*

In our study of duality, we shall make use of a structure result for certain graded bialgebras.

Before we can state this result we need to set up some definitions.

Let k be a field. (Most of what follows can be done over more general ground rings; for our purposes the case of a field suffices.) Consider a graded k-module $H^\bullet = \oplus_{n\geqslant 0} H^n$. An element $x \in H^\bullet$ is said to be homogeneous if it lies in H^n for some n, in which case we write $\deg(x) = n$. By a graded k-algebra we shall mean a graded k-module $H^\bullet$ together with a unit element $1 \in H^0$ and an algebra structure map (multiplication) $\gamma\colon H^\bullet \otimes_k H^\bullet \to H^\bullet$ such that

(i) the element 1 is a left and right unit for the multiplication;

(ii) the multiplication γ is associative, i.e., $\gamma(x, \gamma(y, z)) = \gamma(\gamma(x, y), z)$ for all x, y and z;

(iii) the map γ is a morphism of graded k-modules, i.e., it is k-linear and for all homogeneous elements x and y we have that $\gamma(x, y)$ is homogeneous of degree $\deg(x) + \deg(y)$.

If no confusion arises we shall simply write xy for $\gamma(x, y)$.

A homomorphism between graded k-algebras $H_1^\bullet$ and $H_2^\bullet$ is a k-linear map $f\colon H_1^\bullet \to H_2^\bullet$ which preserves the gradings, with $f(1) = 1$ and such that $f(xy) = f(x)f(y)$ for all x and y in $H_1^\bullet$.

We say that the graded algebra $H^\bullet$ is graded-commutative if

$$xy = (-1)^{\deg(x)\deg(y)} yx$$

for all homogeneous $x, y \in H^\bullet$. (In some literature this is called anti-commutativity, or sometimes even commutativity.) The algebra $H^\bullet$ is said to be connected if $H^0 = k \cdot 1$; it is said to be of finite type over k if $\dim_k(H^n) < \infty$ for all n (which is weaker than saying that $H^\bullet$ is finite-dimensional).

If $H_1^\bullet$ and $H_2^\bullet$ are graded k-algebras then the graded k-module $H_1^\bullet \otimes_k H_2^\bullet$ inherits the structure of a graded k-algebra: for homogeneous elements $x, \xi \in H_1^\bullet$ and $y, \eta \in H_2^\bullet$ one sets $(x \otimes y) \cdot (\xi \otimes \eta) = (-1)^{\deg(y)\deg(\xi)} \cdot (x\xi \otimes y\eta)$. As an exercise the reader may check that $H^\bullet$ is graded-commutative if and only if the map $\gamma\colon H^\bullet \otimes H^\bullet \to H^\bullet$ is a homomorphism of graded k-algebras. The field k itself shall be viewed as a graded k-algebras with all elements of degree zero.

GrHopfDef **(6.10) Definition.** A *graded bialgebra over k* is a graded k-algebra $H^\bullet$ together with two homomorphisms of k-algebras

$$\begin{aligned} \mu\colon H^\bullet \to H^\bullet \otimes_k H^\bullet \qquad & \text{called co-multiplication,} \\ \varepsilon\colon H^\bullet \to k \qquad & \text{the identity section,} \end{aligned}$$

such that

$$(\mu \otimes \mathrm{id}) \circ \mu = (\mathrm{id} \otimes \mu) \circ \mu\colon H^\bullet \to H^\bullet \otimes_k H^\bullet \otimes_k H^\bullet$$

and

$$(\varepsilon \otimes \mathrm{id}) \circ \mu = (\mathrm{id} \otimes \varepsilon) \circ \mu\colon H^\bullet \to H^\bullet$$

(using the natural identifications $H^\bullet \otimes_k k = H^\bullet = k \otimes_k H^\bullet$).

GrHopfExa **(6.11) Examples.** (i) If all elements of $H^\bullet$ have degree zero, i.e., $H^\bullet = H^0$, then we can ignore the grading and we "almost" find back the definition of a Hopf algebra as in (3.9). The main distinction between Hopf algebras and bialgebras is that for the latter we do not require an antipode.

(ii) If V is a vector space over k then we can form the exterior algebra $\wedge^\bullet V = \oplus_{n\geqslant 0} \wedge^n V$. The multiplication is given by the "exterior product", i.e.,

$$(x_1 \wedge \cdots \wedge x_r) \cdot (y_1 \wedge \cdots \wedge y_s) = x_1 \wedge \cdots \wedge x_r \wedge y_1 \wedge \cdots \wedge y_s \,.$$

By definition we have $\wedge^0 V = k$.

A k-linear map $V_1 \to V_2$ induces a homomorphism of graded algebras $\wedge^\bullet V_1 \to \wedge^\bullet V_2$. Furthermore, there is a natural isomorphism $\wedge^\bullet(V \oplus V) \xrightarrow{\sim} (\wedge^\bullet V) \otimes (\wedge^\bullet V)$. Therefore, the diagonal map $V \to V \oplus V$ induces a homomorphism $\mu\colon \wedge^\bullet V \to \wedge^\bullet V \otimes \wedge^\bullet V$. Taking this as co-multiplication, and defining $\varepsilon\colon \wedge^\bullet V \to k$ to be the projection onto the degree zero component we obtain the structure of a graded bialgebra on $\wedge^\bullet V$.

(iii) If $H_1^\bullet$ and $H_2^\bullet$ are two graded bialgebras over k then $H_1^\bullet \otimes_k H_2^\bullet$ naturally inherits the structure of a graded bialgebra; if $a \in H_1^\bullet$ with $\mu_1(a) = \sum x_i \otimes \xi_i$ and $b \in H_2^\bullet$ with $\mu_2(b) = \sum y_j \otimes \eta_j$ then the co-multiplication $\mu = \mu_1 \otimes \mu_2$ is described by

$$\mu(a \otimes b) = \sum_{i,j} (-1)^{\deg(y_j)\deg(\xi_i)} (x_i \otimes y_j) \otimes (\xi_i \otimes \eta_j) \,.$$

(iv) Let $x_1, x_2, \ldots$ be indeterminates. We give each of them a degree $d_i = \deg(x_i) \geqslant 1$ and we choose $s_i \in \mathbb{Z}_{\geqslant 2} \cup \{\infty\}$. Then we can define a graded-commutative k-algebra $H^\bullet = k\langle x_1, x_2, \ldots\rangle$ generated by the x_i, subject to the conditions $x_i^{s_i} = 0$. Namely, we take the monomials

$$m = x_1^{r_1} x_2^{r_2} \cdots \qquad (r_i \neq 0 \text{ for finitely many } i)$$

as a k-basis, with $\deg(m) = r_1 d_1 + r_2 d_2 + \cdots$, and where we set $x_i^{s_i} = 0$. Then there is a unique graded-commutative multiplication law such that $\gamma(x_i, x_j) = x_i x_j$ for $i \leqslant j$, and with this multiplication $k\langle x_1, x_2, \ldots\rangle$ becomes a graded k-algebra. Note that $k\langle x_1, x_2, \ldots x_N\rangle$ is naturally isomorphic to $k\langle x_1\rangle \otimes_k \cdots \otimes k\langle x_N\rangle$.

It is an interesting question whether $k\langle x_1, x_2, \ldots\rangle$ can have the structure of a bialgebra. It turns out that the existence of such a structure imposes conditions on the numbers d_i and s_i. Let us first do the case of one generator; the case of finitely many generators will follow from this together with Borel's theorem to be discussed next. So, we consider a graded k-algebra $H^\bullet = k\langle x \mid x^s = 0\rangle$ with $\deg(x) = d > 0$. Suppose that $H^\bullet$ has the structure of a bialgebra. Then:

	conditions on s:
$\mathrm{char}(k) = 0$, d odd	$s = 2$
$\mathrm{char}(k) = 0$, d even	$s = \infty$
$\mathrm{char}(k) = 2$	either $s = \infty$ or $s = 2^n$ for some n
$\mathrm{char}(k) = p > 2$, d odd	$s = 2$
$\mathrm{char}(k) = p > 2$, d even	either $s = \infty$ or $s = p^n$ for some n

For a proof of this result (in fact a more general version of it) we refer to Milnor and Moore [1], § 7. Note that the example given in (ii) is of the form $k\langle x_1, x_2, \ldots\rangle$ where all x_i have $d_i = 1$ and $s_i = 2$.

BorelHopf **(6.12) Theorem.** (Borel-Hopf structure theorem) *Let $H^\bullet$ be a connected, graded-commutative bialgebra of finite type over a perfect field k. Then there exist graded bialgebras $H_i^\bullet$ $(i = 1, \ldots, r)$ and an isomorphism of bialgebras*

$$H^\bullet \cong H_1^\bullet \otimes_k \cdots \otimes_k H_r^\bullet$$

such that the algebra underlying $H_i^\bullet$ is generated by one element, i.e., the algebras $H_i^\bullet$ are of the form $k\langle x_i \mid x_i^{s_i} = 0\rangle$, with $\deg(x_i) = d_i > 0$.

For a proof of this result, which is due to A. Borel, we refer to Borel [1] or Milnor and Moore [1].

BorHCor **(6.13) Corollary.** *Let $H^\bullet$ be as in* (6.12)*. Assume there is an integer g such that $H^n = (0)$ for all $n > g$. Then $\dim_k(H^1) \leqslant g$. If $\dim_k(H^1) = g$ then $H^\bullet \cong \wedge^\bullet H^1$ as graded bialgebras.*

Proof. Decompose $H^\bullet = H_1^\bullet \otimes_k \cdots \otimes_k H_r^\bullet$ as in (6.12). Note that $\dim_k(H^1)$ equals the number of generators x_i such that $d_i = 1$. Now $x_1 \cdots x_r$ ($:= x_1 \otimes \cdots \otimes x_r$) is a nonzero element of $H^\bullet$ of degree $d_1 + \cdots + d_r$. Therefore $d_1 + \cdots + d_r \leqslant g$, which implies $\dim_k(H^1) \leqslant g$. Next suppose $\dim_k(H^1) = g$, so that all generators x_i have degree 1. If $x_i^2 \neq 0$ for some i then $x_1 \cdots x_{i-1} x_i^2 x_{i+1} \cdots x_g$ is a nonzero element of degree $g+1$, contradicting our assumptions. Hence $x_i^2 = 0$ for all i which means that $H^\bullet \cong \wedge^\bullet H^1$. □

BorHAppl **(6.14)** Let us now turn to the application of the above results to our study of abelian varieties. Given a g-dimensional variety X over a field k, consider the graded k-module

$$H^\bullet = H^\bullet(X, O_X) := \bigoplus_{n=0}^{g} H^n(X, O_X)\,.$$

Cup-product makes $H^\bullet$ into a graded-commutative k-algebra, which is connected since X is connected.

In case X is a group variety the group law induces on $H^\bullet$ the structure of a graded bialgebra. Namely, via the Künneth formula $H^\bullet(X \times_k X, O_{X\times X}) \cong H^\bullet(X, O_X) \otimes_k H^\bullet(X, O_X)$ (which is an isomorphism of graded k-algebras), the group law $m\colon X \times_k X \to X$ induces a co-multiplication

$$\mu\colon H^\bullet \to H^\bullet \otimes_k H^\bullet\,.$$

For the identity section $\varepsilon\colon H^\bullet \to k$ we take the projection onto the degree zero component, which can also be described as the map induced on cohomology by the unit section $e\colon \operatorname{Spec}(k) \to X$. Now the statement that these μ and e make $H^\bullet$ into a graded bialgebra over k becomes a simple translation of the axioms in (1.2) satisfied by m and e.

As a first application of the above we thus find the estimate $\dim_k(H^1(X, O_X)) \leqslant g$ for a g-dimensional group variety X over a field k. (Note that $\dim_k(H^1(X, O_X))$ does not change if we pass from k to an algebraic closure; we therefore need not assume k to be perfect.) For abelian varieties we shall prove in (6.18) below that we in fact have equality.

We summarize what we have found.

DimEstim **(6.15) Proposition.** *Let X be a group variety over a field k. Then $H^\bullet(X, O_X)$ has a natural structure of a graded k-bialgebra. We have $\dim_k(H^1(X, O_X)) \leqslant \dim(X)$.*

To conclude this digression on bialgebras, let us introduce one further notion that will be useful later.

PrimEltDef **(6.16) Definition.** Let $H^\bullet$ be a graded bialgebra with comultiplication $\mu\colon H^\bullet \to H^\bullet \otimes_k H^\bullet$. Then an element $h \in H^\bullet$ is called a *primitive* element if $\mu(h) = h \otimes 1 + 1 \otimes h$.

PrimEltLem **(6.17) Lemma.** *Let V be a finite dimensional k vector space, and consider the exterior algebra $\wedge^\bullet V$ as in (6.11). Then $V = \wedge^1 V \subset \wedge^\bullet V$ is the set of primitive elements in $\wedge^\bullet V$.*

Proof. We follow Serre [1]. Since the co-multiplication μ is degree-preserving, an element of a graded bialgebra $H^\bullet$ is primitive if and only if all its homogeneous components are primitive. Thus we may restrict our attention to homogeneous elements of $\wedge^\bullet V$.

It is clear that the non-zero elements of $\wedge^0 V = k$ are not primitive. Further we see directly from the definitions that the elements of $\wedge^1 V = V$ are primitive. Let now $y \in \wedge^n V$ with $n \geqslant 2$. Write

$$[(\wedge^\bullet V) \otimes (\wedge^\bullet V)]^n = \bigoplus_{p+q=n} \wedge^p V \otimes \wedge^q V\,,$$

and write $\mu(y) = \sum \mu(y)^{p,q}$ with $\mu(y)^{p,q} \in \wedge^p V \otimes \wedge^q V$. For instance, one easily finds that $\mu(y)^{n,0} = y = \mu(y)^{0,n}$ via the natural identifications $\wedge^n V \otimes k = \wedge^n V = k \otimes \wedge^n V$. Similarly, we find that the map $y \mapsto \mu(y)^{1,n-1}$ is given (on decomposable tensors) by

$$v_1 \wedge \cdots \wedge v_n \mapsto \sum_{i=1}^{n} (-1)^{i+1} v_i \otimes (v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_n)\,.$$

It follows that for $\lambda \in V^*$ the composition $\wedge^n V \to V \otimes \wedge^{n-1} V \to \wedge^{n-1} V$ given by $y \mapsto (\lambda \otimes \mathrm{id})(\mu(y)^{1,n-1})$ is just the interior contraction $y \mapsto y \lrcorner \lambda$. The assumption that y is primitive and $n \geqslant 2$ implies that $\mu(y)^{1,n-1} = 0$ so we find $y \lrcorner \lambda = 0$ for all $\lambda \in V^*$. This only holds for $y = 0$. □

§3. *The dual of an abelian variety.*

From now on, let $\pi\colon X \to S = \mathrm{Spec}(k)$ be an abelian variety over a field k. We shall admit from the general theory that $\mathrm{Pic}_{X/k}$ is a group scheme over k with projective connected components. One of the main results of this section is that $\mathrm{Pic}^0_{X/k}$ is reduced, and is therefore again an abelian variety.

Note that $\mathrm{Pic}_{X/k}$ also represents the functor $P_{X/k,0}$ of line bundles with rigidification along the zero section. As above, the identification between the two functors is given by sending the class of a line bundle L on $X \times_k T$ to the class of $L \otimes \mathrm{pr}_T^* e^* L^{-1}$ with its canonical rigidification along $\{0\} \times T$. (In order to avoid the notation 0^*L we write e for the zero section of X_T.) In particular, we have a Poincaré bundle $\mathscr{P}$ on $X \times_k \mathrm{Pic}_{X/k}$ together with a rigidification $\alpha\colon O_{\mathrm{Pic}_{X/k}} \xrightarrow{\sim} \mathscr{P}_{|\{0\}\times \mathrm{Pic}_{X/k}}$.

If L is a line bundle on X we have the associated Mumford bundle $\Lambda(L)$ on $X \times X$. In order to distinguish the two factors X, write $X^{(1)} = X \times \{0\}$ and $X^{(2)} = \{0\} \times X$. Viewing $\Lambda(L)$ as a family of line bundles on $X^{(1)}$ parametrised by $X^{(2)}$ we obtain a morphism

$$\varphi_L\colon X = X^{(2)} \longrightarrow \mathrm{Pic}_{X/k}$$

which is the unique morphism with the property that $(\mathrm{id}_X \times \varphi_L)^* \mathscr{P} \cong \Lambda(L)$. On points, the morphism φ_L is of course given by $x \mapsto [t_x^* L \otimes L^{-1}]$, just as in (2.10). We have seen in (2.10), as a consequence of the Theorem of the Square, that φ_L is a homomorphism. Further we note that φ_L factors through $\mathrm{Pic}^0_{X/k}$, as X is connected and $\varphi_L(0) = 0$.

PicReduced **(6.18) Theorem.** *Let X be an abelian variety over a field k. Then $\mathrm{Pic}^0_{X/k}$ is reduced, hence it is an abelian variety. For every ample line bundle L the homomorphism $\varphi_L\colon X \to \mathrm{Pic}^0_{X/k}$ is an isogeny with kernel $K(L)$. We have $\dim(\mathrm{Pic}^0_{X/k}) = \dim(X) = \dim_k H^1(X, O_X)$.*

Proof. Let L be an ample line bundle on X. By Lemma (2.17), φ_L has kernel $K(L)$. Since $K(L)$ is a finite group scheme it follows that $\dim(\mathrm{Pic}^0_{X/k}) \geqslant \dim(X)$. Combining this with (6.6) and (6.15) we find that $\dim(\mathrm{Pic}^0_{X/k}) = \dim(X) = \dim_k H^1(X, O_X)$ and that $\mathrm{Pic}^0_{X/k}$ is reduced. □

DualAVDef **(6.19) Definition and Notation.** The abelian variety $X^t := \mathrm{Pic}^0_{X/k}$ is called the *dual* of X. We write $\mathscr{P}$, or $\mathscr{P}_X$, for the Poincaré bundle on $X \times X^t$ (i.e., the restriction of the Poincaré bundle on $X \times \mathrm{Pic}_{X/k}$ to $X \times X^t$). If $f\colon X \to Y$ is a homomorphism of abelian varieties over k then we write $f^t\colon Y^t \to X^t$ for the induced homomorphism, called the *dual* of f or the *transpose* of f. Thus, f^t is the unique homomorphism such that

$$(\mathrm{id} \times f^t)^* \mathscr{P}_X \cong (f \times \mathrm{id})^* \mathscr{P}_Y$$

as line bundles on $X \times Y^t$ with rigidification along $\{0\} \times Y^t$.

fftRem **(6.20) Remark.** We do not yet know whether $f \mapsto f^t$ is additive; in other words: if we have two homomorphisms $f, g\colon X \to Y$, is then $(f+g)^t$ equal to $f^t + g^t$? Similarly, is $(n_X)^t$ equal to n_{X^t} ? We shall later prove that the answer to both questions is "yes"; see (7.17). Note however that such relations certainly do not hold on all of $\mathrm{Pic}_{X/k}$; for instance, we know that if L is a line bundle with $(-1)^*L \cong L$ then $n^*L \cong L^{n^2}$ which is in general not isomorphic to L^n.

Exercises.

Ex:PXSnotRep **(6.1)** Show that the functor $P_{X/S}$ defined in §1 is *never* representable, at least if we assume X to be a non-empty scheme.

Ex:XxYdual **(6.2)** Let X and Y be two abelian varieties over a field k.

(i) Write $i_X\colon X \to X \times Y$ and $i_Y\colon Y \to X \times Y$ for the maps given by $x \mapsto (x, 0)$ and $y \mapsto (0, y)$, respectively. Show that the map $(i_X^t, i_Y^t)\colon (X \times Y)^t \to X^t \times Y^t$ that sends a class $[L] \in \mathrm{Pic}^0_{(X\times Y)/k}$ to $\big([L_{|X\times\{0\}}], [L_{|\{0\}\times Y}]\big)$, is an isomorphism. [*Note:* in general it is certainly not true that the full Picard scheme $\mathrm{Pic}_{X\times Y/k}$ is isomorphic to $\mathrm{Pic}_{X/k} \times \mathrm{Pic}_{Y/k}$.]

(ii) Write

$$p\colon X \times Y \times X^t \times Y^t \longrightarrow X \times X^t \quad \text{and} \quad q\colon X \times Y \times X^t \times Y^t \longrightarrow Y \times Y^t$$

for the projection maps. Show that the Poincaré bundle of $X \times Y$ is isomorphic to $p^*\mathscr{P}_X \otimes q^*\mathscr{P}_Y$.

Ex:(1phiL)*P **(6.3)** Let L be a line bundle on an abelian variety X. Consider the homomorphism $(1, \varphi_L)\colon X \to X \times X^t$. Show that $(1, \varphi_L)^*\mathscr{P}_X \cong L \otimes (-1)^*L$.

Ex:GrHopfEx **(6.4)** The goal of this exercise is to prove the restrictions listed in (iv) of (6.11). We consider a graded bialgebra $H^\bullet$ over a field k, with co-multiplication μ. We define the height of an element $x \in H^\bullet$ to be the smallest positive integer n such that $x^n = 0$, if such an n exists, and to be ∞ if x is not nilpotent.

(i) If $y \in H^\bullet$ is an element of odd degree, and $\mathrm{char}(k) \neq 2$, show that $y^2 = 0$.

(ii) If $x \in H^\bullet$ is primitive, show that $\mu(x^n) = \sum_{i=0}^{n} \binom{n}{i} x^i \otimes x^{n-i}$. Conclude that if x has height $n < \infty$ then $\mathrm{char}(k) = p > 0$ and n is a power of p.

(iii) If $H^\bullet = k\langle x \mid x^s = 0\rangle$ with $\deg(x) = d$, show that x is a primitive element. Deduce the restrictions on the height of x listed in (iv) of (6.11).

§1. *Formation of quotients and the descent of coherent sheaves.*

GrActonSh **(7.1) Definition.** Let S be a base scheme. Let $\rho\colon G \times_S X \to X$ be an action (from the left) of an S-group scheme G on an S-scheme X. Let F be a coherent sheaf of O_X-modules. Then an *action of G on F, compatible with the action ρ*, is an isomorphism $\lambda\colon \mathrm{pr}_2^*F \xrightarrow{\sim} \rho^*F$ of sheaves on $G \times_S X$, such that on $G \times_S G \times_S X$ we have a commutative diagram

$$\begin{array}{ccc} \mathrm{pr}_3^*F & \xrightarrow{\mathrm{pr}_{23}^*(\lambda)} & \mathrm{pr}_{23}^*\rho^*F \\ {\scriptstyle (m\times \mathrm{id}_X)^*(\lambda)}\downarrow & & \downarrow{\scriptstyle (\mathrm{id}_G\times\rho)^*(\lambda)} \\ (m\times \mathrm{id}_X)^*\rho^*F & = & (\mathrm{id}_G\times\rho)^*\rho^*F \end{array} .$$

Here is a more concrete explanation of what this means. If T is an S-scheme and $g \in G(T)$, write $\rho_g\colon X_T \to X_T$ for the action of the element g. Then to have an action of G on F that is compatible with ρ means that for every $g \in G(T)$ we have an isomorphism of sheaves $\lambda_g\colon F_T \xrightarrow{\sim} \rho_g^*F_T$ such that $\lambda_{gh} = \rho_h^*(\lambda_g)\circ\lambda_h$ for all g, $h \in G(T)$.

If F is a locally free O_X-module we can take a more geometric point of view. First recall that a locally free O_X-module is "the same" as a geometric vector bundle over X. Namely, $V := \mathbb{V}(F^\vee)$ is a geometric vector bundle over X, and F is the sheaf of sections of the structure morphism $\pi\colon V \to X$. Then a ρ-compatible G-action on F corresponds to an action $\tilde\rho\colon G\times_S V \to V$ such that (i) the structure morphism $\pi\colon V \to X$ is G-equivariant, and (ii) the action $\tilde\rho$ is "fibrewise linear", meaning that for every S-scheme T and every $g \in G(T)$, $x \in X(T)$, the isomorphism $\tilde\rho(g)\colon V_x \to V_{gx}$ is O_T-linear. We refer to such an action $\tilde\rho$ as a lifting of ρ.

With this notion of a G-action on a sheaf, we can formulate a useful result on the descent of modules.

ShQuot **(7.2) Proposition.** *Let $\rho\colon G \times_S X \to X$ be an action of an S-group scheme G on an S-scheme X. Suppose there exists an fppf quotient $p\colon X \to Y$ of X by G. If F is a coherent sheaf of O_Y-modules then the canonical isomorphism $\lambda_{\mathrm{can}}\colon \mathrm{pr}_2^*(p^*F) \xrightarrow{\sim} \rho^*(p^*F)$ defines a ρ-compatible G-action on p^*F. The functor $F \mapsto (p^*F, \lambda_{\mathrm{can}})$ gives an equivalence between the category of coherent O_Y-modules and the category of coherent O_X-modules with (ρ-compatible) G-action. This restricts to an equivalence between the category of finite locally free O_Y-modules and the category of finite locally free O_X-modules with G-action.*

This proposition should be seen as a statement in (faithfully flat) descent theory; it follows for instance from the results of SGA 1, Exp. VIII, § 1. (See also [BLR], § 6.1, Thm. 4.) Given such results in descent theory, the only point here is that a ρ-compatible G-action on a coherent O_X-module is *the same* as a descent datum on this module. (Recall that we have an isomorphism $(\rho, \mathrm{pr}_2)\colon G \times_S X \xrightarrow{\sim} X \times_Y X$.) The assertion that finite locally free O_X-modules with G-action give rise to finite locally free O_Y-modules follows from EGA IV, Prop. 2.5.2.

ShQuotExa **(7.3) Example.** We consider the situation of the proposition. The geometric vector bundle corresponding to the structure sheaf O_X is just the affine line $\mathbb{A}^1_X$ over X.

On O_X (geometrically: on $\mathbb{A}^1_X$) we have a "trivial" action $\tilde\rho_{\text{triv}}$, given by

$$\tilde\rho_{\text{triv}} = \rho \times \mathrm{id}_{\mathbb{A}^1_S} \colon G \times_S \mathbb{A}^1_X = G \times_S X \times_S \mathbb{A}^1_S \longrightarrow X \times_S \mathbb{A}^1_S = \mathbb{A}^1_X \,.$$

The O_Y-module corresponding to $(O_X, \tilde\rho_{\text{triv}})$ is just O_Y itself.

Let $\tilde\rho$ be some other lifting of ρ to a G-action on $\mathbb{A}^1_X$. Let T be an S-scheme and $g \in G(T)$. The automorphism $\tilde\rho(g) \cdot \tilde\rho_{\text{triv}}(g)^{-1}$ of $\mathbb{A}^1_X \times_S T = \mathbb{A}^1_{X_T}$ is given on every fibre $\mathbb{A}^1_x$ by some (invertible) scalar multiplication. This means that $\tilde\rho(g) \cdot \tilde\rho_{\text{triv}}(g)^{-1}$ is given by an element $\nu(g) \in \Gamma(X_T, O^*_{X_T})$. We find that an action $\tilde\rho$ gives rise to a morphism of functors $\nu\colon G \to \mathrm{Res}_{X/S}\mathbb{G}_{m,X}$ on the category $\mathsf{Sch}_{/S}$. The condition that $\tilde\rho$ is a group action means that ν satisfies a cocycle condition $\nu(g_1g_2)\big(x\big) = \nu(g_1)\big(g_2x\big)\cdot\nu(g_2)\big(x\big)$, where we simply write g_2x for $\rho(g_2)\big(x\big)$. Conversely, given a morphism $\nu\colon G \to \mathrm{Res}_{X/S}\mathbb{G}_{m,X}$ that satisfies this condition, one finds back a G-action $\tilde\rho$ by $\tilde\rho(g) = \nu(g)\cdot\tilde\rho_{\text{triv}}(g)$.

Now suppose that the structure morphism $f\colon X \to S$ satisfies $f_*(O_{X_T}) = O_T$ for all S-schemes T. This holds for instance if X is a proper variety over a field. Then $\mathrm{Res}_{X/S}\mathbb{G}_{m,X} \cong \mathbb{G}_{m,S}$ as functors on $\mathsf{Sch}_{/S}$. In particular, any morphism $\nu\colon G \to \mathrm{Res}_{X/S}\mathbb{G}_{m,X}$ is G-invariant, in the sense that for all g_1, $g_2 \in G(T)$ and $x \in X(T)$ we have $\nu(g_1)\big(g_2x\big) = \nu(g_1)\big(x\big)$. Hence the cocycle condition in this case just says that ν is a homomorphism. So the conclusion is that the liftings $\tilde\rho$ of ρ to a G-action on $\mathbb{A}^1_X$ are in bijective correspondence with $\mathrm{Hom}_{\mathsf{GSch}_{/S}}(G, \mathbb{G}_m)$. In case G is a commutative, finite locally free S-group scheme this is just the Cartier dual $G^D(S)$.

Via Proposition (7.2), we can use this to obtain a description of the line bundles L on Y such that $p^*L \cong O_X$. The result is as follows.

LBonQuot **(7.4) Proposition.** *Let G be a commutative, finite locally free S-group scheme. Let $\rho\colon G \times_S X \to X$ be a free action of G on an S-scheme X. Let $p\colon X \to Y$ be the quotient of X by G. Suppose that $f_*(O_{X_T}) = O_T$ for all S-schemes T. Then for any S-scheme T there is a canonical isomorphism of groups*

$$\delta_T\colon \begin{pmatrix}\text{isomorphism classes of line bundles}\\ L \text{ on } Y_T \text{ with } p^*L \cong O_{X_T}\end{pmatrix} \xrightarrow{\sim} G^D(T)\,,$$

and this isomorphism is compatible with base change $T' \to T$.

Proof. To define δ_T for arbitrary S-schemes T we may replace S by T and $p\colon X \to Y$ by $p_T\colon X_T \to Y_T$. Note that by Theorem (4.16) and what was explained in Example (4.29), p_T is again the quotient morphism of X_T by the action of G_T, and of course also the assumption that $f_*(O_{X_T}) = O_T$ for all S-schemes T is preserved under base change. Hence it suffices to define the isomorphism δ_S.

Let L be a line bundle on Y with $p^*L \cong O_X$. Via the choice of an isomorphism $\alpha\colon p^*L \xrightarrow{\sim} O_X$ (or, more geometrically, the isomorphism $\alpha\colon p^*\mathbb{V}(L^{-1}) \xrightarrow{\sim} \mathbb{A}^1_X$ over X) the canonical G-action on p^*L translates into a G-action $\tilde\rho$ on $\mathbb{A}^1_X$, and as explained above this gives us a character $\nu\colon G \to \mathbb{G}_{m,S}$. We claim that this character is independent of the choice of α. In general, any other isomorphism $p^*L \xrightarrow{\sim} O_X$ is of the form $\alpha' = \gamma\circ\alpha$ for some $\gamma \in \Gamma(X, O^*_X)$. Write $\tilde\rho$ and $\tilde\rho'$ for the G-actions on $\mathbb{A}^1_X$ obtained using α and α', respectively, and let ν and ν' be the associated characters. If $g \in G(T)$ and y is a T-valued point of $p^*\mathbb{V}(L^{-1})$ lying over $x \in X(T)$ then we have the relations

$$\tilde\rho_{\text{triv}}\big(g, \alpha'(y)\big) = \gamma(x)\cdot\tilde\rho_{\text{triv}}\big(g, \alpha(y)\big) \quad\text{and}\quad \tilde\rho'\big(g, \alpha'(y)\big) = \gamma(gx)\cdot\tilde\rho\big(g, \alpha(y)\big)\,,$$

where $\gamma(x)$ is the image of γ under the homomorphism $\Gamma(X, O_X^*) \to \Gamma(T, O_T^*)$ induced by $x\colon T \to X$, and similarly for $\gamma(gx)$. (Note that elements such as $\tilde{\rho}\big(g, \alpha(y)\big)$ are T-valued points of $\mathbb{A}^1_X$ lying over the point $gx \in X(T)$, and on such elements we have the "fibrewise" multiplication by functions on T.) But now our assumption that $f_*(O_X) = O_S$ implies that γ is the pull-back of an element in $\Gamma(S, O_S^*)$, so $\gamma(x) = \gamma(gx)$. Hence $\nu = \nu'$, as claimed.

Now we can simply apply the conclusion from (7.3), and define δ_S as the map that sends the isomorphism class of L to the character $\nu\colon G \to \mathbb{G}_{m,S}$ given on points by $\nu(g) = \tilde{\rho}(g) \cdot \tilde{\rho}_{\mathrm{triv}}(g)^{-1}$. By Proposition (7.2), together with what was explained in Example (7.3), the map δ_S thus obtained is indeed an isomorphism.

Finally we note that the maps δ_T are indeed compatible with base change, as is immediate from the construction. □

§2. *Two duality theorems.*

Duality1 **(7.5) Theorem.** *Let $f\colon X \to Y$ be an isogeny of abelian varieties. Then $f^t\colon Y^t \to X^t$ is again an isogeny and there is a canonical isomorphism of group schemes*

$$\mathrm{Ker}(f)^D \xrightarrow{\sim} \mathrm{Ker}(f^t)\,.$$

Proof. If T is a k-scheme, any class in $\mathrm{Ker}(f^t)(T)$ is uniquely represented by a line bundle L on Y_T such that $f^*L \cong O_{X_T}$. Indeed, if L' represents a class in $\mathrm{Ker}(f^t)(T)$ then there is a line bundle M on T such that $f^*L' \cong \mathrm{pr}_T^*M$. Then $L := L' \otimes \mathrm{pr}_T^*M^{-1}$ represents the same class as L' and satisfies $f^*L \cong O_{X_T}$. Conversely, if L_1 and L_2 represent the same class then they differ by a line bundle of the form pr_T^*M; hence $f^*L_1 \cong f^*L_2$ implies $L_1 \cong L_2$.

Applying Proposition (7.4) we obtain the desired isomorphism $\mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$. In particular this shows that f^t has a finite kernel and therefore is again an isogeny. □

PullbphiL **(7.6) Proposition.** *Let $f\colon X \to Y$ be a homomorphism. Let M be a line bundle on Y and write $L = f^*M$. Then $\varphi_L\colon X \to X^t$ equals the composition*

$$X \xrightarrow{f} Y \xrightarrow{\varphi_M} Y^t \xrightarrow{f^t} X^t\,.$$

If f is an isogeny and M is non-degenerate then L is non-degenerate too, and $\mathrm{rank}(K(L)) = \deg(f)^2 \cdot \mathrm{rank}(K(M))$.

Proof. That $\varphi_L = f^t \circ \varphi_M \circ f$ is clear from the formula $t_x^* f^*M = f^* t_{f(x)}^* M$. For the second assertion recall that a line bundle L is non-degenerate precisely if φ_L is an isogeny, in which case $\mathrm{rank}(K(L)) = \deg(\varphi_L)$. Now use (7.5). □

kappaXDef **(7.7)** The Poincaré bundle on $X \times X^t$ comes equipped with a rigidification along $\{0\} \times X^t$. As $\mathscr{P}_{|X\times\{0\}} \cong O_X$ we can also choose a rigidification of $\mathscr{P}$ along $X \times \{0\}$. Such a rigidification is unique up to an element of $\Gamma(X, O_X^*) = k^*$. Hence there is a unique rigidification along $X \times \{0\}$ such that the two rigidifications agree at the origin $(0, 0)$.

Now we view $\mathscr{P}$ as a family of line bundles on X^t parametrised by X. This gives a morphism

$$\kappa_X\colon X \longrightarrow X^{tt}\,.$$

As $\kappa_X(0) = 0$ it follows from Prop. (1.14) that κ_X is a homomorphism.

phiLtLem **(7.8) Lemma.** *Let L be a line bundle on X. Then $\varphi_L = \varphi_L^t \circ \kappa_X \colon X \to X^t$.*

Proof. Let $s\colon X \times X \to X \times X$ and $s\colon X \times X^t \to X^t \times X$ be the morphisms switching the two factors; on points: $s(x,y) = (y,x)$. We have a canonical isomorphism $s^*\Lambda(L) \cong \Lambda(L)$. Let T be a k-scheme and $x \in X(T)$. Writing $[M]$ for the class of a bundle M on $X \times T$ in $\mathrm{Pic}^0_{X/k}(T)$ we have

$$\begin{aligned}
\varphi_L(x) &= \Big[(X \times T \xrightarrow{\mathrm{id}\times x} X \times X)^*\Lambda(L)\Big] \\
&= \Big[(X \times T \xrightarrow{\mathrm{id}\times x} X \times X \xrightarrow{s} X \times X)^*\Lambda(L)\Big] \\
&= \Big[(X \times T \xrightarrow{\mathrm{id}\times x} X \times X \xrightarrow{s} X \times X \xrightarrow{\mathrm{id}\times\varphi_L} X \times X^t)^*\mathscr{P}\Big] \\
&= \Big[(X \times T \xrightarrow{\varphi_L\times\mathrm{id}} X^t \times T \xrightarrow{\mathrm{id}\times x} X^t \times X \xrightarrow{s} X \times X^t)^*\mathscr{P}\Big] = \varphi_L^t \circ \kappa_X(x)\,.
\end{aligned}$$

As this holds for all T and x the lemma is proven. □

Duality2 **(7.9) Theorem.** *Let X be an abelian variety over a field. Then the homomorphism $\kappa_X\colon X \longrightarrow X^{tt}$ is an isomorphism.*

Proof. Choose an ample line bundle L on X. The formula $\varphi_L = \varphi_L^t \circ \kappa_X$ shows that $\mathrm{Ker}(\kappa_X)$ is finite; hence κ_X is an isogeny. Furthermore,

$$\mathrm{rank}\big(K(L)\big) = \deg(\varphi_L) = \deg(\varphi_L^t)\cdot\deg(\kappa_X) = \mathrm{rank}\big(K(L)^D\big)\cdot\deg(\kappa_X)\,,$$

using (7.5). But $\mathrm{rank}\big(K(L)^D\big) = \mathrm{rank}\big(K(L)\big)$, so κ_X has degree 1. □

K(L)selfdual **(7.10) Corollary.** *If L is a non-degenerate line bundle on X then $K(L) \cong K(L)^D$.*

Proof. Apply (7.5) to φ_L and use (7.8) and (7.9). □

§3. *Further properties of* $\mathrm{Pic}^0_{X/k}$.

Let X be an abelian variety over a field k. A line bundle L on X gives rise to a homomorphism $\varphi_L\colon X \to X^t$. We are going to extend this construction to a more general situation. Namely, let T be a k-scheme, and suppose L is a line bundle on $X_T := X \times_k T$. We are going to associate to L a homomorphism $\varphi_L\colon X_T \to X_T^t$.

As usual we write $\Lambda(L) := m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$ for the Mumford bundle on $X_T \times_T X_T$ associated to L. (Note that we are working in the relative setting, viewing T as the base scheme. If we rewrite $X_T \times_T X_T$ as $X \times_k X \times_k T$ then $\Lambda(L)$ becomes $(m \times \mathrm{id}_T)^*L \otimes p_{13}^*L^{-1} \otimes p_{23}^*L^{-1}$.) In order to distinguish the two factors X_T, let us write $X_T^{(1)} = X_T \times_T e(T)$ and $X_T^{(2)} = e(T) \times_T X_T$ where $e(T) \subset X_T$ is the image of the zero section $e\colon T \to X_T$. Viewing $\Lambda(L)$ as a family of line bundles on $X_T^{(1)}$ parametrized by $X_T^{(2)}$ we obtain a morphism

$$\varphi_L\colon X_T = X_T^{(2)} \longrightarrow \mathrm{Pic}_{X_T/T} = \mathrm{Pic}_{X/k} \times_k T\,.$$

As $\varphi_L(0) = 0$ and the fibres X_t are connected, φ_L factors through $X_T^t = \mathrm{Pic}^0_{X/k} \times_k T$.

phiL/TLem **(7.11) Lemma.** (i) *The morphism φ_L only depends on the class of L in $\mathrm{Pic}_{X/k}(T)$.*

(ii) *Let $f\colon T \to S$ be a morphism of k-schemes. If M is a line bundle on X_S and $L = (\mathrm{id}_X \times f)^*M$ on X_T, then $\varphi_L\colon X_T \to X_T^t$ is the morphism obtained from $\varphi_M\colon X_S \to X_S^t$ by pulling back via f on the basis.*

(iii) *The morphism $\varphi_L\colon X_T \to X_T^t$ is a homomorphism.*

Part (i) of the lemma will be sharpened in (7.15) below. As a particular case of (ii), note that the fibre of φ_L above a point $t \in T$ is just φ_{L_t}, where we write L_t for the restriction of L to $X \times \{t\}$.

Proof. (i) If L_1 and L_2 have the same class then they differ by a factor pr_T^*M. But then $\Lambda(L_1)$ and $\Lambda(L_2)$ differ by a factor π^*M^{-1}, where $\pi\colon X_T \times_T X_T \to T$ is the structural morphism. This implies that $\varphi_{L_1} = \varphi_{L_2}$, as claimed.

(ii) This readily follows from the definitions.

(iii) The assertion that φ_L is a homomorphism means that we have an equality of two morphisms

$$\varphi_L \circ m = m \circ (\varphi_L \times \varphi_L)\colon X_T \times_T X_T \longrightarrow X_T^t\,.$$

For every $t \in T$ we already know that the two morphisms agree on the fibres above t. Hence the lemma is true if T is reduced. In particular, the lemma is true in the "universal" case that $T = \mathrm{Pic}_{X/k}$ and L is the Poincaré bundle on $X \times_k \mathrm{Pic}_{X/k}$. In the general case, consider the morphism $f\colon T \to \mathrm{Pic}_{X/k}$ associated to the line bundle L. This morphism is characterized by the property that L and $(\mathrm{id} \times f)^*\mathscr{P}$ have the same class in $\mathrm{Pic}_{X/k}(T)$. Now apply (i) and (ii). □

In the above we allow L—to be thought of as a family of line bundles on X parametrized by T—to be non-constant. But the abelian variety we work on is a constant one. We can go one step further by also letting the abelian varieties X_t "vary with t". This generalization will be discussed in Chapter ??; see in particular (?.?).

We write $K(L) := \mathrm{Ker}(\varphi_L) \subset X_T$. It is the maximal subscheme of X_T over which $\Lambda(L)$ is trivial, viewing $X_T \times_T X_T$ as a scheme over X_T via the second projection. In particular, $\varphi_L = 0$ if and only if $\Lambda(L)$ is trivial over X_T, meaning that $\Lambda(L) = \mathrm{pr}_2^*M$ for some line bundle M on X_T. Using (2.17) we can make this a little more precise.

phiLtriv **(7.12) Lemma.** *Let T be a locally noetherian k-scheme. Write $\pi\colon X_T \times_T X_T \to T$ for the structural morphism. For a line bundle L on X_T, consider the following conditions.*

(a) $\varphi_L = 0$.

(b) $\Lambda(L) \cong \mathrm{pr}_2^*M$ *for some line bundle M on X_T.*

(c) $\Lambda(L) \cong \pi^*N$ *for some line bundle N on T.*

(d) $\varphi_{L_t} = 0$ *for some $t \in T$.*

Then (a) ⇔ (b) ⇔ (c) ⇒ (d), *and if T is connected then all four conditions are equivalent. If these equivalent conditions are satisfied then $N \cong e^*L^{-1}$ and $M = \mathrm{pr}_T^*N$.*

Proof. The implications (d) ⇐ (a) ⇔ (b) ⇐ (c) are clear. Let us write $X_T \times_T X_T$ as $X \times_k X \times_k T$. In this notation we have $\Lambda(L) = (m \times \mathrm{id}_T)^*L \otimes p_{13}^*L^{-1} \otimes p_{23}^*L^{-1}$ and π becomes the projection onto the third factor. Set $N := e^*L^{-1}$. We find that

$$\Lambda(L)_{|\{0\}\times X\times T} \cong \mathrm{pr}_T^*N \cong \Lambda(L)_{|X\times\{0\}\times T}$$

as line bundles on $X \times T$.

Suppose T is connected and $\varphi_{L_t} = 0$ for some $t \in T$. Then

$$\Lambda(L)_{|X\times X\times\{t\}} \cong O_{X\times X\times\{t\}}$$

by (iii) of (2.17). By Thm. (2.5) the line bundle $\Lambda(L) \otimes p_3^* N^{-1}$ on $X \times X \times T$ is trivial, i.e., $\Lambda(L) \cong \pi^* N$. This shows that (d) $\Rightarrow$ (a) for connected T. For arbitrary T we get the implication (a) $\Rightarrow$ (c) by applying the previous to each of its connected components.

The last assertion of the lemma is obtained by restricting $\Lambda(L)$ to $\{0\} \times \{0\} \times T$ and to $\{0\} \times X \times T$. □

HomFact **(7.13) Fact.** *Let X and Y be two projective varieties over a field k. Then the contravariant functor*

$$\mathit{Hom}_{\mathsf{Sch}}(X,Y)\colon (\mathsf{Sch}_{/k}) \to \mathsf{Sets} \quad \text{given by} \quad T \mapsto \mathrm{Hom}_{\mathsf{Sch}_{/T}}(X_T, Y_T)$$

is representable by a k-scheme, locally of finite type.

This fact is a consequence of the theory of Hilbert schemes. A reference is ??. Note that in this proof the projectivity of X and Y is used in an essential way. See also Matsumura-Oort [1] for related results for non-projective varieties.

HomAVProp **(7.14) Proposition.** *Let X and Y be two abelian varieties over a field k. Then the functor*

$$\mathit{Hom}_{\mathsf{AV}}(X,Y)\colon (\mathsf{Sch}_{/k}) \to \mathsf{Ab} \quad \text{given by} \quad T \mapsto \mathrm{Hom}_{\mathsf{GSch}_{/T}}(X_T, Y_T)$$

is representable by an étale commutative k-group scheme.

Proof. Let $H = \mathit{Hom}_{\mathsf{Sch}}(X,Y)$ and $H' = \mathit{Hom}_{\mathsf{Sch}}(X\times X, Y)$. Let $f\colon X_H \to Y_H$ be the universal morphism. Consider the morphism $g\colon (X\times X)_H \to Y_H$ given on points by $g(x_1,x_2) = f(x_1 + x_2) - f(x_1) - f(x_2)$. Consider also the "trivial" morphism $e\colon (X\times X)_H \to Y_H$ given on points by $e(x_1,x_2) = e_Y$. Then g and e are H-valued points of H'; in other words, they correspond to morphisms ψ_g, $\psi_e\colon H \to H'$. The functor $\mathit{Hom}_{\mathsf{AV}}(X,Y)$ is represented by the subscheme of H given by the condition that $\psi_g = \psi_e$; in other words, it is given by the cartesian diagram

$$\begin{array}{ccc} \mathit{Hom}_{\mathsf{AV}}(X,Y) & \longrightarrow & H' \\ \big\downarrow & & \big\downarrow{\scriptstyle \Delta_{H'/k}} \\ H & \xrightarrow{(\psi_g,\psi_e)} & H' \times_k H' \end{array} .$$

To get a group scheme structure on $\mathit{Hom}_{\mathsf{AV}}(X,Y)$ we just note that $\mathit{Hom}_{\mathsf{AV}}(X,Y)$ is naturally a group functor; now apply (3.6).

It remains to be shown that $\mathit{Hom}_{\mathsf{AV}}(X,Y)$ is an étale group scheme. We already know it is locally of finite type over k, so it suffices to show that its tangent space at the origin is trivial. It suffices to prove this in the special case that $Y = X$, for $\mathit{Hom}_{\mathsf{AV}}(X,Y)$ embeds as a closed subgroup scheme of $\mathscr{E}\mathit{nd}_{\mathsf{AV}}(X\times Y) := \mathit{Hom}_{\mathsf{AV}}(X\times Y, X\times Y)$ by sending $f\colon X \to Y$ to the endomorphism $(x,y) \mapsto \big(0, f(x)\big)$ of $X \times Y$.

A tangent vector of $\mathscr{E}\mathit{nd}_{\mathsf{AV}}(X)$ at the point id_X is the same as a homomorphism $\xi\colon X_{k[\varepsilon]} \to X_{k[\varepsilon]}$ over $\mathrm{Spec}\big(k[\varepsilon]\big)$ that reduces to the identity modulo ε. Note that ξ is necessarily an automorphism. (It is the identity on underlying topological spaces, and it is an easy exercise to show that ξ gives an automorphism of the structure sheaf.) Hence by the results in Exercise (1.2), ξ corresponds to a global vector field Ξ on X. As we know, the global vector fields on X are

precisely the translation-invariant vector fields. On the other hand, a necessary condition for ξ to be an endomorphism is that it maps the identity section of $X_{k[\varepsilon]}$ to itself. This just means that $\Xi(e_X) = 0$. Hence Ξ is the trivial vector field. This shows that id_X has non non-trivial first order deformations. □

In line with the notational conventions introduced in (1.17), we shall usually simply write $Hom(X, Y)$ for the group scheme of homomorphisms from X to Y. If we wish to refer to the bigger scheme of arbitrary scheme morphisms from X to Y, or if there is a risk of confusion, we shall use a subscript "AV" or "Sch" to indicate which of the two we mean.

By (i) and (ii) of Lemma (7.11), $L \mapsto \varphi_L$ gives rise to a morphism of functors $\varphi\colon \mathrm{Pic}_{X/k} \to Hom(X, X^t)$. If L and M are line bundles on X_T then $\Lambda(L \otimes M) \cong \Lambda(L) \otimes \Lambda(M)$ and we find that $\varphi_{L\otimes M} = \varphi_L + \varphi_M$. Summing up, we obtain a homomorphism of k-group schemes

$$\varphi\colon \mathrm{Pic}_{X/k} \to Hom(X, X^t)\,.$$

KerphiLem1 **(7.15) Lemma.** *Let T be a connected k-scheme. Let L be a line bundle on X_T. Write L_t for $L_{|X\times\{t\}}$. Then for any two k-valued points s, $t \in T(k)$ we have $\varphi_{L_s} = \varphi_{L_t}$. In particular, $\mathrm{Pic}^0_{X/k} \subset \mathrm{Ker}(\varphi)$.*

Proof. By (d) ⇒ (a) of (7.12), applied with $T = X^t$ and with $L = \mathscr{P}$ the Poincaré bundle, we find that $X^t = \mathrm{Pic}^0_{X/k} \subset \mathrm{Ker}(\varphi)$. As φ is a homomorphism, it is constant on the connected components of $\mathrm{Pic}_{X/k}$.

Let $f\colon T \to \mathrm{Pic}_{X/k}$ be the morphism corresponding to L; it factors through some connected component $C \subset \mathrm{Pic}_{X/k}$. Let $M := \mathscr{P}_{|X\times C}$ be the restriction of the Poincaré bundle to $X \times C$. Using (i) and (ii) of (7.11) we find that $\varphi_L\colon X_T \to X^t_T$ is obtained from $\varphi_M\colon X_C \to X^t_C$ by pulling back via f on the basis. But by the above, $\varphi_{M_{f(s)}} = \varphi_{M_{f(t)}}$. □

KerphiLem2 **(7.16) Lemma.** *Let X be an abelian variety over k. Let T be a k-scheme and let L be a line bundle on X_T such that $\varphi_L = 0$.*

(i) *If Y is a T-scheme then for any two morphisms f, $g\colon Y \to X_T$ of schemes over T we have $\big[(f+g)^*L\big] = \big[f^*L \otimes g^*L\big]$ in $\mathrm{Pic}_{Y/T}(T)$.*

(ii) *For $n \in \mathbb{Z}$ we have $[n^*L] = [L^n]$ in $\mathrm{Pic}_{X/k}(T)$.*

Proof. If $\varphi_L = 0$ then $\Lambda(L) = \pi^*N$ for some line bundle N on T. Pulling back via $(f, g)\colon Y \to X_T \times_T X_T$ gives $(f+g)^*L = f^*L \otimes g^*L \otimes \pi^*N$, where $\pi\colon Y \to T$ is the structural morphism. But π^*N is trivial in $\mathrm{Pic}_{Y/T}(T)$, so we get (i). Applying this with $f = \mathrm{id}_{X_T}$ and $g = n_{X_T}$ gives the relation $[(n+1)^*L] = [L \otimes n^*L]$. By double induction on n, starting with the cases $n = 0$ and $n = 1$, we obtain (ii). □

Using that $\mathrm{Pic}^0_{X/k} \subset \mathrm{Ker}(\varphi)$ we obtain a positive answer to the questions posed in (6.20).

fftCor **(7.17) Corollary.** *Let X and Y be abelian varieties over k. Then the map $Hom(X, Y) \to Hom(Y^t, X^t)$ given on points by $f \mapsto f^t$ is a homomorphism of k-group schemes. For all $n \in \mathbb{Z}$ we have $(n_X)^t = n_{X^t}$.*

Combining this last result with (7.5) we find that $X^t[n]$ is canonically isomorphic to the Cartier dual of $X[n]$, for every $n \in \mathbb{Z}_{>0}$.

SymmHomXXt **(7.18)** Let X be an abelian variety. We call a homomorphism $f\colon X \to X^t$ symmetric if $f = f^t$, taking the isomorphism $\kappa_X\colon X \xrightarrow{\sim} X^{tt}$ of (7.9) as an identification. It follows from the previous

corollary that the functor of symmetric homomorphisms $X \to X^t$ is represented by a closed subgroup scheme

$$Hom^{\mathrm{sym}}(X, X^t) \subset Hom(X, X^t)\,.$$

In fact, $Hom^{\mathrm{sym}}(X, X^t)$ is just the kernel of the endomorphism of $Hom(X, X^t)$ given by $f \mapsto f - f^t$.

By Lemma (7.8), the homomorphism φ: $\mathrm{Pic}_{X/k} \to Hom(X, X^t)$ factors through the subgroup $Hom^{\mathrm{sym}}(X, X^t)$. (Because $Hom(X, X^t)$ is étale, it suffices to know that φ maps into Hom^{sym} for points with values in a field.)

Our next goal is to show that not only $\mathrm{Pic}^0_{X/k} \subset \mathrm{Ker}(\varphi)$ but that the two are in fact equal. First we prove a lemma about the cohomology of line bundles L with $\varphi_L = 0$. Note that we are here again working over a field; this lemma has no straightforward generalization to the relative setting.

KerphiLem3 **(7.19) Lemma.** *Let L be a line bundle on X with $\varphi_L = 0$. If $L \ncong O_X$ then $H^i(X, L) = 0$ for all i.*

Proof. First we treat the group $H^0(X, L)$. If there is a non-trivial section s then $(-1)^*s$ is a non-trivial section of $(-1)^*L \cong L^{-1}$; so both L and L^{-1} have a non-trivial section, and this implies that L is trivial. Since we have assumed this is not the case, $H^0(X, L) = \{0\}$.

Let now $i \geqslant 1$ be the smallest positive integer such that $H^i(X, L) \neq 0$. Consider the composition

$$X \to X \times X \xrightarrow{m} X\,, \quad \text{given by } x \mapsto (x, 0) \mapsto x\,.$$

On cohomology this induces the maps

$$H^i(X, L) \to H^i(X \times X, m^*L) \to H^i(X, L)\,,$$

the composition of which is the identity. But since $m^*L \cong p_1^*L \otimes p_2^*L$, the Künneth formula gives

$$H^i(X \times X, m^*L) \cong H^i(X \times X, p_1^*L \otimes p_2^*L) \cong \sum_{a+b=i} H^a(X, L) \otimes H^b(X, L)\,.$$

Since $H^0(X, L) = \{0\}$ we may consider only those terms in the RHS where $a \geqslant 1$ and $b \geqslant 1$. But then $a < i$ which by our choice of i implies that $H^a(X, L) = 0$. This shows that the identity map on $H^i(X, L)$ factors via zero. □

In the proof of the next proposition we need some facts about cohomology and base change. Here is what we need.

CohBCFacts **(7.20) Fact.** *Let f: $X \to Y$ be a proper morphism of noetherian schemes, with Y reduced and connected. Let F be a coherent sheaf of O_X-modules on X.*

(i) *If $y \mapsto \dim_{k(y)} H^q(X_y, F_y)$ is a constant function on Y then $R^q f_*(F)$ is a locally free sheaf on Y, and for all $y \in Y$ the natural map $R^q f_*(F) \otimes_{O_Y} k(y) \to H^q(X_y, F_y)$ is an isomorphism.*

(ii) *If $R^q f_*(F) = 0$ for all $q \geqslant q_0$ then $H^q(X_y, F_y) = 0$ for all $y \in Y$ and $q \geqslant q_0$.*

A proof of this result can be found in [MAV], § 5.

Kerphikbar **(7.21) Proposition.** *Let X be an abelian variety over an algebraically closed field k. Let L be an ample line bundle on X and M a line bundle with $\varphi_M = 0$. Then there exists a point $x \in X(k)$ with $M \cong t_x^*L \otimes L^{-1}$.*

Proof. We follow Mumford's beautiful proof. The idea is to look at the cohomology on $X \times X$ of the line bundle

$$K := \Lambda(L) \otimes p_2^* M^{-1} .$$

The projections $p_1, p_2 \colon X \times X \to X$ give rise to two Leray spectral sequences

$$E_2^{p,q} = H^p(X, R^q p_{1,*}(K)) \Rightarrow H^{p+q}(X \times X, K)$$

and

$$E_2'^{p,q} = H^p(X, R^q p_{2,*}(K)) \Rightarrow H^{p+q}(X \times X, K) .$$

The restrictions of K to the horizontal and vertical fibres are given by

$$\begin{aligned} K_{|\{x\}\times X} &\cong t_x^* L \otimes L^{-1} \otimes M^{-1} , \\ K_{|X\times\{x\}} &\cong t_x^* L \otimes L^{-1} . \end{aligned}$$

Assume that there is no $x \in X(k)$ such that $t_x^* L \otimes L^{-1} \cong M$. It then follows that $K_{|\{x\}\times X}$ is a non-trivial bundle in $\mathrm{Ker}(\varphi)$ for every x. (Note that $[t_x^* L \otimes L^{-1}] = \varphi_L(x) \in \mathrm{Pic}^0_{X/k} \subset \mathrm{Ker}(\varphi)$.) By Lemma (7.19) and (7.20) this gives $R^q p_{1,*}(K) = (0)$ for all q, and from the first spectral sequence we find that $H^n(X \times X, K) = 0$ for all n.

Now use the second spectral sequence. For $x \notin K(L)$ the bundle $t_x^* L \otimes L^{-1}$ is a non-trivial bundle in $\mathrm{Ker}(\varphi)$. Again by Lemma (7.15) we find that $\mathrm{supp}(R^q p_{2,*} K) \subset K(L)$. Since $K(L)$ is a finite subscheme of X (the bundle L being ample) we find

$$E_2'^{p,q} = \begin{cases} \bigoplus\limits_{x \in K(L)} R^q p_{2,*}(K)_x & \text{if } p = 0; \\ 0 & \text{otherwise.} \end{cases}$$

As we only have non-zero terms for $p = 0$, the spectral sequence degenerates at level E_2'. This gives $H^n(X \times X, K) = \oplus_{x \in K(L)} R^n p_{2,*}(K)_x$.

Comparing the two answers for $H^n(X \times X, K)$ we find that $R^n p_{2,*}(K) = 0$ for all n. By (7.20) this implies that $H^n(X, K_{|X\times\{x\}}) = 0$ for all x. But $K_{|X\times\{0\}}$ is the trivial bundle, so taking $n = 0$ and $x = 0$ gives a contradiction. □

KerphiPic **(7.22) Corollary.** *Let X be an abelian variety over a field k. Then* $\mathrm{Pic}^0_{X/k} = \mathrm{Ker}\big(\varphi \colon \mathrm{Pic}_{X/k} \to \mathit{Hom}(X, X^t)\big)$.

Proof. We already know that $\mathrm{Ker}(\varphi)$ is a subgroup scheme of $\mathrm{Pic}_{X/k}$ that contains $\mathrm{Pic}^0_{X/k}$. Hence $\mathrm{Ker}(\varphi)$ is the union of a number of connected components of $\mathrm{Pic}_{X/k}$. By the proposition, every $\overline{k}$-valued point of $\mathrm{Ker}(\varphi)$ lies in Pic^0. The claim follows. □

LinPic0 **(7.23) Corollary.** *Let X be an abelian variety over a field k. Let L be a line bundle on X.*

(i) *If $[L^n] \in \mathrm{Pic}^0_{X/k}$ for some $n \neq 0$ then $[L] \in \mathrm{Pic}^0_{X/k}$. In particular, if L has finite order, i.e., $L^n \cong O_X$ for some $n \in \mathbb{Z}_{\geqslant 1}$, then $[L] \in \mathrm{Pic}^0_{X/k}$.*

(ii) *We have $[L \otimes (-1)^* L^{-1}] \in \mathrm{Pic}^0_{X/k}$.*

(iii) *We have*

$$\begin{aligned} [L] \in \mathrm{Pic}^0_{X/k} &\iff n^* L \cong L^n \quad \textit{for all } n \in \mathbb{Z} \\ &\iff n^* L \cong L^n \quad \textit{for some } n \in \mathbb{Z} \setminus \{0, 1\}. \end{aligned}$$

Proof. (i) Since φ is a homomorphism we have $\varphi_{L^n}(x) = n \cdot \varphi_L(x) = \varphi_L(n \cdot x)$. Hence if $[L^n] \in \mathrm{Pic}^0(X)$ then φ_L is trivial on all points in the image of n_X. But n_X is surjective, so φ_L is trivial.

(ii) Direct computation shows that $\varphi_{(-1)^*L}(x) = -\varphi_L(x)$ for all L and x. Since also $\varphi_{L^{-1}}(x) = -\varphi_L(x)$, we find that $[L \otimes (-1)^* L^{-1}] \in \mathrm{Ker}(\varphi)$.

(iii) The first implication "$\Rightarrow$" was proven in (7.16) above; the second is trivial. Suppose that $n^*L \cong L^n$ for some $n \notin \{0, 1\}$. Since $n^*L \cong L^n \otimes [L \otimes (-1)^* L]^{(n^2-n)/2}$ it follows that $L \otimes (-1)^* L$ has finite order, hence its class lies in $\mathrm{Pic}^0_{X/k}$. By (ii) we also have $[L \otimes (-1)^* L^{-1}] \in \mathrm{Pic}^0_{X/k}$. Hence $[L^2] \in \mathrm{Pic}^0_{X/k}$ and by (i) then also $[L] \in \mathrm{Pic}^0_{X/k}$. □

NerSeveri **(7.24)** In (3.29) we have associated to any group scheme G locally of finite type over a field k an étale group scheme of connected components, denoted by $\varpi_0(G)$. We now apply this with $G = \mathrm{Pic}_{X/k}$ for X/k an abelian variety. The associated component group scheme

$$\mathrm{NS}_{X/k} := \varpi_0(\mathrm{Pic}_{X/k})$$

is called the Néron-Severi group scheme of X over k. The natural homomorphism $q\colon \mathrm{Pic}_{X/k} \to \mathrm{NS}_{X/k}$ realizes $\mathrm{NS}_{X/k}$ as the fppf quotient of $\mathrm{Pic}_{X/k}$ modulo $\mathrm{Pic}^0_{X/k}$; hence we could also write

$$\mathrm{NS}_{X/k} = \mathrm{Pic}_{X/k}/\mathrm{Pic}^0_{X/k}\,.$$

We refer to the group

$$\mathrm{NS}(X) := \mathrm{NS}_{X/k}(k)$$

as the Néron-Severi group of X. Note that $\mathrm{NS}(X)$ equals the subgroup of $\mathrm{Gal}(k_s/k)$-invariants in $\mathrm{NS}(X_{k_s})$.

We say that two line bundles L and M are algebraically equivalent, notation $L \sim_{\mathrm{alg}} M$, if $[L]$ and $[M]$ have the same image in $\mathrm{NS}(X)$. As $\mathrm{NS}(X)$ naturally injects into $\mathrm{NS}(X_{\overline{k}})$, algebraic equivalence of line bundles (or divisors) can be tested over $\overline{k}$, and there it coincides with the notion defined in Remark (6.9). Hence we can think of the Néron-Severi group scheme as being given by the classical, geometric Néron-Severi group $\mathrm{NS}(X_{k_s}) = \mathrm{NS}(X_{\overline{k}})$ of line bundles (or divisors) modulo algebraic equivalence, together with its natural action of $\mathrm{Gal}(k_s/k)$. Note, however, that a k-rational class $\xi \in \mathrm{NS}(X)$ may not always be representable by a line bundle on X over the ground field k.

Let us rephrase some of the results that we have obtained in terms of the Néron-Severi group.

NSquadratic **(7.25) Corollary.** *The Néron-Severi group* $\mathrm{NS}(X)$ *is torsion-free. If* $n \in \mathbb{Z}$ *and* L *is a line bundle on* X *then* n^*L *is algebraically equivalent to* L^{n^2}*; in other words,* $n^*\colon \mathrm{NS}(X) \to \mathrm{NS}(X)$ *is multiplication by* n^2*.*

Proof. The first assertion is just (i) of Corollary (7.23). The second assertion follows from (ii) of that Corollary together with Corollary (2.12). □

NSHomSymm **(7.26)** Corollary (7.22) can be restated by saying that the natural homomorphism $\varphi\colon \mathrm{Pic}_{X/k} \to \mathit{Hom}^{\mathrm{sym}}(X, X^t) \subset \mathit{Hom}(X, X^t)$ factors as

$$\mathrm{Pic}_{X/k} \xrightarrow{\ q\ } \mathrm{NS}_{X/k} \xhookrightarrow{\ \psi\ } \mathit{Hom}^{\mathrm{sym}}(X, X^t)$$

for some injective homomorphism $\psi\colon \mathrm{NS}_{X/k} \hookrightarrow \mathit{Hom}^{\mathrm{sym}}(X, X^t)$. This says that the homomorphism φ_L associated to a line bundle L only depends on the algebraic equivalence class of L, and that $\varphi_L = \varphi_M$ only if $L \sim_{\mathrm{alg}} M$. We shall later show that ψ is actually an isomorphism; see Corollary (11.3).

§4. *Applications to cohomology.*

HodgeCohom **(7.27) Proposition.** *Let X be an abelian variety with $\dim(X) = g$. Cup-product gives an isomorphism $\wedge^\bullet H^1(X, O_X) \xrightarrow{\sim} H^\bullet(X, O_X)$. For every p and q we have a natural isomorphism $H^q(X, \Omega^p_{X/k}) \cong (\wedge^q T_{X^t,0}) \otimes (\wedge^p T^\vee_{X,0})$. The Hodge numbers $h^{p,q} = \dim H^q(X, \Omega^p_{X/k})$ are given by $h^{p,q} = \binom{g}{p}\binom{g}{q}$.*

Proof. Use (6.13) and the isomorphisms $\Omega^p_{X/k} \cong (\wedge^p T^\vee_{X,0}) \otimes_k O_X$. □

nXonCohom **(7.28) Corollary.** *Multiplication by an integer n on X induces multiplication by n^{p+q} on $H^q(X, \Omega^p_X)$.*

Proof. Immediate from the fact that n_X induces multiplication by n on $T_{X,0}$, applied to both X and X^t. □

Before we state the next corollary, let us recall that the algebraic de Rham cohomology of a smooth proper algebraic variety X over a field k is defined to be the hypercohomology of the de Rham complex

$$\Omega^\bullet_{X/k} = (O_X \xrightarrow{d} \Omega^1_{X/k} \xrightarrow{d} \Omega^2_{X/k} \xrightarrow{d} \cdots),$$

with O_X in degree zero. We have the so-called "stupid filtration" of this complex, by the subcomplexes $\sigma_{\geqslant p}\Omega^\bullet_{X/k}$ given by

$$[\sigma_{\geqslant p}\Omega^\bullet_{X/k}]^i = \begin{cases} 0 \text{ for } i < p \\ \Omega^i_{X/k} \text{ for } i \geqslant p. \end{cases}$$

This gives rise to a spectral sequence

$$E_1^{p,q} = H^q(X, \Omega^p_X) \Rightarrow H^{p+q}_{\mathrm{dR}}(X/k)$$

called the "Hodge–de Rham" spectral sequence.

If k has characteristic zero then it follows from Hodge theory that this spectral sequence degenerates at the E_1-level, see Deligne [1], section 5. If k has characteristic $p > 0$ then this is no longer true in general. For examples and further results we refer to Deligne-Illusie [1] and Oesterlé [1].

As we shall now show, for abelian varieties the degeneration of the Hodge-de Rham spectral sequence at level E_1 follows from (6.12) without any restrictions on the field k.

HdeRSS **(7.29) Corollary.** *Let X be an abelian variety over a field k. Then the "Hodge-de Rham" spectral sequence of X degenerates at level E_1.*

Proof. We follow the proof given by Oda [1]. We have to show that the differentials $d_r\colon E_r^{p,q} \to E_r^{p+r,q-r+1}$ are zero for all $r \geqslant 1$. By induction we may assume that this holds at all levels $< r$. (The empty assumption if $r = 1$.)

Write $E_r^*(X) = \oplus E_r^{p,q}$, graded by total degree. Cup-product makes $E_r^*(X)$ into a connected, graded-commutative k-algebra. By our induction assumption and the Künneth formula there is a canonical isomorphism

$$E_r^*(X \times X) \cong E_r^*(X) \otimes_k E_r^*(X)\,.$$

Write $\mu\colon E_r^*(X) \to E_r^*(X) \otimes_k E_r^*(X)$ for the map induced by the multiplication law on X, and write $\varepsilon\colon E_r^*(X) \to E_k^0(X) = k$ for the projection onto the degree zero component. One checks that μ and ε give $E_r^*(X)$ the structure of a graded bialgebra over k.

Let $g = \dim(X)$. By what was shown above, $E_r^1(X) = H^1(X, O_X) \oplus H^0(X, \Omega^1_{X/k})$ has dimension $2g$. Also, $E_r^i(X) = 0$ for $i > 2g$. The Borel-Hopf structure theorem (6.12) then gives

$$E_r^*(X) \cong \wedge^* E_r^1(X)\,.$$

Since d_r is compatible with the product structure (cup-product) on $E_r^*(X)$, it suffices to show that d_r is zero on $E_r^1(X)$, which is just the space of primitive elements of $E_r^*(X)$. (See 6.17.) By functoriality of the Hodge–de Rham spectral sequence we have $\mu \circ d_r = (d_r \otimes d_r) \circ \mu$. Therefore, for $\xi \in E_r^1(X)$ we have $\mu(d_r(\xi)) = d_r(\xi) \otimes 1 + 1 \otimes d_r(\xi)$. This shows that $d_r(\xi)$ is again a primitive element. But $d_r(\xi) \in E_r^2(X)$ which, by (6.17), contains no non-zero primitive elements. This shows that $d_r = 0$. □

HdeRCor **(7.30) Corollary.** *There is an exact sequence*

$$0 \longrightarrow \mathrm{Fil}^1 H^1_{\mathrm{dR}}(X/k) \longrightarrow H^1_{\mathrm{dR}}(X/k) \longrightarrow H^1(X, O_X) \longrightarrow 0\,,$$

where $\mathrm{Fil}^1 H^1_{\mathrm{dR}}(X/k) := H^0(X, \Omega^1_{X/k}) \cong T^\vee_{X,0}$.

To close this section let us fulfil an earlier promise and give an example of a smooth projective variety with non-reduced Picard scheme. We refer to Katsura-Ueno [1] for similar examples.

IgusaExa **(7.31) Example.** Let k be an algebraically closed field of characteristic 3. Let E_1 be the elliptic curve over k given by the Weierstrass equation $y^2 = x^3 - x$. From (5.27) we know that E_1 is supersingular. Let σ be the automorphism of E_1 given by $(x, y) \mapsto (x + 1, y)$. Then σ has order 3, so that we get an action of $G := \mathbb{Z}/3\mathbb{Z}$ on E_1. The quotient of E_1 by G is isomorphic to $\mathbb{P}^1_k$; in affine coordinates te quotient map is just $(x, y) \mapsto y$.

Let E_2 be an ordinary elliptic curve over k. Let τ be the translation over a point of (exact) order 3 on E_2. Then (σ, τ) is an automorphism of order 3 of the abelian surface $X := E_1 \times E_2$; this gives a strictly free action of $G := \mathbb{Z}/3\mathbb{Z}$ on X, and we can form the quotient $\pi\colon X \to Y := G\backslash X$. By (??) π is an étale morphism, so Y is again a non-singular algebraic surface. We have a natural morphism $Y \to (G\backslash E_1) \cong \mathbb{P}^1$; this exhibits Y as an elliptic surface over $\mathbb{P}^1$. In fact, for all $P \in \mathbb{P}^1(k)$ with $P \neq \infty$ the fibre Y_P above P is isomorphic to E_2.

We compute $h^1(Y, O_Y)$ using Hirzebruch-Riemann-Roch and Chern numbers for algebraic surfaces. (A reference is ??.) The Euler number c_2 of Y is a multiple of the Euler number of X, and this is 0. By the Hirzebruch-Riemann-Roch formula we have

$$1 - h^1(Y, O_Y) + h^2(Y, O_Y) = (c_1^2 + c_2)/12 = 0\,,$$

since $c_1^2 = 0$ for every elliptic surface. By Serre duality, $h^2(Y, O_Y) = h^0(Y, \Omega^2_{Y/k})$. Now we use that $H^0(Y, \Omega^2_{Y/k})$ is isomorphic to the space of G-invariants in $H^0(X, \Omega^2_{X/k})$. If ω_i is a basis for $H^0(E_i, \Omega^1_{E_i/k})$ then $\omega_1 \wedge \omega_2$ is a basis for $H^0(X, \Omega^2_{X/k})$. But ω_1 is a multiple of dy, which is

invariant under σ, and ω_2 is translation invariant, in particular invariant under τ. In sum, we find that $h^2(Y, O_Y) = 1$ and $h^1(Y, O_Y) = 2$.

On the other hand, $\pi\colon X \to Y$ induces a homomorphism $\pi^*\colon \mathrm{Pic}^0_{Y/k} \to X^t = \mathrm{Pic}^0_{X/k}$. The same arguments as in the proof of Theorem (7.5) show that $\mathrm{Ker}(\pi^*) \cong \mu_3$. On the other hand, π^* factors via the subscheme of G-invariants in X^t. (See Exercise ?? for the existence of such a subscheme of G-invariants.) The point here is that we are describing line bundles on Y as coming from line bundles L on X together with an action of G. But such an action is given by an isomorphism $\rho^*L \xrightarrow{\sim} \mathrm{pr}_X^* L$ of line bundles on $G \times_k X$. The existence of such an isomorphism says precisely that L corresponds to a G-invariant point of X^t.

By Exercises ?? and ??, $X^t \xrightarrow{\sim} X$. The induced action of G on X^t is given by the automorphism (σ, id). (Cf. Exercise ??) Therefore, the subscheme of G-invariants in X^t is $E_1^{\langle\sigma\rangle} \times E_2$. The only geometric point of E_1 fixed under σ is the origin. A computation in local coordinates reveals that $E_1^{\langle\sigma\rangle}$ is in fact the Frobenius kernel $E_1[F] \subset E_1$ which can be shown to be isomorphic to α_3. In any case, we find that $\mathrm{Pic}^0_{Y/k}$ is 1-dimensional, whereas we have shown its tangent space at the identity, isomorphic to $H^1(Y, O_Y)$, to be 2-dimensional. Hence $\mathrm{Pic}^0_{Y/k}$ is non-reduced.

§5. *The duality between Frobenius and Verschiebung.*

RelFrobRevisit **(7.32)** Let S be a scheme of characteristic p. Recall that for any S-scheme $a_X\colon X \to S$ we have a commutative diagram with Cartesian square

$$\begin{array}{ccc} X & & \\ & & \\ X^{(p/S)} & \xrightarrow{W_{X/S}} & X \\ \downarrow{\scriptstyle a_X^{(p)}} & & \downarrow{\scriptstyle a_X} \\ S & \xrightarrow{\mathrm{Frob}_S} & S \end{array}$$

If there is no risk of confusion we simply write $X^{(p)}$ for $X^{(p/S)}$. Note that if $a_T\colon T \to S$ is an S-scheme then we have $a_T \circ \mathrm{Frob}_T = \mathrm{Frob}_S \circ a_T$ and this gives a natural identification $(X_T)^{(p/T)} = (X^{(p/S)})_T$. We denote this scheme simply by $X_T^{(p)}$.

Let us write $T_{(p)}$ for the scheme T viewed as an S-scheme via the morphism $a_{T_{(p)}} := \mathrm{Frob}_S \circ a_T = a_T \circ \mathrm{Frob}_T\colon T \to S$. The morphism $\mathrm{Frob}_T\colon T \to T$ is not, in general, a morphism of S-schemes, but if we view it as a morphism $T_{(p)} \to T$ then it is a morphism over S. To avoid confusion, let us write $\mathrm{Fr}_T\colon T_{(p)} \to T$ for the morphism of S-schemes given by Frob_T.

Let Y be an S-scheme. Recall that we write $Y(T)$ for the T-valued points of Y. It is understood here (though not expressed in the notation) that all schemes and morphisms of schemes are over a fixed base scheme S; so $Y(T)$ is the set of morphisms $T \to Y$ over S. There is a natural bijection

$$w_{Y,T}\colon Y^{(p)}(T) \xrightarrow{\sim} Y(T_{(p)})\,,$$

sending a point $\eta\colon T \to Y^{(p)}$ to $W_{Y/S} \circ \eta$, which is a $T_{(p)}$-valued point of Y. The composition

$$w_{Y,T} \circ F_{Y/S}(T)\colon Y(T) \to Y(T_{(p)})$$

is the map that sends $y \in Y(T)$ to $y \circ \mathrm{Fr}_T \colon T_{(p)} \to Y$, which is the same as $y \circ \mathrm{Frob}_T \colon T \to Y$ viewed as a morphism $T_{(p)} \to Y$.

RelFrobPic **(7.33)** Consider an abelian variety X over a field k of characteristic p. Take $S := \mathrm{Spec}(k)$. If T is any S-scheme then $X \times_S T_{(p)}$ is the same as $X^{(p)} \times_S T$, and we find that

$$\begin{aligned} \mathrm{Pic}^{(p)}_{X/k}(T) \xrightarrow[w_{\mathrm{Pic}_{X/k},T}]{\sim} \mathrm{Pic}_{X/k}(T_{(p)}) &= \left\{ \begin{matrix} \text{isomorphism classes of rigidified} \\ \text{line bundles } (L,\alpha) \text{ on } X \times_S T_{(p)} \end{matrix} \right\} \\ &= \left\{ \begin{matrix} \text{isomorphism classes of rigidified} \\ \text{line bundles } (L,\alpha) \text{ on } X^{(p)} \times_S T \end{matrix} \right\} = \mathrm{Pic}_{X^{(p)}/S}(T)\,. \end{aligned}$$

In this way we obtain an isomorphism $\mathrm{Pic}^{(p)}_{X/S} \xrightarrow{\sim} \mathrm{Pic}_{X^{(p)}/S}$, which we take as an identification. Applying (7.32) with $Y = \mathrm{Pic}_{X/k}$ we find that the relative Frobenius of $\mathrm{Pic}_{X/k}$ over k is the homomorphism that sends a point $y \in \mathrm{Pic}_{X/k}(T)$ to $y \circ \mathrm{Frob}_T$, viewed as a morphism $T_{(p)} \to \mathrm{Pic}_{X/k}$. Because the diagram

$$\begin{array}{ccc} X_T^{(p)} & \xrightarrow{W_{X_T/T}} & X_T \\ {\scriptstyle a_X^{(p)}}\downarrow & & \downarrow{\scriptstyle a_X} \\ T & \xrightarrow{\mathrm{Frob}_T} & T \end{array}$$

is Cartesian this just means that $F_{\mathrm{Pic}/k} \colon \mathrm{Pic}_{X/k} \to \mathrm{Pic}_{X^{(p)}/k}$ sends the class of a rigidified line bundle (L,α) on X_T to the class of $\bigl(L^{(p)},\alpha^{(p)}\bigr)$ on $X_T^{(p)}$, where $L^{(p)} := W^*_{X_T/T}L$, and where $\alpha^{(p)} \colon O_T \xrightarrow{\sim} e^*L^{(p)} = \mathrm{Frob}_T^*(e^*L)$ is the rigidification of $L^{(p)}$ along the zero section obtained by pulling back α via Frob_T.

FVDualProp **(7.34) Proposition.** *Let X be an abelian variety over a field k of characteristic p. We identify $(X^t)^{(p)} = (X^{(p)})^t$ as in* (7.33)*, and we denote this abelian variety by $X^{t,(p)}$. Then we have the identities*

$$F^t_{X/k} = V_{X^t/k} \colon X^{t,(p)} \to X^t \qquad \textit{and} \qquad V^t_{X/k} = F_{X^t/k} \colon X^t \to X^{t,(p)}\,.$$

Proof. It suffices to prove that $F^t_{X/k} \circ F_{X^t/k} \colon X^t \to X^t$ equals $[p]_{X^t}$, because if this holds then together with Proposition (5.20) and the fact that $F_{X^t/k}$ is an isogeny it follows that $F^t_{X/k} = V_{X^t/k}$. The other assertion follows by duality.

Let T be a k-scheme. Consider a rigidified line bundle (L,α) on X_T that gives a point of $X^t(T)$. As explained in (7.33) $F_{X^t/k}$ sends (L,α) to $\bigl(L^{(p)},\alpha^{(p)}\bigr)$ with $L^{(p)} = W^*_{X_T/T}L$. Because $W_{X_T/T} \circ F_{X_T/T} = \mathrm{Frob}_{X_T}$, pull-back via $F_{X_T/T}$ gives the line bundle $\mathrm{Frob}^*_{X_T}L$ on X_T. But if Y is any scheme of characteristic p and M is a line bundle on Y then $\mathrm{Frob}^*_Y(M) \cong M^p$; this follows for instance by taking a trivialization of M and remarking that Frob_Y raises all transition functions to the power p. The rigidification we have on $F^*_{X_T/T}W^*_{X_T/T}L = \mathrm{Frob}^*_{X_T}L = L^p$ is the isomorphism

$$O_T = \mathrm{Frob}^*_T O_T \xrightarrow{\sim} e^*_{X_T}F^*_{X_T/T}W^*_{X_T/T}L = e^*_{X_T^{(p)}}W^*_{X_T/T}L = \mathrm{Frob}^*_T e^*_{X_T}L = (e^*_{X_T}L)^p$$

that is obtained from α by pulling back via Frob_T, which just means it is α^p. In sum, $F^t_{X/k} \circ F_{X^t/k}$ sends (L,α) to (L^p,α^p), which is what we wanted to prove. □

Exercises.

Ex:mtdiagt **(7.1)** Let X be an abelian variety. Let $m_X\colon X \times X \to X$ be the group law, and let $\Delta_X\colon X \to X \times X$ be the diagonal morphism. Show that $(m_X)^t = \Delta_{X^t}\colon X^t \times X^t \to X^t$, and that $(\Delta_X)^t = m_{X^t}\colon X^t \times X^t \to X^t$.

Ex:Ln=OX **(7.2)** Let L be a line bundle on an abelian variety X.

(i) Show that, for $n \in \mathbb{Z}$,

$$n^*L \cong O_X \quad \Longleftrightarrow \quad L^n \cong O_X\,.$$

(ii) Show that, for $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$,

$$n^*L \cong L \quad \Longleftrightarrow \quad L^{n-1} \cong O_X\,.$$

Ex:L=L1L2 **(7.3)** Let X be an abelian variety over an algebraically closed field k. Show that every line bundle L on X can be written as $L = L_1 \otimes L_2$, where L_1 is symmetric and $[L_2] \in \mathrm{Pic}^0_{X/k}$. [*Hint:* By (7.23), the class of the line bundle $(-1)^*L \otimes L^{-1}$ is in $\mathrm{Pic}^0_{X/k}$. As Pic^0 is an abelian variety and $k = \overline{k}$, there exists a line bundle M on X with $[M] \in \mathrm{Pic}^0$ and $M^2 \cong (-1)^*L \otimes L^{-1}$. Now show that $L \otimes M$ is symmetric.]

Ex:(m,n)P **(7.4)** Let $\mathscr{P}$ be the Poincaré bundle on $X \times X^t$. For m, $n \in \mathbb{Z}$, consider the endomorphism (m, n) of $X \times X^t$. Show that $(m, n)^*\mathscr{P} \cong \mathscr{P}^{mn}$.

Ex:phiP **(7.5)** Let $\mathscr{P}$ be the Poincaré bundle on $X \times X^t$. Show that the associated homomorphism $\varphi_{\mathscr{P}}\colon X \times X^t \to X^t \times X^{tt}$ is the homomorphism given by $\varphi_{\mathscr{P}}(x, \xi) = \big(\xi, \kappa_X(x)\big)$. [*Hint:* Compute the restrictions of $t_(x,\xi)^*\mathscr{P} \otimes \mathscr{P}^{-1}$ to $X \times \{0\}$ and $\{0\} \times X^t$.]

Ex:transldual **(7.6)** If τ is a translation on an abelian variety, then what is the induced automorphism τ^t of the dual abelian variety?

Ex:AVQuotDual **(7.7)** Let X be an abelian variety over a field k. Let $i\colon Y \hookrightarrow X$ be an abelian subvariety. Write $q\colon X \to Z := X/Y$ for the fppf quotient morphism, which exists by Thm. (4.38). Note that Z is an abelian variety; see Example (4.40).

(i) Show that for any k-scheme T we have $q_*(O_{X_T}) = O_{Z_T}$.

(ii) Prove that $q^t\colon Z^t \to X^t$ is injective and gives an isomorphism between Z^t and $\mathrm{Ker}(i^t\colon X^t \to Y^t)^0_{\mathrm{red}}$.

Ex:Lsqtens **(7.8)** Let L be a line bundle on an abelian variety X. For a symmetric $m \times m$-matrix S with integer coefficients s_{ij} we define a line bundle $L^{\boxtimes S}$ on X^m by

$$L^{\boxtimes S} := \Big(\bigotimes_{i=1}^{m} p_i^* L^{s_{ii}}\Big) \otimes \Big(\bigotimes_{1 \leqslant i < j \leqslant m} p_{ij}^* \Lambda(L)^{s_{ij}}\Big)\,.$$

If $\alpha = \big(a_{ij}\big)$ is an integer valued matrix of size $m \times n$ we define a homomorphism of abelian varieties $[\alpha]_X\colon X^n \to X^m$ by $\alpha(x_1, \ldots, x_n) = (y_1, \ldots, y_m)$ with $y_i = \sum_{j=1}^n a_{ij} x_j$.

(i) Prove that $[\alpha]_X^*\big(L^{\boxtimes S}\big)$ is algebraically equivalent to $L^{\boxtimes({}^{\mathrm{t}}\alpha S \alpha)}$.

(ii) Assume that L is a symmetric line bundle. Prove that $[\alpha]_X^*\big(L^{\boxtimes S}\big) \cong L^{\boxtimes({}^{\mathrm{t}}\alpha S \alpha)}$.

Notes. (nog aanvullen)

To a line bundle L on an abelian variety X we shall associate a group scheme, the *theta group* $\mathscr{G}(L)$ of L. If the class of L is in $\mathrm{Pic}^0_{X/k} = X^t$ then $\mathscr{G}(L)$ is an extension of X by the multiplicative group $\mathbb{G}_m$ and is commutative. If $[L] \notin \mathrm{Pic}^0_{X/k}$ then $\mathscr{G}(L)$ is much smaller and in general not commutative. The theta group is a convenient tool for studying when a line bundle descends over an isogeny. Further we study the structure of so-called non-degenerate theta groups, and their representations.

§1. *The theta group $\mathscr{G}(L)$.*

G(L)Def **(8.1)** Let X be an abelian variety over a field k. Let L be a line bundle on X. Write $\mathbb{L} = \mathbb{V}(L^\vee)$ for the corresponding geometric line bundle over X.

For a k-scheme T define $\mathscr{G}(L)(T)$ to be the set of pairs (x, φ) where $x \in X(T)$ and where $\varphi\colon L_T \to t_x^* L_T$ is an isomorphism. Geometrically this means that we have $\varphi_{\mathbb{L}}\colon \mathbb{L}_T \xrightarrow{\sim} \mathbb{L}_T$, fibrewise linear, fitting in a commutative diagram

$$\begin{array}{ccc} \mathbb{L}_T & \xrightarrow{\varphi_{\mathbb{L}}} & \mathbb{L}_T \\ \big\downarrow & & \big\downarrow \\ X_T & \xrightarrow[t_x]{} & X_T. \end{array}$$

Note that x is uniquely determined by φ, so that $\mathscr{G}(L)(T)$ is in natural bijection with the set of $\varphi_{\mathbb{L}}\colon \mathbb{L}_T \xrightarrow{\sim} \mathbb{L}_T$ lying over a translation on X_T.

The set $\mathscr{G}(L)(T)$ carries a natural group structure, with multiplication given by $(x_1, \varphi_1) \cdot (x_2, \varphi_2) = (x_1 + x_2, t_{x_2}^* \varphi_1 \circ \varphi_2)$. Since the association $T \mapsto \mathscr{G}(L)(T)$ is functorial in T we obtain a group functor $\mathscr{G}(L)\colon (\mathsf{Sch}_{/k})^0 \to \mathsf{Gr}$.

The (fibrewise linear) automorphisms of $\mathbb{L}_T$ lying over the identity on X_T are just the multiplications by elements of $\Gamma(X_T, O_{X_T})^* = \Gamma(T, O_T)^*$. This gives an identification of $\mathbb{G}_{m,k}$ with the kernel of the natural homomorphism (of group functors) $\mathscr{G}(L) \to K(L) \subset X$. Notice that $\mathbb{G}_{m,k}$ is central in $\mathscr{G}(L)$.

G(L)Repr **(8.2) Lemma.** *The group functor $\mathscr{G}(L)$ is representable. There is an exact sequence of group schemes*

ThetaGr:exseq
$$0 \longrightarrow \mathbb{G}_{m,k} \longrightarrow \mathscr{G}(L) \longrightarrow K(L) \longrightarrow 0\,, \tag{1}$$

where the map $\mathscr{G}(L) \to K(L)$ is given on points by $(x, \varphi) \mapsto x$.

Proof. Since the functor $K(L)$ is representable, it suffices to show that the homomorphism $\pi\colon \mathscr{G}(L) \to K(L)$ is (relatively) representable by a $\mathbb{G}_m$-torsor. So, let T be a k-scheme and $x \in K(L)(T)$. Write

$$M := \mathrm{pr}_{T,*}(L_T^{-1} \otimes t_x^* L_T)\,,$$

which is a line bundle on T. If T' is a T-scheme then the $\varphi\colon \mathbb{L}_{T'} \xrightarrow{\sim} \mathbb{L}_{T'}$ such that $(x,\varphi) \in \mathscr{G}(L)(T')$ are precisely the nowhere vanishing sections of $M_{T'}$. Thus, writing $\mathbb{M}^*$ for the $\mathbb{G}_{m,T}$-torsor corresponding to M (i.e., the T-scheme obtained from the geometric line bundle $\mathbb{M} := \mathbb{V}(M^\vee)$ by removing the zero section), we find that the fibre $\pi^{-1}(x)$ is representable by the T-scheme $\mathbb{M}^*$. That the sequence (1) is exact (even as a sequence of Zariski sheaves on $\mathsf{Sch}_{/k}$) is clear from the remarks preceding the lemma and the definition of $K(L)$. □

G(L)ReprBis **(8.3)** We indicate another proof of (8.2). For this, consider the $\mathbb{G}_m$-torsor $\mathbb{L}^*$ over X associated to L. Write $\xi\colon \mathbb{L}^* \to X$ for the structure morphism. Let $Y = \xi^{-1}(K(L)) = K(L) \times_X \mathbb{L}^*$, the scheme obtained by pulling back $\mathbb{L}^*$ via the inclusion map $K(L) \hookrightarrow X$. Choose a k-rational point $P \in \mathbb{L}^*(0)$. (This gives a trivialization $\mathbb{L}^*(0) \cong \mathbb{G}_{m,k}$.) We obtain a morphism $r_P\colon \mathscr{G}(L) \to Y$ by sending a point $(x,\varphi) \in \mathscr{G}(L)(T)$ to the image point $\varphi_{\mathbb{L}}(P) \in Y(T) \subset \mathbb{L}^*(T)$. It is not difficult to see that r_P gives an isomorphism of (set-valued) functors. So $\mathscr{G}(L)$ is represented by the scheme $Y = \xi^{-1}(K(L))$.

ThetaGrDef **(8.4) Definition.** Let L be a line bundle on an abelian variety. The group scheme $\mathscr{G}(L)$ is called the *theta group* of L.

eLDef **(8.5)** Consider the morphism $[\ ,\ ]\colon \mathscr{G}(L)\times\mathscr{G}(L) \to \mathscr{G}(L)$ given on points by $(g_1,g_2) \mapsto [g_1,g_2] = g_1g_2g_1^{-1}g_2^{-1}$. Since $K(L)$ is commutative this morphism factors through $\mathbb{G}_m \subset \mathscr{G}(L)$. The fact that $\mathbb{G}_m$ is central in $\mathscr{G}(L)$ then implies that $[\ ,\ ]$ factors modulo $\mathbb{G}_m \times \mathbb{G}_m$. We thus obtain a pairing

$$e^L\colon K(L) \times K(L) \to \mathbb{G}_m\,,$$

called the *commutator pairing* of the theta group. Note that e^L is alternating, meaning that $e^L(x,x) = 1$ for every $x \in K(L)$. For fixed $x \in K(L)(T)$ the morphisms $K(L)_T \to \mathbb{G}_{m,T}$ given by $y \mapsto e^L(x,y)$ resp. $y \mapsto e^L(y,x)$ are homomorphisms. In sum we find that the theta group $\mathscr{G}(L)$ gives rise to an alternating bilinear form e^L.

The alternating form e^L has the following properties.

eLProps **(8.6) Proposition.** (i) *If $f\colon X \to Y$ is a homomorphism of abelian varieties and L is a line bundle on Y then*

$$e^{f^*(L)} = e^L \circ (f,f) \qquad \text{on } f^{-1}(K(L)) \times f^{-1}(K(L))\,.$$

(ii) *If L and M are line bundles on X then $e^{L\otimes M} = e^L \cdot e^M$ on $K(L) \cap K(M)$.*
(iii) *If $[L] \in \mathrm{Pic}^0_{X/k}$ then $e^L = 1$.*
(iv) *For $x \in K(L)$ and $y \in n_X^{-1}(K(L)) = K(L^n)$ we have $e^{L^n}(x,y) = e^L(x,ny)$.*

Proof. (i) Note that $f^{-1}(K(L)) \subseteq K(f^*L)$, for if $x \in X$ then

ThetaGr:pullb
$$t_x^* f^* L = f^*(t_{f(x)}^* L)\,. \tag{2}$$

Now suppose T is a k-scheme and $x_1, x_2 \in f^{-1}(K(L))(T)$. We can cover T by Zariski-open subsets U such that there exist automorphisms $\varphi_{1,\mathbb{L}}$ and $\varphi_{2,\mathbb{L}}$ of the geometric line bundle $\mathbb{L}_U$, lying over the translations $t_{f(x_1)}$ and $t_{f(x_2)}$, respectively. As it suffices to show that $e^{f^*(L)} = e^L \circ (f,f)$ on $[f^{-1}(K(L)) \times f^{-1}(K(L))](U)$ for every such U, we may replace T by U.

By construction, the automorphism $[\varphi_{1,\mathbb{L}}, \varphi_{2,\mathbb{L}}]$ of $\mathbb{L}$ is the (fibrewise) multiplication by $e^L(f(x_1), f(x_2))$. Then $f^*\varphi_{1,\mathbb{L}}$ and $f^*\varphi_{2,\mathbb{L}}$ are automorphisms of $f^*\mathbb{L}$ which, by formula (2), lie

over the translations t_{x_1} resp. t_{x_2} on X. Since clearly $[f^*\varphi_{1,\mathbb{L}}, f^*\varphi_{2,\mathbb{L}}] = f^*[\varphi_{1,\mathbb{L}}, \varphi_{2,\mathbb{L}}]$, we find that $e^{f^*(L)}(x_1, x_2) = e^L(f(x_1), f(x_2))$.

(ii) If we have elements (φ_1, x), $(\varphi_2, y) \in \mathscr{G}(L)(T)$ and (ψ_1, x), $(\psi_2, y) \in \mathscr{G}(M)(T)$ then $(\varphi_{1,\mathbb{L}} \otimes \psi_{1,\mathbb{M}}) \circ (\varphi_{2,\mathbb{L}} \otimes \psi_{2,\mathbb{M}}) = (\varphi_{1,\mathbb{L}} \circ \varphi_{2,\mathbb{L}}) \otimes (\psi_{1,\mathbb{M}} \circ \psi_{2,\mathbb{M}})$ as (fibrewise linear) automorphisms of $\mathbb{L} \otimes \mathbb{M}$. The claim readily follows from this.

(iii) If the class of L is in Pic^0 then $K(L) = X$, and since X is complete the pairing $e^L\colon X \times X \to \mathbb{G}_m$ must be constant.

(iv) For $n \geqslant 0$ this follows by induction from (ii) and the bilinearity of the pairing e^L. The case $n \leqslant 0$ then follows from (ii) and (iii). □

Let k be a field. As we have seen in (4.41), the category $\boldsymbol{C}$ of commutative group schemes of finite type over k is abelian. In particular, given objects A and B of $\boldsymbol{C}$ we can form the groups $\mathrm{Ext}^n_{\boldsymbol{C}}(A, B)$ of n-extensions of A by B. If there is no risk of confusion we shall simply write $\mathrm{Ext}(A, B)$ for $\mathrm{Ext}^1_{\boldsymbol{C}}(A, B)$. Thus, the elements of $\mathrm{Ext}(A, B)$ are equivalence classes of exact sequences

$$0 \longrightarrow B \longrightarrow E \longrightarrow A \longrightarrow 0$$

where E is again an object of $\boldsymbol{C}$.

It can be shown (but this requires some work) that $\boldsymbol{C}$ does not contain any injective or projective objects. In particular, the computation of Ext-groups by homological methods cannot be done "directly" in $\boldsymbol{C}$. To repair this, one may work in an Ind- or Pro-category, cf. ?? and ??.

We shall further discuss extensions of group schemes in Chapter ??. In this chapter we only need the following two facts.

ExtGmFact **(8.7) Fact.** *Let k be an algebraically closed field.*

(i) *Write $\boldsymbol{C}$ for the category of commutative group schemes of finite type over k. If G is a finite commutative k-group scheme then $\mathrm{Ext}^1_{\boldsymbol{C}}(G, \mathbb{G}_m) = 0$. In other words, for every extension $0 \to \mathbb{G}_{m,k} \to \mathscr{G} \to G \to 0$ with $\mathscr{G}$ commutative, there exists a section $s\colon G \to \mathscr{G}$ which is a homomorphism of group schemes.*

(ii) *Let G be a finite k-group scheme of prime order. If $0 \to \mathbb{G}_{m,k} \to \mathscr{G} \to G \to 0$ is an exact sequence of k-group schemes then $\mathscr{G}$ is commutative.*

LBExtGM **(8.8)** We shall use the notion of a theta group to obtain an interpretation of $X^t = \mathrm{Pic}^0_{X/k}$ as being $\mathrm{Ext}_{\boldsymbol{C}}(X, \mathbb{G}_m)$, where $\boldsymbol{C}$ is the category of commutative k-group schemes of finite type.

In one direction this is quite easy. Namely, suppose that L is a line bundle on X which gives a class in Pic^0. Then $K(L) = X$ and the pairing e^L is trivial. This means that $G = \mathscr{G}(L)$ is a commutative group scheme fitting in an exact sequence

ThetaGr:GmExt
$$0 \longrightarrow \mathbb{G}_m \longrightarrow G \longrightarrow X \longrightarrow 0. \tag{3}$$

Thus, if $[L] \in \mathrm{Pic}^0_{X/k}$ then $\mathscr{G}(L)$ gives an element of $\mathrm{Ext}(X, \mathbb{G}_m)$.

Conversely, suppose G is a commutative k-group scheme for which we have an exact sequence (3). Then G can be viewed as a $\mathbb{G}_m$-torsor over X. Write L_G for the corresponding line bundle on X. (See Appendix ??) We claim that L_G is a line bundle in $\mathrm{Pic}^0_{X/k}$ with theta group isomorphic to G. To see this, suppose that G_1 and G_2 are commutative k-group schemes and that we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{j_1} & G_1 & \xrightarrow{\pi_1} & X & \longrightarrow & 0 \\
 & & \gamma\downarrow & & \downarrow\varphi & & \downarrow f & & \\
0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{j_2} & G_2 & \xrightarrow{\pi_2} & X & \longrightarrow & 0
\end{array}$$

with exact rows. Here f is only required to be a morphism of schemes and φ is required to be "fibrewise linear" (meaning that $\varphi(j_1(c)\cdot g) = j_2\gamma(c)\cdot\varphi(g)$ for all $c \in \mathbb{G}_m$ and $g \in G_1$.) Then φ gives an isomorphism of $\mathbb{G}_m$-torsors $G_1 \xrightarrow{\sim} f^*G_2$, hence it induces a homomorphism $\varphi\colon L_{G_1} \xrightarrow{\sim} f^*L_{G_2}$. Now take $G_1 = G_2 = G$ and let $\varphi = t_g$ be the translation over an element $g \in G$. If $x \in X$ is the image of g then we obtain a pair $(x,\varphi) \in \mathscr{G}(L_G)$. Since this construction is obviously functorial, it gives a homomorphism $h\colon G \to \mathscr{G}(L_G)$, compatible with the projections to X. In particular this shows that $K(L_G) = X$, so that the class of L_G is in $\mathrm{Pic}^0_{X/k}$. Furthermore it is clear that h is injective, and it follows that h is an isomorphism.

In sum, we can pass from line bundles L on X with $[L] \in \mathrm{Pic}^0$ to commutative group schemes G as in (3) and vice versa.

Xt=ExtGm **(8.9) Theorem.** *Let X be an abelian variety over a field k. Write $\boldsymbol{C}$ for the (abelian) category of commutative group schemes of finite type over k. Associating $\mathscr{G}(L)$ to a line bundle L with $[L] \in \mathrm{Pic}^0_{X/k}$ gives an isomorphism $X^t(k) \xrightarrow{\sim} \mathrm{Ext}^1_{\boldsymbol{C}}(X, \mathbb{G}_m)$.*

Proof. All that remains to be shown is that $L \cong L_{\mathscr{G}(L)}$ as line bundles on X. This follows from the construction in (8.3), as it shows that $\mathscr{G}(L)$ is (non-canonically) isomorphic to $\mathbb{L}^*$ as a $\mathbb{G}_m$-torsor. □

We shall later extend this result, obtaining an isomorphism of group schemes $X^t \xrightarrow{\sim} \mathscr{E}xt(X, \mathbb{G}_m)$. The main problem here is to set up a framework in which we can define $\mathscr{E}xt(X, \mathbb{G}_m)$ correctly.

§2. *Descent of line bundles over homomorphisms.*

Theta groups are a useful tool in studying when a line bundle on an abelian variety descends over an isogeny. The basic result is in fact just a reformulation of what we have seen in (7.2).

DescLB1 **(8.10) Theorem.** *Let $f\colon X \to Y$ be a surjective homomorphism of abelian varieties. Let L be a line bundle on X. Then there is a bijective correspondence between the $M \in \mathrm{Pic}(Y)$ with $f^*M \cong L$ and the homomorphisms $\mathrm{Ker}(f) \to \mathscr{G}(L)$ lying over the natural inclusion $\mathrm{Ker}(f) \hookrightarrow X$.*

Note that such homomorphisms $\mathrm{Ker}(f) \to \mathscr{G}(L)$ can only exist if $\mathrm{Ker}(f) \subseteq K(L)$ and $\mathrm{Ker}(f)$ is totally isotropic for the pairing e^L.

Proof. Write V_1 for the set of isomorphism classes of pairs (M,α) where M is a line bundle on Y and $\alpha\colon f^*M \xrightarrow{\sim} L$. Write V_2 for the set of isomorphism classes of line bundles M on Y such that $f^*M \cong L$. Using that $\mathrm{Aut}(M) = k^* = \mathrm{Aut}(L)$ we see that the natural map $V_1 \to V_2$ (forgetting α) is a bijection.

Write $H = \mathrm{Ker}(f)$. Then Y represents the fppf quotient of X by H. We have seen in (7.2) that the pairs $(M,\alpha) \in V_1$ correspond to the H-actions on L compatible with the natural action of H on X. It is an immediate translation of the definitions that such H-actions correspond to homomorphisms $H \to \mathscr{G}(L)$ lifting the inclusion $H \hookrightarrow X$. □

For isogenies over an algebraically closed field this leads to a handy criterion for when a line bundle descends. To prove it we shall make use of a result about extensions that we stated above.

LBDesc2 **(8.11) Corollary.** *Let X and Y be abelian varieties over an algebraically closed field k. Let $f\colon X \to Y$ be an isogeny. Then a line bundle L on X is the pull-back of a line bundle on Y if and only if* $\mathrm{Ker}(f)$ *is a subgroup scheme of $K(L)$ which is totally isotropic with respect to the pairing e^L.*

Proof. According to the preceding theorem one must check whether $\mathrm{Ker}(f) \hookrightarrow X$ can be lifted to a homomorphism $\mathrm{Ker}(f) \to \mathscr{G}(L)$. If it can then $\mathrm{Ker}(f)$ is a subgroup scheme of $K(L)$ and e^L is trivial when restricted to $\mathrm{Ker}(f) \times \mathrm{Ker}(f)$.

Conversely, if $\mathrm{Ker}(f)$ is a totally isotropic subgroup scheme of $K(L)$ then we consider the extension

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \pi^{-1}(\mathrm{Ker}(f))) \longrightarrow \mathrm{Ker}(f) \longrightarrow 0\,,$$

where $\pi\colon \mathscr{G}(L) \to K(L)$ is the projection. Since we assume $\mathrm{Ker}(f)$ to be totally isotropic, the group scheme $G := \pi^{-1}(\mathrm{Ker}(f)))$ is commutative. By (8.7), the extension splits, i.e., there exists a (homomorphic) section $\mathrm{Ker}(f) \to G$. □

LBDescRem **(8.12) Remarks.** (i) In the "if" statement of the theorem we really need the assumption that $k = \bar{k}$: if k is an arbitrary field and $\mathrm{Ker}(f)$ is a totally isotropic subgroup scheme of $K(L)$ then in general L descends to a line bundle on Y only after we pass to a finite extension of k.

(ii) The condition in (8.11) that the kernel of f is finite is necessary. If $K(L)$ is not finite (i.e., L is degenerate) then $Y := K(L)^0_{\mathrm{red}}$ is a nonzero abelian subvariety of X (assuming the ground field is perfect), and the quotient $Z = X/Y$ exists as an abelian variety; see Example (4.40). In this situation L is not, in general, the pullback of a line bundle on Z, even though $Y \subset K(L)$ is totally isotropic with respect to e^L. For example, if the class of L is in $\mathrm{Pic}^0_{X/k}$ then $Y = X$, so if L is non-trivial it is not a pullback from $Z = \{0\}$.

If $q\colon X \to Z$ is the quotient map then possibly after replacing the ground field by a finite separable extension it is still true that there exists a line bundle M on Z such that $L \otimes q^*M^{-1}$ is in $\mathrm{Pic}^0_{X/k}$; see Exercise (11.3) below.

LevelSgDef **(8.13) Definition.** A *level subgroup* of the theta group $\mathscr{G}(L)$ is a subgroup scheme $\tilde{H} \subset \mathscr{G}(L)$ such that $\mathbb{G}_m \cap \tilde{H} = \{1\}$, i.e., $\tilde{H}$ maps isomorphically to its image $H \subset K(L)$ under π.

With this notion of a level subgroup we have the following corollary to the theorem.

LBDesc3 **(8.14) Corollary.** *Let L be a line bundle on an abelian variety X over a field k. Then there is a bijective correspondence between the set of level subgroups $\tilde{H} \subset \mathscr{G}(L)$ and the set of isomorphism classes of pairs (f, M) where $f\colon X \to Y$ is a surjective homomorphisms and M is a line bundle on Y with $f^*M \cong L$. If $\tilde{H}$ corresponds to the pair (f, M) then* $\mathrm{Ker}(f) = \pi\big(\tilde{H}\big)$.

Proof. Given a level subgroup $\tilde{H} \subset \mathscr{G}(L)$, set $H := \pi(\tilde{H}) \subset K(L)$ and write $\xi\colon H \xrightarrow{\sim} \tilde{H} \subset \mathscr{G}(L)$ for the inverse of $\pi_{|\tilde{H}}$. The projection $f\colon X \to X/H =: Y$ is a surjective homomorphism and Theorem (8.10) shows that ξ corresponds to a line bundle M on Y with $f^*M \cong L$.

Conversely, if $f\colon X \to Y$ is a surjective homomorphism and M is a line bundle on Y with $f^*M \cong L$ then the image of the corresponding homomorphism $\mathrm{Ker}(f) \to \mathscr{G}(L)$ is a level subgroup. One now easily verifies that these two constructions give the desired bijection. □

Given a pair (f, M) as in the corollary, we can describe the theta group $\mathscr{G}(M)$ in terms of $\mathscr{G}(L)$ and the level subgroup $\tilde{H}$.

LevSgDesc **(8.15) Proposition.** *Let $f\colon X \to Y$ be a surjective homomorphism of abelian varieties. Let L*

be a line bundle on X and let M be a line bundle on Y with $f^*M \cong L$. Write $\tilde{H} \subset \mathscr{G}(L)$ for the level subgroup corresponding to the pair (f, M). Then $f^{-1}\big(K(M)\big) \subseteq K(L)$, the centralizer $C_{\tilde{H}}$ of $\tilde{H}$ inside $\mathscr{G}(L)$ is given by

$$C_{\tilde{H}} = \{g \in \mathscr{G}(L) \mid \pi(g) \in f^{-1}(K(M))\}\,,$$

and $\mathscr{G}(M) \cong C_{\tilde{H}}/\tilde{H}$.

Proof. As already remarked in the proof of (8.6), we have $f^{-1}\big(K(M)\big) \subseteq K(L)$. Write $H = \mathrm{Ker}(f) = \pi(\tilde{H}) \subset K(L)$. Let $\xi\colon H \to \mathscr{G}(L)$ be the homomorphism giving the canonical H-action on L. By construction, $\tilde{H}$ is the image of ξ. As remarked after (7.2), such an H-action on L (compatible with the H-action on X by translations) is nothing but a descent datum on L with respect to the morphism f.

Let T be a k-scheme and $(x, \varphi) \in \mathscr{G}(L)(T)$. Write $y = f(x) \in Y(T)$. Then $t_x^*\xi\colon H \to \mathscr{G}(t_x^*L)$ gives a descent datum on t_x^*L. This descent datum corresponds to the line bundle t_y^*M on Y, and we have a natural identification $f^*(t_y^*M) = t_x^*L$. Now the isomorphism $\varphi\colon L \xrightarrow{\sim} t_x^*L$ descends to an isomorphism $\psi\colon M \xrightarrow{\sim} t_y^*M$ if and only if φ is equivariant with respect to the descent data ξ and $t_x^*\xi$. This last condition precisely means that $(x, \varphi) \cdot (h, \xi(h)) = (h, \xi(h)) \cdot (x, \varphi)$ for all $(h, \xi(h)) \in \tilde{H}$, i.e., $(x, \varphi) \in C_{\tilde{H}}$. Thus we obtain a homomorphism $\gamma\colon C_{\tilde{H}} \to \mathscr{G}(M)$.

By construction, if (x, φ) maps to (y, ψ) then $f^*\psi = \varphi$ as homomorphisms from L to t_x^*L. Thus, if $(x, \varphi) \in \mathrm{Ker}(\gamma)$ then $x \in H = \mathrm{Ker}(f)$ and $\varphi = \xi(x)\colon L \xrightarrow{\sim} t_x^*L$. This means precisely that $(x, \varphi) \in \tilde{H} \subset C_{\tilde{H}}$. (Note that $\tilde{H}$ is commutative, being isomorphic to H, so that $\tilde{H}$ is indeed contained in $C_{\tilde{H}}$.)

Conversely, if $(\psi, y) \in \mathscr{G}(M)(T)$, then there is an fppf cover $T' \to T$ and an $x \in X(T')$ with $f(x) = y$. Then $(f^*\psi, x)$ is an element of $C_{\tilde{H}}(T')$ with $\gamma(f^*\psi, x) = (\psi, y)$. Thus γ is surjective and $\mathscr{G}(M) \cong C_{\tilde{H}}/\tilde{H}$.

Finally, it is clear from the above that $C_{\tilde{H}} \subseteq \{g \in \mathscr{G}(L) \mid \pi(g) \in f^{-1}(K(M))\}$. Conversely, if $g = (\varphi, x) \in \mathscr{G}(L)$ with $f(x) \in K(M)$ then we have shown that there exists an element of the form (φ', x) in $C_{\tilde{H}}$. As $C_{\tilde{H}}$ clearly contains the central subgroup $\mathbb{G}_{m,k} \subset \mathscr{G}(L)$, it follows that also $g \in C_{\tilde{H}}$. □

If x is a T-valued point of $K(L)$ for some k-scheme T then $y \mapsto e^L(x, y)$ defines a homomorphism $K(L)_T \to \mathbb{G}_{m,T}$. The bilinearity of the pairing e^L implies that the map $K(L) \to \mathit{Hom}\big(K(L), \mathbb{G}_m\big)$ given on points by $x \mapsto e^L(x, -)$ is a homomorphism of group schemes.

K(M)Cor **(8.16) Corollary.** *In the situation of the proposition we have $f^{-1}(K(M)) = H^\perp := \{k \in K(L) \mid e^L(k, h) = 1$ for every $h \in H\}$. We have $K(M) \cong H^\perp/H$.*

Proof. It easily follows from the definition of e^L that $C_{\tilde{H}} = \{(x, \varphi) \in \mathscr{G}(L) \mid x \in H^\perp\}$. With this remark the corollary directly follows from the proposition. □

§3. *Theta groups of non-degenerate line bundles.*

It will be helpful to reformulate some of the notions we have encountered without reference to line bundles.

AbstrThGr **(8.17) Definition.** Let k be a field. A *theta-group over k* is an exact sequence of k-group

schemes

$$0 \longrightarrow \mathbb{G}_{m,k} \xrightarrow{i} \mathscr{G} \xrightarrow{\pi} K \longrightarrow 0$$

such that $i(\mathbb{G}_{m,k})$ is contained in the center of $\mathscr{G}$ and K is commutative. The commutator pairing $e\colon K \times K \to \mathbb{G}_{m,k}$ of the theta group is the alternating bilinear pairing induced by the commutator $[\ ,\ ]\colon \mathscr{G} \times \mathscr{G} \to \mathscr{G}$. We say that two theta groups are isomorphic if they are isomorphic as extensions of a group scheme K by $\mathbb{G}_{m,k}$.

Suppose that we have a theta group as above such that K is finite. If T is a k-scheme and $x \in K(T)$ then $y \mapsto e(x,y)$ defines a homomorphism $K_T \to \mathbb{G}_{m,T}$, i.e., an element of $K^D(T)$. In this way the pairing e gives a homomorphism $\nu\colon K \to K^D$. The relation $e(x,y) = e(y,x)^{-1}$ gives that $\nu^D = \nu^{-1}$.

NondegThGr **(8.18) Definition.** A theta group $\mathscr{G}$ as above is said to be *non-degenerate* if K is finite and if $\nu\colon K \to K^D$ is an isomorphism.

Notice that the non-degeneracy condition can also be expressed by saying that $i(\mathbb{G}_{m,k})$ is the center of $\mathscr{G}$.

As the terminology suggests, the theta group of a non-degenerate line bundle is non-degenerate. This is a consequence of the following result.

MaxIsotrop **(8.19) Proposition.** *Let L be a non-degenerate line bundle on an abelian variety X. If $H \subset K(L)$ is a subgroup scheme which is maximal totally isotropic with respect to the pairing e^L then $H = H^\perp$ and* $\operatorname{rank}(H)^2 = \operatorname{rank}(K(L))$.

Proof. It suffices to prove this over an algebraically closed field. Write $f\colon X \to X/H =: Y$ for the projection. By (8.11) there is a line bundle M on Y with $f^*M \cong L$.

We claim that $K(M) = \{1\}$. Suppose not. Then there is a subgroup scheme $K' \subset K(M)$ of prime order. By (8.7) this K' is totally isotropic for e^M. Then (i) of (8.6) shows that $f^{-1}(K')$ is totally isotropic for e^L. As $H \subsetneq f^{-1}(K')$ this contradicts our choice of H. So indeed $K(M) = \{1\}$. It then follows from (8.16) that $H^\perp = H$ and by (7.6) we have $\operatorname{rank}(K(L)) = \operatorname{rank}(H)^2$. □

NondegCor **(8.20) Corollary.** *If L is a non-degenerate line bundle on an abelian variety then the theta group $\mathscr{G}(L)$ is non-degenerate.*

Proof. Choose H as above. Remark that $\nu\colon K(L) \to K(L)^D$ fits in a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^\perp & \longrightarrow & K(L) & \longrightarrow & K(L)/H^\perp & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \nu'} & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \bar\nu} & & \\
0 & \longrightarrow & [K(L)/H]^D & \longrightarrow & K(L)^D & \longrightarrow & H^D & \longrightarrow & 0\,.
\end{array}$$

By definition of $H^\perp$ the homomorphism $\bar\nu$ is injective. Now $\nu^D = \nu^{-1}$ so that $\bar\nu^D\colon H \to [K(L)/H^\perp]^D$ is the map obtained by restricting ν^{-1} to H. But $H = H^\perp$, so we find that $\nu' = (\bar\nu^D)^{-1}$ is surjective. By rank considerations it follows that ν' and $\bar\nu$ are isomorphisms. Hence ν is an isomorphism. □

HeisGr **(8.21)** *Heisenberg groups.* We now discuss an important example of non-degenerate theta-groups, the so-called Heisenberg groups.

We work over a field k. Let H be a finite abelian group; we shall view it as a (constant) k-group scheme. Write $H^D := \mathrm{Hom}(H, \mathbb{G}_{m,k})$ for its Cartier dual. (If $k = \overline{k}$ one would also refer to H^D as the character group of H.) So

$$H \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})\,, \qquad H^D \cong \mu_{d_1,k} \times \cdots \times \mu_{d_n,k}\,,$$

with $d_1|d_2|\cdots|d_n$. To the pair (H, H^D) we associate a Heisenberg group $\mathscr{H}$; it is defined by $\mathscr{H} = \mathbb{G}_{m,k} \times H \times H^D$ as a k-scheme, with multiplication given by

ThetaGr:Heisenb
$$(\lambda, x, \chi) \cdot (\lambda', x', \chi') = (\lambda\lambda'\chi'(x), x + x', \chi\chi')\,. \tag{4}$$

Then $\mathscr{H}$ is a theta-group: we have an exact sequence

$$0 \longrightarrow \mathbb{G}_{m,k} \longrightarrow \mathscr{H} \longrightarrow H \times H^D \longrightarrow 0\,.$$

The commutator pairing e: $(H \times H^D) \times (H \times H^D) \to \mathbb{G}_{m,k}$ is given by $e((x,\chi),(x',\chi')) = \chi'(x)\chi(x')^{-1}$. As this is clearly a perfect pairing, $\mathscr{H}$ is non-degenerate.

The construction clearly generalizes to the case where we start with an arbitrary finite commutative k-group scheme H. For $\mathscr{H}$ we now take $\mathbb{G}_{m,k} \times H \times H^D$, and the group structure is again given on points by (4). We refer to the resulting theta group as the Heisenberg group associated to the group scheme H (or to the pair (H, H^D)).

Our next goal is to show that under suitable assumptions the theta group of a line bundle can be described as a Heisenberg group.

LagrLem **(8.22) Lemma.** *Let $0 \longrightarrow \mathbb{G}_{m,k} \longrightarrow \mathscr{G} \xrightarrow{\pi} K \longrightarrow 0$ be a non-degenerate theta group over a field k. Let $H \subset K$ be a subgroup scheme. Consider the following conditions.*

(i) *H is maximal totally isotropic w.r.t. the commutator pairing e: $K \times K \to \mathbb{G}_{m,k}$,*

(ii) *H is totally isotropic and $\mathrm{rank}(H)^2 = \mathrm{rank}(K)$,*

(iii) *$H = H^\perp$.*

Then (iii) $\Leftrightarrow$ (ii) $\Rightarrow$ (i). *If k is algebraically closed the three conditions are equivalent.*

Proof. The isomorphism ν: $K \xrightarrow{\sim} K^D$ induces an isomorphism $K/H^\perp \xrightarrow{\sim} H^D$. In particular, $\mathrm{rank}(K) = \mathrm{rank}(H) \cdot \mathrm{rank}(H^\perp)$. Now H is totally isotropic precisely if $H \subseteq H^\perp$. This readily gives (iii) $\Leftrightarrow$ (ii) $\Rightarrow$ (i).

To see that (i) $\Rightarrow$ (iii) if $k = \overline{k}$, let H be maximal totally isotropic and assume that $H \subsetneq H^\perp$. By (8.7) the extension $0 \longrightarrow \mathbb{G}_{m,k} \longrightarrow \pi^{-1}(H) \xrightarrow{\pi} H \longrightarrow 0$ splits, so there exists a level subgroup $\tilde{H} \subset \mathscr{G}$ with $\pi(\tilde{H}) = H$. Writing $\mathscr{G}' := \pi^{-1}(H^\perp)/\tilde{H}$ we obtain a new theta group $0 \longrightarrow \mathbb{G}_{m,k} \longrightarrow \mathscr{G}' \xrightarrow{\pi'} H^\perp/H \longrightarrow 0$. As $H \neq H'$ and $k = \overline{k}$ we can choose a subgroup scheme $\Gamma \subset H^\perp/H$ of prime order. By (8.7) ${\pi'}^{-1}(\Gamma)$ is commutative. It follows that the inverse image of Γ under $H^\perp \to H^\perp/H$ is totally isotropic. This contradicts the assumption that H is maximal totally isotropic. □

LagrDef **(8.23) Definition.** Let $\mathscr{G}$ be a non-degenerate theta group over a field k.

(i) A k-subgroup scheme $H \subset K$ satisfying (ii) and (iii) in (8.22) is called a *Lagrangian subgroup*. If $\tilde{H} \subset \mathscr{G}$ is a level subgroup then we say that $\tilde{H}$ is a *Lagrangian level subgroup* if $\pi(\tilde{H}) \subset K$ is Lagrangian.

(ii) A *Lagrangian decomposition* of K is an isomorphism $K \xrightarrow{\sim} H_1 \times H_2$ such that ν: $K \xrightarrow{\sim} K^D$ induces an isomorphism $\bar{\nu}$: $H_1 \xrightarrow{\sim} H_2^D$.

Condition (i) in (8.22) shows that for every non-degenerate theta group over $k = \overline{k}$ there exist Lagrangian subgroups $H \subset K$. By (8.7) every such H can be lifted (still with $k = \overline{k}$) to a Lagrangian level subgroup of $\mathscr{G}$.

If $\mathscr{H}$ is a Heisenberg group then, with the notations of (8.21), H and H^D are Lagrangian subgroups. So, a necessary condition for a theta group $\mathscr{G}$ to be a Heisenberg group is that there exists a Lagrangian decomposition. This is not always the case. For instance, suppose that E is a supersingular elliptic curve over a field k of characteristic $p > 0$ and that $\mathscr{G}$ is a theta group with finite quotient equal to $E[p]$. One can show that $E[p]$ has a *unique* non-trivial subgroup scheme, isomorphic to α_p. It follows that $\mathscr{G}$ is not a Heisenberg group $\mathscr{H}$ as in (8.21).

If the ground field is algebraically closed and K admits a Lagrangian decomposition then we can describe $\mathscr{G}$ as a Heisenberg group.

LagrDecLem **(8.24) Lemma.** *Suppose $\mathscr{G}$ is a non-degenerate theta group over an algebraically closed field k.*

(i) *Assume that $K = \mathscr{G}/\mathbb{G}_{m,k}$ admits a Lagrangian decomposition, say $K \cong H_1 \times H_2$. Then $\mathscr{G}$ is isomorphic, as a theta group, to the Heisenberg group associated to the pair (H_1, H_1^D).*

(ii) *If $\mathrm{rank}(K)$ is prime to $\mathrm{char}(k)$ then K admits a Lagrangian decomposition.*

Proof. (i) Lift H_i $(i = 1, 2)$ to a Lagrangian level subgroup $\tilde{H}_i \subset \mathscr{G}$ and write $\xi_i \colon H_i \xrightarrow{\sim} \tilde{H}_i$ for the inverse of the projection. Write $\mathscr{H} = \mathbb{G}_{m,k} \times H_1 \times H_1^D$ for the Heisenberg group associated to the pair (H_1, H_1^D). If $\alpha \colon H_1^D \xrightarrow{\sim} H_2$ is the inverse of $\bar{\nu}^D \colon H_2 \xrightarrow{\sim} H_1^D$ then the map $\mathscr{H} \to \mathscr{G}$ given by

$$(\lambda, x, \chi) \mapsto i(\lambda) \cdot \xi_2(\alpha(\chi)) \cdot \xi_1(x)$$

gives the desired isomorphism of theta groups.

The proof of (ii) is done by the usual procedure of putting a symplectic pairing in canonical form. For details we refer to Exercise ??. □

We apply this to non-degenerate line bundles L such that $K(L)$ is finite and prime to $\mathrm{char}(k)$. This last condition is equivalent to saying that the isogeny $\varphi_L \colon X \to X^t$ is separable (see Exercise ??), hence we say that L is a non-degenerate line bundle *of separable type.*

ThGr=Heis **(8.25) Corollary.** *Let k be algebraically closed field. Let X be an abelian variety over k and let L be a non-degenerate line bundle on X of separable type. Then there is a sequence of integers $d_1|d_2|\cdots|d_n$, called the type of L such that $\mathscr{G}(L)$ is isomorphic to the Heisenberg group associated to the group $H = (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})$.*

Here is another case where a theta group can be descibed as a Heisenberg group.

ThGr=HeisExa **(8.26) Example.** Let X be an abelian variety. If $\mathscr{P} = \mathscr{P}_X$ is the Poincaré bundle on $X \times X^t$ then we know from Exercise (7.5) that $\varphi_{\mathscr{P}} \colon X \times X^t \to X^t \times X$ is given by $(x, y) \mapsto (y, x)$. Hence $K(\mathscr{P}) = \{0\}$ and $\mathscr{G}(\mathscr{P}) = \mathbb{G}_m$ is the trivial theta group.

Next consider an isogeny $h \colon X \to X^t$, and let $M := (1 \times h)^* \mathscr{P}_X$ on $X \times X$. (If $h = \varphi_L$ for some non-degenerate line bundle L then $M = \Lambda(L)$.) Note that also $M = (h^t \times 1)^* s^* \mathscr{P}$, where $s \colon X \times X^t \xrightarrow{\sim} X^t \times X$ is the isomorphism switching the two factors. Identifying $\mathrm{Ker}(h^t) = \mathrm{Ker}(h)^D$ as in Thm. (7.5) we find that $\{0\} \times \mathrm{Ker}(h) \subset K(M)$ and $\mathrm{Ker}(h)^D \times \{0\} \subset K(M)$, and by comparing ranks it follows that in fact $K(M) = \mathrm{Ker}(h)^D \times \mathrm{Ker}(h)$.

We claim that the theta group $\mathscr{G}(M)$ is naturally isomorphic to the Heisenberg group $\mathscr{H}$ associated to the pair $\big(\mathrm{Ker}(h)^D, \mathrm{Ker}(h)\big)$. We already have natural actions of $\mathrm{Ker}(h)^D \times \{0\}$ and $\{0\} \times \mathrm{Ker}(h)$ on M, compatible with the actions on the basis by translations; this realizes

$\mathrm{Ker}(h)^D$ and $\mathrm{Ker}(h)$ as Lagrangian level subgroups of $\mathscr{G}(M)$. An isomorphism $\mathscr{H} \xrightarrow{\sim} \mathscr{G}(M)$ is then obtained in the same manner as in the proof of (8.24).

§4. *Representation theory of non-degenerate theta groups.*

As we have seen in (2.27), an abelian variety X of dimension g can only be embedded in projective spaces of dimension at least $2g$. Hence we will need, at least for large g, a rather large number of equations to describe X. In a beautiful series of papers, Mumford [1] showed how one can nevertheless set up a systematic study of the equations defining an abelian variety. Theta groups play a crucial role in this. To explain why, suppose we choose an ample line bundle L on X. To find the equations for X in the projective embedding defined by (some power of) L, we must try to describe the kernel of the map

$$\mathrm{Sym}^\bullet H^0(X, L) \longrightarrow \bigoplus_{n \geqslant 0} H^0(X, L^n)$$

given by cup-product. The key observation is that $H^0(X, L)$ has a natural action of $\mathscr{G}(L)$. Under suitable assumptions we can identify $\mathscr{G}(L)$ with a Heisenberg group, in which case the representation $H^0(X, L)$ can be described very precisely. This then allows to choose a basis for $H^0(X, L)$ (the elements of which are referred to as theta functions) that has particular properties.

What is sketched here is discussed in much greater detail in Chapter ?? below. First, however, we shall study representations of non-degenerate theta groups.

RepWtDef **(8.27) Definition.** Let $\mathscr{G}$ be a theta group over a field k. If $\rho\colon \mathscr{G} \to \mathrm{GL}(V)$ is a representation of $\mathscr{G}$ then we say that ρ is a representation *of weight* n ($n \in \mathbb{Z}$) if $\rho \circ i\colon \mathbb{G}_{m,k} \to \mathrm{GL}(V)$ is given by $z \mapsto z^n \cdot \mathrm{id}_V$.

We shall mainly be interested in representations of weight 1.

HeisRepThm **(8.28) Theorem.** *Let k be an algebraically closed field. Let $0 \to \mathbb{G}_{m,k} \to \mathscr{G} \to K \to 0$ be a non-degenerate theta group over k such that $\mathrm{rank}(K)$ is prime to $\mathrm{char}(k)$. Then $\mathscr{G}$ has a unique irreducible representation $\rho = \rho_{\mathscr{G}} : \mathscr{G} \to \mathrm{GL}(V)$ of weight 1 (up to isomorphism). We have $\dim(V)^2 = \mathrm{rank}(K)$.*

If W is any representation of $\mathscr{G}$ of weight 1 then W is isomorphic to a direct sum of copies of $\rho_{\mathscr{G}}$. More precisely, if $\tilde{H} \subset \mathscr{G}$ is a maximal level subgroup then $W \cong V^{\oplus a}$ with $a = \dim_k(W^{\tilde{H}})$ equal to the dimension of the subspace of $\tilde{H}$-invariants in W.

Proof. Choose a maximal level subgroup $\tilde{H} \subset \mathscr{G}$. (By (8.22) it is Lagrangian.) As $\mathrm{rank}(K)$ is prime to $\mathrm{char}(k)$ and $k = \overline{k}$ we can view K and $\tilde{H}$ as constant groups.

Let $\tau\colon \mathscr{G} \to \mathrm{GL}(W)$ be a representation of weight 1. Viewing W as a module under $\tilde{H}$ (which is abelian) it decomposes as a direct sum of character spaces:

$$W = \bigoplus_{\chi \in \mathrm{Hom}(\tilde{H}, k^*)} W_\chi\,, \qquad \text{with} \quad W_\chi := \{w \in W \mid \tau(h)(w) = \chi(h) \cdot w \text{ for all } h \in \tilde{H}\}\,.$$

An element $g \in \mathscr{G}$ defines a character $\chi_g \in \mathrm{Hom}(\tilde{H}, k^*)$ by $g^{-1} \cdot h \cdot g = \chi_g(h) \cdot h$. (That is, $\chi_g(h) = [g^{-1}, h] \in \mathbb{G}_m$.) Then $\tau(g)W_\chi = W_{\chi \cdot \chi_g}$.

As $\tilde{H}$ is Lagrangian, its centralizer $C_{\tilde{H}} \subset \mathscr{G}$ equals $\mathbb{G}_m \cdot \tilde{H}$ (cf. the proof of (8.16)) and $g \mapsto \chi_g$ gives an isomorphism

$$\gamma\colon C_{\tilde{H}}\backslash\mathscr{G} \xrightarrow{\sim} \mathrm{Hom}(\tilde{H}, k^*)\,.$$

As furthermore the elements of $C_{\tilde{H}} = \mathbb{G}_m \cdot \tilde{H}$ act on each W_χ through scalar multiplications, it follows that: (a) all W_χ have the same dimension, and (b) if $0 \neq w \in W_\chi$ then the elements $\tau(g)(w)$ span a $\mathscr{G}$-submodule $V \subset W$ with $\dim(V \cap W_\chi) = 1$ for all χ.

Choose a section $\sigma\colon \mathrm{Hom}(\tilde{H}, k^*) \cong C_{\tilde{H}}\backslash\mathscr{G} \to \mathscr{G}$ of the projection $\mathscr{G} \twoheadrightarrow C_{\tilde{H}}\backslash\mathscr{G}$. Suppose that W is irreducible. Choose $0 \neq w_1 \in W_1$, where $1 \in \mathrm{Hom}(\tilde{H}, k^*)$ is the trivial character. For $\chi \in \mathrm{Hom}(\tilde{H}, k^*)$ set $w_\chi := \tau(\sigma(\chi))(w_1) \in W_\chi$. Then $\{w_\chi\}$ is a k-basis of W. If $g \in \mathscr{G}$ has image η in $\mathrm{Hom}(\tilde{H}, k^*)$ then there is a unique $c = c(g,\chi) \in C_{\tilde{H}}$ such that $g \cdot \sigma(\chi) = c \cdot \sigma(\eta \cdot \chi)$. Then the representation τ is completely described by $\tau(g)(w_\chi) = \tau(c(g,\chi))(w_{\eta\chi})$. (Note that $c(g,\chi) \in \mathbb{G}_m \cdot \tilde{H}$, so we know how it acts on the spaces W_ψ.) As the elements $c(g,\chi)$ only depend on the structure of $\mathscr{G}$ and the chosen section σ, it follows that there is at most one irreducible representation of weight 1, up to isomorphism. Conversely, our description gives a simple recipe of how to construct one. (See also (8.29) below.) This shows that there is a unique irreducible representation $\rho\colon \mathscr{G} \to \mathrm{GL}(V)$ of weight 1.

To prove the last assertions, write $r = \mathrm{rank}(K) = \mathrm{rank}(\tilde{H})^2$ and consider the subgroup $\mathscr{G}[r] \subset \mathscr{G}$ of elements g with $g^r = 1$. As $\mathscr{G}$ is generated by $\mathbb{G}_m$ and $\mathscr{G}[r]$, a weight 1 representation W of $\mathscr{G}$ is completely reducible (i.e., a direct sum of irreducible representations) if and only if it is completely reducible as a representation of $\mathscr{G}[r]$. But $\mathscr{G}[r]$ is a finite group of order not divisible by $\mathrm{char}(k)$. Therefore all k-representations of $\mathscr{G}[r]$ are completely reducible. If $W \cong V^{\oplus a}$ then $a = \dim(W_1) = \dim(W^{\tilde{H}})$. □

StRepHeis **(8.29)** *The standard representation of a Heisenberg group.* By (8.24), the theta group $\mathscr{G}$ in the theorem is isomorphic to a Heisenberg group $\mathscr{H} = \mathbb{G}_{m,k} \times H \times H^D$ with

$$H \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})\,, \qquad H^D = \mathrm{Hom}(H, k^*) \cong \mu_{d_1}(k) \times \cdots \times \mu_{d_n}(k)\,.$$

We can take $\tilde{H} := \{(1,h,1) \mid h \in H\}$ as a Lagrangian level subgroup. In the proof of the theorem we have seen how to construct an irreducible weight 1 representation. The result can be described as follows.

Let V be the space of functions on H with values in k. Then we have a representation $\rho\colon \mathscr{H} \to \mathrm{GL}(V)$ given by $[\rho(\lambda,x,\chi)(f)](h) = \lambda \cdot \chi(h) \cdot f(x+h)$ for $f \in V$ and $h \in H$. One easily checks that this indeed gives an irreducible representation of weight 1.

More generally, let H be an arbitrary finite commutative group scheme over a field k. Write $A_H := \Gamma(H, O_H)$ for its affine algebra and let $\mathscr{H} = \mathbb{G}_{m,k} \times H \times H^D$ be the associated Heisenberg group, as defined in (8.21). Then we have a representation

$$\rho\colon \mathscr{H} \longrightarrow \mathrm{GL}(A_H)$$

by letting $(\lambda,x,\chi) \in \mathscr{H}$ act on A_H by

$$f \mapsto \lambda \cdot \chi \cdot t_x^*(f)\,,$$

where we view χ as an invertible element of A_H. More precisely, we should write $(\lambda,x,\chi) \in \mathscr{H}(T)$, where T is a k-scheme. For simplicity, assume that $T = \mathrm{Spec}(R)$ is affine. Then $\rho(\lambda,x,\chi)$ is an R-linear automorphism of $A_H \otimes_k R$. Now notice that χ is given by an invertible element of $A_H \otimes_k R$.

Again this resentation ρ is irreducible of weight 1. We shall refer to it as ??.

RepGeneral **(8.30)** We now wish to lift the restrictions on the characteristic of k. In the case considered above the desired representation was realized as a representation on the space of functions on a Lagrangian level subgroup. Therefore is natural to consider representations of $\mathscr{G}$ on spaces of functions on $\mathscr{G}$.

We work over an algebraically closed field k. As K is a semi-local scheme, we can trivialize $\mathscr{G}$ as a $\mathbb{G}_m$-torsor over K. So, we can choose an isomorphism $\mathscr{G} \xrightarrow{\sim} \mathbb{G}_m \times K$ of K-schemes via which the $\mathbb{G}_m$-action on $\mathscr{G}$ corresponds to multiplication in $\mathbb{G}_m$ on the right hand term. Writing $K = \operatorname{Spec}(A_0)$ this gives $\mathscr{G} = \operatorname{Spec}(B)$, with

$$B = A_0[t, t^{-1}] = \bigoplus_{i \in \mathbb{Z}} A_i \,, \qquad \text{where we set} \quad A_i := A_0 \cdot t^i \,.$$

We can view A_i as the vector space of those functions $f\colon \mathscr{G} \to \mathbb{A}^1$ such that $f(\lambda x) = \lambda^i \cdot f(x)$ for all $\lambda \in \mathbb{G}_m$. (This has to be read functorially: if R is a k-algebra then $A_i \otimes_k R = \{f \in \operatorname{Hom}_R(\mathscr{G}_R, \mathbb{A}^1_R) \mid f(\lambda x) = \lambda^i \cdot f(x) \text{ for all } \lambda \in \mathbb{G}_m\}$.)

As will become clear in the proof of (8.32), the space A_1 is the most interesting for us. (That is, if we want to study representations of weight 1.) Note that $\dim(A_1)$ is the square of the dimension of the irreducible $\mathscr{G}$-representation that we are looking for. We consider the action of $\mathscr{G} \times \mathscr{G}$ on A_1 given by

$$[(g,h) \cdot f](x) = f(h^{-1}xg) \qquad \text{for} \quad f \in A_1 \,, (g,h) \in \mathscr{G} \times \mathscr{G} \quad \text{and} \quad x \in \mathscr{G} \,.$$

(Again this has to be read functorially.)

A1Lemma **(8.31) Lemma.** *With this action A_1 is an irreducible $\mathscr{G} \times \mathscr{G}$-module.*

Proof. First we look at the diagonal $\mathscr{G}$-action. If $g \in \mathscr{G}$ and $f \in A_1$ then $(g,g) \cdot f$ is the function given by

$$\begin{aligned} x \mapsto f(g^{-1}xg) &= f(g^{-1}xgx^{-1} \cdot x) \\ &= f([g^{-1}, x] \cdot x) \\ &= [g^{-1}, x] \cdot f(x) \qquad\qquad (\text{because } f \in A_1 \text{ and } [g^{-1}, x] \in \mathbb{G}_m) \\ &= e(\pi(g)^{-1}, \pi(x)) \cdot f(x) \,. \end{aligned}$$

Each $\gamma \in K$ defines a character $e(\gamma, -)\colon K \to \mathbb{G}_m$. If χ is any such character then $\chi \circ \pi\colon \mathscr{G} \to \mathbb{G}_m \subset \mathbb{A}^1$ can be viewed as an element of A_0. The previous calculations show that $\mathscr{G} \xrightarrow{\Delta} \mathscr{G} \times \mathscr{G} \to \mathrm{GL}(A_1)$ factors through $\mathscr{G} \twoheadrightarrow K$ and that the resulting action of K on A_1 is given by

$$\gamma \cdot f = [\pi \circ e(\gamma^{-1}, -)] \cdot f \qquad \text{for} \quad \gamma \in K \,, f \in A_1 \,.$$

Suppose that $E \subset A_1$ is a $\mathscr{G} \times \mathscr{G}$-submodule. The non-degeneracy of our theta group means that every character $\chi\colon K \to \mathbb{G}_m$ is of the form $e(\gamma^{-1}, -)$ for some $\gamma \in K$. Furthermore, the k-characters χ form a k-basis of the k-algebra A_0; see Exercise ??. It thus follows from the above that E is an A_0-submodule of A_1. But $A_1 = A_0 \cdot t$, so E is of the form IA_1 with I an ideal of A_0.

So far we have only used the diagonal action of $\mathscr{G}$. Using the full action of $\mathscr{G} \times \mathscr{G}$ again we see that E is stable under all translations by elements of $\mathscr{G}$. Combined with the previous it now readily follows that $E = (0)$ or $E = A_1$ $\square$

We can now generalize Theorem (8.28).

HeisRepBIS **(8.32) Theorem.** *Let $\mathscr{G}$ be a non-degenerate theta group over an algebraically closed field k. Then $\mathscr{G}$ has a unique irreducible representation $\rho = \rho_{\mathscr{G}}\colon \mathscr{G} \to \mathrm{GL}(V)$ of weight 1 (up to isomorphism). We have $\dim(V)^2 = \mathrm{rank}(K)$. If W is any representation of $\mathscr{G}$ of weight 1 then W is isomorphic to a direct sum of copies of $\rho_{\mathscr{G}}$.*

Proof. Let $\tau\colon \mathscr{G} \to \mathrm{GL}(W)$ be a representation of $\mathscr{G}$ of weight 1. Then τ gives rise to a homomorphism of $\mathscr{G} \times \mathscr{G}$-modules $r\colon W^* \otimes W \to A_1$, by

$$r(\varphi \otimes w)(g) = \varphi(\tau(g)(w)) \qquad \text{for} \quad \varphi \in W^*\,, w \in W \text{ and } \quad g \in \mathscr{G}\,.$$

Suppose that W is irreducible. Then $W^* \otimes_k W$ is an irreducible $\mathscr{G} \times \mathscr{G}$-module. (Here we need that $k = \overline{k}$! The point is that $\mathrm{End}_{\mathscr{G}\times\mathscr{G}}(W^* \otimes W) = \mathrm{End}_{\mathscr{G}}(W^*) \otimes_k \mathrm{End}_{\mathscr{G}}(W)$. As $k = \overline{k}$ the irreducibility of W implies that $\mathrm{End}_{\mathscr{G}}(W) = k = \mathrm{End}_{\mathscr{G}}(W^*)$.) As r is obviously not the zero map it follows from the lemma that r is an isomorphism. We conclude that $A_1 \cong W \oplus \cdots \oplus W$ ($\dim(W)$ factors) as a $\mathscr{G}$-module, that there is a unique irreducible $\mathscr{G}$-module of weight 1, and that $\mathrm{rank}(K) = \dim(A_1)$ is the square of its dimension. We also see that A_1 is completely reducible as a $\mathscr{G}$-module.

Now let W be an arbitrary $\mathscr{G}$-module of weight 1 again. Then r gives a k-linear map $r'\colon W \to \mathrm{Hom}(W^*, A_1) = W \otimes A_1$, sending $w \in W$ to $\varphi \mapsto r(\varphi \otimes w)$. From $r(\varphi \otimes w)(1) = \varphi(w)$ we see that r' is injective. Moreover, if we let $\mathscr{G}$ act on $W \otimes A_1$ through its action on A_1 then r' is $\mathscr{G}$-equivariant. We conclude that W is isomorphic to a $\mathscr{G}$-submodule of $A_1^{\dim(W)}$. As A_1 is a completely reducible $\mathscr{G}$-module, W is also completely reducible. □

Exercises.

Ex:K+pairing **(8.1)** Let k be an algebraically closed field. Let K be a finite commutative group scheme of order prime to $\mathrm{char}(k)$. Let $e\colon K \times K \to \mathbb{G}_m$ be a non-degenerate alternating bilinear pairing, i.e., e is a morphism of k-schemes such that (a) $e(x,y) = e(y,x)^{-1}$, (b) for fixed $x \in K$ the maps $y \mapsto e(x,y)$ and $y \mapsto e(y,x)$ are homomorphisms, and (c) the homomorphism $K \to K^D$ given by $x \mapsto e(x,-)$ is an isomorphism.

(i) Show that K is isomorphic to a constant group scheme of the form

$$K \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})\,,$$

where we may require that $d_1 | d_2 | \cdots | d_n$. (And if $\mathrm{char}(k) = p > 0$ then $p \nmid d_n$.)

(ii) Choose an element $a \in K$ such that K is a product $K = \langle a \rangle \times K'$. Let d be the order of a and let $\zeta_d \in k$ be a primitive dth root of unity. Show that there is a unique $b \in K$ with $e(a,b) = \zeta_d$ and $e(k,b) = 1$ for all $k \in K'$.

(iii) Let $K'' := \{k \in K' \mid e(a,k) = 1\}$. Show that K decomposes as a product of groups $K = \langle a \rangle \times \langle b \rangle \times K''$. Also show that the restriction of e to $K'' \times K''$ is again non-degenerate.

(iv) Prove that there exists a finite commutative k-group scheme H and an isomorphism $K \xrightarrow{\sim} H \times H^D$ via which the pairing e corresponds to the pairing on $H \times H^D$ given by

$$\big((x,\chi),(x',\chi')\big) \mapsto \chi'(x) \cdot \chi(x')^{-1}\,.$$

In this chapter we study the cohomology of line bundles on abelian varieties. The main results are the Riemann-Roch Theorem (9.11) and the Vanishing Theorem for non-degenerate line bundles (9.14). The key step in deriving these results is the computation of the cohomology of the Poincaré bundle on $X \times X^t$.

CohPBThm **(9.1) Theorem.** *Let X be a g-dimensional abelian variety over a field k. Let $\mathscr{P}$ be the Poincaré bundle on $X \times X^t$ and write $p_2\colon X \times X^t \to X^t$ for the second projection. Then the sheaves $R^n p_{2,*}\mathscr{P}$ and the cohomology of $\mathscr{P}$ are given by*

$$R^n p_{2,*}\mathscr{P} = \begin{cases} 0 & \text{if } n \neq g; \\ i_0(k) & \text{if } n = g, \end{cases}$$

and

$$H^n(X \times X^t, \mathscr{P}) = \begin{cases} 0 & \text{if } n \neq g; \\ k & \text{if } n = g. \end{cases}$$

Here $i_0(k)$ denotes the skyscraper sheaf at $0 \in X^t$ with stalk k.

Proof. As the proof is a somewhat long we divide it into steps, (9.2)–(9.9).

CPBStep1 **(9.2)** We look at the higher direct image sheaves $R^n p_{2,*}\mathscr{P}$ on X^t. If $y \in X^t \setminus \{0\}$ then the restriction of $\mathscr{P}$ to $X \times \{y\}$ is a non-trivial line bundle on X with class in Pic^0. As was proven in (7.19) such sheaves have zero cohomology. Applying (i) of (7.20), it follows that $R^n p_{2,*}\mathscr{P}$ has support only at $0 \in X^t$, for all n. As the closed point 0 is a zero-dimensional subscheme of X^t we have $H^i(X^t, R^n p_{2,*}\mathscr{P}) = 0$ for all $i \geqslant 1$. (Use HAG, III, Thm. 2.7 and Lemma 2.10.)

Applying the Leray spectral sequence

$$E_2^{p,q} = H^p(X^t, R^q p_{2,*}\mathscr{P}) \;\Rightarrow\; H^{p+q}(X \times X^t, \mathscr{P})$$

we find that

CohomLB:HnP $$H^n(X \times X^t, \mathscr{P}) \cong H^0(X^t, R^n p_{2,*}\mathscr{P})\,. \tag{1}$$

As p_2 is projective of relative dimension g we have (HAG, III, Cor. 11.2) $R^n p_{2,*}\mathscr{P} = 0$ for all $n > g$. Hence also $H^n(X \times X^t, \mathscr{P}) = 0$ for $n > g$.

Next we apply Serre duality to the Poincaré bundle. We have $\mathscr{P}^{-1} \cong (-1,1)^*\mathscr{P} \cong (1,-1)^*\mathscr{P}$; see Exercise (7.4). In particular the cohomology of $\mathscr{P}^{-1}$ is the same as that of $\mathscr{P}$. As $X \times X^t$ is an abelian variety its dualizing sheaf is trivial, and Serre duality (in the form given by HAG, III, Cor. 7.7) gives

$$H^n(X \times X^t, \mathscr{P}) \cong H^{2g-n}(X \times X^t, \mathscr{P}^{-1})^\vee \cong H^{2g-n}(X \times X^t, \mathscr{P})^\vee\,.$$

Hence $H^n(X \times X^t, \mathscr{P}) = 0$ for all $n < g$ too. By (1) and the fact that the $R^n p_{2,*}\mathscr{P}$ are supported at 0 we also have $R^n p_{2,*}\mathscr{P} = 0$ for $n \neq g$.

CPBStep2 **(9.3)** Let $A := O_{X^t,0}$ be the local ring of X^t at 0. Let $\mathfrak{m} \subset A$ be the maximal ideal. It follows from (1) that $(R^g p_{2,*}\mathscr{P})_0$ is an A-module of finite length. By (??) the natural map

$$(R^g p_{2,*}\mathscr{P}) \otimes_{O_{X^t}} \kappa(0) \longrightarrow H^g\big(X \times \{0\}, \mathscr{P}_{|X\times\{0\}}\big) = H^g(X, O_X) \cong k$$

is an isomorphism. Using the Nakayama lemma, we find that $(R^g p_{2,*}\mathscr{P})_0 \cong A/\mathfrak{a}$ for some $\mathfrak{m}$-primary ideal $\mathfrak{a} \subset A$.

To complete the proof of (9.1) it remains to be shown that $\mathfrak{a} = \mathfrak{m}$. This is the hardest part of the proof. We need to exploit the fact that $\mathscr{P}$ is the universal line bundle on $X \times X^t$; thus far we have not made full use of this. In particular, we know that $\mathscr{P}$ is trivial over $X \times \{0\} = X \times \mathrm{Spec}(A/\mathfrak{m})$, but not over any "thickening" $X \times \mathrm{Spec}(A/J)$ for $J \subsetneq \mathfrak{m}$. The problem is how to translate this into information about $R^g p_{2,*}\mathscr{P}$.

We shall give two proofs of the fact that $\mathfrak{a} = \mathfrak{m}$. The first proof uses Grothendieck duality and is fairly short; the second relies on essentially the same ideas but is more elementary.

CPBStep3 **(9.4)** Let Z be a scheme. Write $\mathrm{Mod}(Z)$ for the category of O_Z-modules and $D(Z)$ for its derived category. If F is a sheaf of O_Z-modules and $n \in \mathbb{Z}$, write $F[n]$ for the object of $D(Z)$ represented by the complex whose only non-zero term is the sheaf F, sitting in degree $-n$. The functor $\mathrm{Mod}(Z) \to D(Z)$ given by $F \mapsto F[0]$ realizes $\mathrm{Mod}(Z)$ as a full subcategory of $D(Z)$. If $C^\bullet$ is a complex of O_Z-modules with the property that $\mathscr{H}^i(C^\bullet) = 0$ for all $i \neq n$, for some integer n, then $C^\bullet \cong \mathscr{H}^n(C^\bullet)[-n]$ in $D(Z)$.

To simplify notation we write $Y := X \times X^t$. A corollary of Grothendieck duality, applied to the morphism $p_2\colon Y \to X^t$, is that for quasi-coherent O_{X^t}-modules G we have an isomorphism

CohomLB:GrDual1
$$\mathrm{Hom}_{O_Y}(\mathscr{P}, p_2^* G) \xrightarrow{\sim} \mathrm{Hom}_{O_{X^t}}(R^g p_{2,*}\mathscr{P}, G)\,, \tag{2}$$

which is functorial in G. Before we start exploiting this, let us indicate how this is obtained from the general machinery of Grothendieck duality.

We already know that p_2 is a smooth morphism of relative dimension g and that $\Omega^g_{Y/X^t} \cong O_Y$. Consider a bounded complex $F^\bullet$ of quasi-coherent O_Y-modules and a bounded complex $G^\bullet$ of quasi-coherent O_{X^t}-modules. Then a consequence of Grothendieck duality is that we have a canonical isomorphism

CohomLB:GrDual2
$$\mathrm{Hom}_{D(Y)}\big(F^\bullet, p_2^* G^\bullet[g]\big) \xrightarrow{\sim} \mathrm{Hom}_{D(X^t)}(Rp_{2,*}F^\bullet, G^\bullet)\,. \tag{3}$$

See Hartshorne [1], Chap. III, § 11, and use that the functor $p_2^!$ is given by $G^\bullet \mapsto p_2^* G^\bullet[g]$; see op. cit., Chap. III, § 2. We apply this with $F^\bullet = \mathscr{P}$. We already know that $Rp_{2,*}F^\bullet$ only has cohomology in degree g. As explained above, this implies that $Rp_{2,*}F^\bullet$ is isomorphic, in $D(X^t)$, to $R^g p_{2,*}\mathscr{P}[-g]$. If we now apply (3) with $G^\bullet = G[-g]$ for some quasi-coherent O_{X^t}-module G then we obtain (2).

CPBStep4 **(9.5)** Let $J \subset A$ be a proper ideal (with $A = O_{X^t,0}$, as above). Write $Z(J) := \mathrm{Spec}(A/J)$, and let $i(J)\colon Z(J) \hookrightarrow X^t$ be the natural closed immersion. Write $Y(J) := X \times \mathrm{Spec}(A/J) = p_2^{-1}\big(Z(J)\big) \subset Y$. In particular, $Y(\mathfrak{m}) = X \times \{0\}$. If we write $\mathscr{P}(J)$ for the restriction of $\mathscr{P}$ to $Y(J)$ then $\mathrm{Hom}_{O_Y}(\mathscr{P}, O_{Y(J)}) = \mathrm{Hom}_{O_{Y(J)}}\big(\mathscr{P}(J), O_{Y(J)}\big)$.

Suppose J is an $\mathfrak{m}$-primary ideal. Via the natural map $O_{X^t} \to i(J)_* O_{Z(J)}$, the structure sheaf $O_{Z(J)}$ is then just the skyscraper sheaf $i_0(A/J)$ at $0 \in X^t$ with stalk A/J. Further $Y(J)$ is the closed subscheme of $Y = X \times X^t$ with underlying topological space $|X \times \{0\}|$ and structure sheaf $p_2^* O_{Z(J)} = O_X \otimes_k A/J$.

As explained in (9.3), we have $R^g p_{2,*}\mathscr{P} = i_0(A/\mathfrak{a})$ for some $\mathfrak{m}$-primary ideal $\mathfrak{a} \subset A$. Now consider the commutative diagram

$$\begin{array}{ccccc} \mathrm{Hom}_{O_Y}(\mathscr{P}, O_{Y(\mathfrak{a})}) & \xrightarrow{\sim} & \mathrm{Hom}_{O_{X^t}}\big(i_0(A/\mathfrak{a}), i_0(A/\mathfrak{a})\big) & \cong & A/\mathfrak{a} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Hom}_{O_Y}(\mathscr{P}, O_{Y(\mathfrak{m})}) & \xrightarrow{\sim} & \mathrm{Hom}_{O_{X^t}}\big(i_0(A/\mathfrak{a}), i_0(k)\big) & \cong & k \quad , \end{array}$$

where the horizontal arrows are given by (2) and the vertical arrows are induced by the quotient map $A/\mathfrak{a} \to A/\mathfrak{m} = k$.

We have a natural isomorphism $h\colon \mathscr{P}(\mathfrak{m}) = \mathscr{P}_{|X\times\{0\}} \xrightarrow{\sim} O_X$. This gives us an element

$$h \in \mathrm{Hom}_{O_Y}\big(\mathscr{P}, O_{Y(\mathfrak{m})}\big) = \mathrm{Hom}_{O_{X\times\{0\}}}\big(\mathscr{P}_{|X\times\{0\}}, O_{X\times\{0\}}\big)\,.$$

From the diagram we see that h can be lifted to an element

$$\tilde{h} \in \mathrm{Hom}_{O_Y}(\mathscr{P}, O_{Y(\mathfrak{a})}) = \mathrm{Hom}_{O_{Y(\mathfrak{a})}}\big(\mathscr{P}(\mathfrak{a}), O_{Y(\mathfrak{a})}\big)\,.$$

Then $\tilde{h}\colon \mathscr{P}(\mathfrak{a}) \to O_{Y(\mathfrak{a})}$ is a homomorphism of line bundles on $Y(\mathfrak{a})$ which is an isomorphism modulo $\mathfrak{m}$. It follows that $\tilde{h}$ is an isomorphism, too. This shows that the pull-back of $\mathscr{P}$ under $\mathrm{id}_X \times i(\mathfrak{a})\colon X \times \mathrm{Spec}(A/\mathfrak{a}) \hookrightarrow X \times X^t$ is trivial. By the universal property of $\mathscr{P}$ this implies that $i(\mathfrak{a})\colon \mathrm{Spec}(A/\mathfrak{a}) \hookrightarrow X^t$ factors through the closed point $\{0\} = \mathrm{Spec}(k) \subset X^t$. Hence $\mathfrak{a} = \mathfrak{m}$ and $R^g p_{2,*}\mathscr{P} = i_0(k)$. This finishes our (first) proof of Theorem (9.1). □

CPBStep5 **(9.6)** Our second proof that $(R^g p_{2,*}\mathscr{P})_0 \cong k$ is not very different from the first, but it replaces Grothendieck duality by more explicit arguments.

We use the notation introduced in (9.5). In particular, if $J \subset A$ is a proper ideal, the second projection $p_2\colon X \times X^t \to X^t$ restricts to a morphism $p_2\colon Y(J) \to Z(J)$. We shall systematically confuse $R^g p_{2,*}\mathscr{P}(J)$ with its A/J-module of global sections. Note that $Z\big((0)\big) = \mathrm{Spec}(A) \to X^t$ is a flat morphism; hence $R^g p_{2,*}\mathscr{P}\big((0)\big)$ is the same as the restriction of $R^g p_{2,*}\mathscr{P}$ to $Z\big((0)\big)$. (See HAG, Chap. III, Prop. 9.3.) Thus, our goal is to prove that $R^g p_{2,*}\mathscr{P}\big((0)\big) \cong k$.

We apply the results about cohomology and base-change explained in (??). This gives us a length g complex (with $g = \dim(X) = \dim(A)$) of finitely generated free A-modules

CohomLB:Kdot $$K^\bullet: \qquad 0 \longrightarrow K^0 \xrightarrow{d^0} K^1 \xrightarrow{d^1} \cdots \longrightarrow K^{g-1} \xrightarrow{d^{g-1}} K^g \longrightarrow 0 \tag{4}$$

with the property that for all ideals $J \subset A$ and all n we have

$$R^n p_{2,*}\mathscr{P}(J) \cong \mathscr{H}^n(K^\bullet \otimes_A A/J)\,,$$

functorially in A/J. (In fact, a similar statement holds with A/J replaced by an arbitrary A-algebra, but we will not need this.) In particular $\mathscr{H}^n(K^\bullet) \cong R^n p_{2,*}\mathscr{P}$. But as shown in (9.2), $R^n p_{2,*}\mathscr{P} = 0$ for $n < g$; so $K^\bullet$ is a resolution of $\mathscr{H}^g := \mathscr{H}^g(K^\bullet)$. We want to show that $\mathscr{H}^g \cong A/\mathfrak{m} = k$.

Consider the "dual" complex

$$L^\bullet: \qquad 0 \longrightarrow L^0 \xrightarrow{\delta^0} L^1 \xrightarrow{\delta^1} \cdots \longrightarrow L^{g-1} \xrightarrow{\delta^{g-1}} L^g \longrightarrow 0$$

where $L^j := \mathrm{Hom}_A(K^{g-j}, A)$, and where δ^j is the map induced by d^{g-1-j}. Set

$$Q := \mathscr{H}^g(L^\bullet) = \mathrm{Coker}(\delta^{g-1}\colon L^{g-1} \to L^g)\,.$$

The next lemma (taken from MAV, p. 127) tells us that $L^\bullet$ is a free resolution of Q. (Note that all $\mathscr{H}^n(L^\bullet)$ are artinian A-modules, as easily follows from the corresponding fact for the complex $K^\bullet$.)

CohomLem **(9.7) Lemma.** *Let A be a g-dimensional regular local ring. Let*

$$C^\bullet : \qquad 0 \longrightarrow C^0 \longrightarrow C^1 \longrightarrow \cdots \longrightarrow C^g \longrightarrow 0$$

be a complex of finitely generated free A-modules such that all cohomology groups $\mathscr{H}^j(C^\bullet)$ are artinian A-modules. Then $\mathscr{H}^j(C^\bullet) = 0$ for all $j < g$.

Proof. We use induction on g. For $g = 0$ there is nothing to prove, so we may assume that $g > 0$ and that the lemma holds in smaller dimensions. Choose $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, so that $A/(x)$ is regular of dimension $g-1$. Put $\overline{C}^\bullet := C^\bullet/(x)$, so that we have an exact sequence of complexes

$$0 \longrightarrow C^\bullet \xrightarrow{\cdot x} C^\bullet \longrightarrow \overline{C}^\bullet \longrightarrow 0\,.$$

In cohomology this gives the long exact sequence

$$\cdots \longrightarrow \mathscr{H}^i(C^\bullet) \xrightarrow{\cdot x} \mathscr{H}^i(C^\bullet) \longrightarrow \mathscr{H}^i(\overline{C}^\bullet) \longrightarrow \mathscr{H}^{i+1}(C^\bullet) \xrightarrow{\cdot x} \mathscr{H}^{i+1}(C^\bullet) \longrightarrow \cdots \quad .$$

We see from this that the $\mathscr{H}^i(\overline{C}^\bullet)$ are artinian modules, and by induction $\mathscr{H}^i(\overline{C}^\bullet) = 0$ for all $i < g-1$. Hence multiplication by x is injective on $\mathscr{H}^j(C^\bullet)$ for all $j < g$. But $\mathscr{H}^j(C^\bullet)$ is artinian, so it is killed by x^N for $N \gg 0$. This proves the induction step. □

CPBStep6 **(9.8)** From (7.27) we know the cohomology of the complex $K^\bullet \otimes_A k = [0 \to K^0/\mathfrak{m}K^0 \to K^1/\mathfrak{m}K^1 \to \cdots]$. In particular we have $\mathscr{H}^0(K^\bullet \otimes_A k) = H^0(X, O_X) = k$ and $\mathscr{H}^g(K^\bullet \otimes_A k) = H^g(X, O_X) = k$. This gives us that $\mathscr{H}^g/\mathfrak{m}\mathscr{H}^g \cong k$ and $Q/\mathfrak{m}Q \cong k$. By Nakayama's Lemma it follows that the A-modules $\mathscr{H}^g$ and Q are both generated by a single element, so there exist ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A with

$$\mathscr{H}^g \cong A/\mathfrak{a} \qquad \text{and} \qquad Q \cong A/\mathfrak{b}\,.$$

(For $\mathscr{H}^g$ this repeats what was explained in (9.3).)

Let $J \subset A$ be an ideal. Put

$$H^0_J := \mathrm{Ker}(K^0/JK^0 \to K^1/JK^1) = H^0\big(Y(J), \mathscr{P}(J)\big)\,.$$

Applying $\mathrm{Hom}_A(-, A/J)$ to the exact sequence $L^{g-1}/JL^{g-1} \to L^g/JL^g \to Q/JQ \to 0$ gives the exact sequence

$$0 \longrightarrow \mathrm{Hom}_A(Q/JQ, A/J) \longrightarrow K^0/JK^0 \xrightarrow{\bar{d}^0} K^1/JK^1\,,$$

which shows that

CohomPB:H0J $$H^0_J \cong \mathrm{Hom}_A(A/\mathfrak{b} + J, A/J)\,. \tag{5}$$

The isomorphism (5) is functorial in the ideal J, in the sense that for $J_1 \subseteq J_2$ the natural reduction map $H^0_{J_1} \to H^0_{J_2}$ corresponds to the natural map

$$\mathrm{Hom}_A(A/\mathfrak{b}+J_1, A/J_1) \to \mathrm{Hom}_A(A/\mathfrak{b}+J_1, A/J_2) = \mathrm{Hom}_A(A/\mathfrak{b}+J_2, A/J_2)\,.$$

We now use that, by definition of X^t, the closed point $0 \in X^t$ is the maximal closed subscheme over which $\mathscr{P}$ is trivial, in the sense of (2.4). Taking $J_1 = \mathfrak{b}$ and $J_2 = \mathfrak{m}$ in the above we find that the section $1 \in k = H^0(X, O_X) = H^0\big(Y(\mathfrak{m}), \mathscr{P}(\mathfrak{m})\big)$ lifts to a global section of $\mathscr{P}(\mathfrak{b})$. With the same arguments as in (9.5) it follows that $\mathscr{P}(\mathfrak{b}) \cong O_{Y(\mathfrak{b})}$, and by the universal property of $\mathscr{P}$ this is possible only if $\mathfrak{b} = \mathfrak{m}$.

CPBStep7 **(9.9)** We have shown that $L^\bullet$ is a free resolution of the A-module $A/\mathfrak{m} = k$. Another way to obtain such a resolution is to use a Koszul complex. This works as follows. Choose a regular system of parameters $x_1, x_2, \ldots, x_g \in \mathfrak{m}$, i.e., a sequence of elements which generate $\mathfrak{m}$ and which give a k-basis for $\mathfrak{m}/\mathfrak{m}^2$. Consider the complex

$$F^\bullet: \qquad 0 \longrightarrow F^0 \longrightarrow F^1 \longrightarrow \cdots \longrightarrow F^g \longrightarrow 0$$

where $F^j = \wedge^j_A(A^g)$ and where, writing $\underline{x} = (x_1, \ldots, x_g) \in A^g$, the differential

$$d^j\colon \wedge^j_A(A^g) \longrightarrow \wedge^{j+1}_A(A^g)$$

is given by $v \mapsto \underline{x} \wedge v$. Then $F^\bullet$, the so-called *Koszul complex* associated to the sequence $\underline{x}$, is also a free resolution of k.

By (??) the complexes $L^\bullet$ and $F^\bullet$ are homotopy equivalent. "Dualizing back" we then find that the complex $K^\bullet$ is homotopy equivalent to the dual of the Koszul complex $F^\bullet$. The first terms of $F^\bullet$ are given by

$$0 \longrightarrow A \xrightarrow{d^0} A^g \longrightarrow \cdots \qquad \text{with } d^0\colon a \mapsto (x_1a, x_2a, \ldots, x_ga)\,.$$

The last non-zero terms of the dual complex are therefore given by

$$\cdots \longrightarrow A^g \xrightarrow{(d^0)^*} A \longrightarrow 0 \qquad \text{with } (d^0)^*\colon (a_1, a_2, \ldots, a_g) \mapsto x_1a_1 + x_2a_2 + \cdots + x_ga_g\,.$$

With this we can finally compute:

$$(R^g p_{2,*}\mathscr{P})_0 \cong \mathscr{H}^g(K^\bullet) \cong \mathscr{H}^g\big((F^\bullet)^*\big) = \mathrm{Coker}\big((d^0)^*\big) = A/\mathfrak{m} = k$$

and this finishes the (second) proof of Theorem (9.1). □

EuChProps **(9.10)** The following result we want to prove is the Riemann-Roch theorem for abelian varieties.

Let X be a proper scheme of finite type over a field k. If F is a quasi-coherent O_X-module then its *Euler characteristic* is defined to be the integer

$$\chi(L) := \sum_{i \geqslant 0} (-1)^i \cdot \dim_k H^i(X, F)\,.$$

Suppose X is projective and H is a very ample line bundle on X. Then $n \mapsto \chi(F \otimes H^n)$ is a polynomial function of n. More precisely, there is a polynomial with rational coefficients

$\Phi = \Phi_{F,H} \in \mathbb{Q}[t]$, called the *Hilbert polynomial of* F (with respect to H), such that $\Phi(n) = \chi(F \otimes H^n)$ for all $n \in \mathbb{Z}$. Note that there is a natural number n_0 such that $H^i(X, F \otimes H^n) = 0$ for all $i > 0$ and all $n \geqslant n_0$; hence $\Phi(n) = \dim_k H^0(X, F \otimes H^n)$ for all $n \geqslant n_0$.

This "polynomial behaviour" of the Euler characteristic with respect to its entries is a much more general phenomenon. For instance, suppose X is a smooth proper variety over k and $F_1, \dots, F_r$ are vector bundles on X (or, more generally, coherent O_X-modules). Then the function $(n_1, \dots, n_r) \mapsto \chi(F_1^{n_1} \otimes \cdots \otimes F_r^{n_r})$ is polynomial in the r-tuple of integers $(n_1, \dots, n_r)$. This is a consequence of the Hirzebruch-Riemann-Roch theorem. When X is an abelian variety the Riemann-Roch formula takes a particularly simple form and the polynomial dependence of $\chi(F_1^{n_1} \otimes \cdots \otimes F_r^{n_r})$ on the exponents n_i becomes obvious; cf. (9.13).

RRAbVar **(9.11) Riemann-Roch Theorem.** *Let L be a line bundle on a g-dimensional abelian variety X. Then*

$$\chi(L) = c_1(L)^g/g! \quad \textit{and} \quad \chi(L)^2 = \deg(\varphi_L)\,.$$

Thus, if $L \cong O_X(D)$ for some divisor D then the first equation says that $\chi(L)$ equals $(D^g)/g!$, where (D^g) is g-fold self-intersection number of D. Notice that, by slight abuse of notation, we write $c_1(L)^g$ for $\deg\big(c_1(L)^g\big) = \int_X c_1(L)^g$.

We shall prove the theorem together with the following corollary.

isogchi **(9.12) Corollary.** *Let $f\colon Y \to X$ be an isogeny. If L is a line bundle on X then $\chi(f^*L) = \deg(f) \cdot \chi(L)$.*

Proof of (9.11) *and* (9.12). First we show that $\chi(L) = c_1(L)^g/g!$. For this we use the Hirzebruch-Riemann-Roch formula, which says that

CohomLB;HRR
$$\chi(L) = \int_X \mathrm{ch}(L) \cdot \mathrm{td}(T_X)\,. \tag{6}$$

Here $\mathrm{ch}(L)$, the Chern character of L, is the power series

$$\mathrm{ch}(L) = \exp\big(c_1(L)\big) = 1 + c_1(L) + c_1(L)^2/2 + \cdots$$

which should be thought of as a formal expression. Similiarly, $\mathrm{td}(T_X)$, the Todd class of the tangent bundle T_X, is a formal power series in the Chern classes of T_X. As T_X is trivial we have $c_i(T_X) = 0$ for all $i \geqslant 1$ and $\mathrm{td}(T_X) = 1$. This reduces (6) to the desired equality $\chi(L) = \int_X c_1(L)^g/g!$. Notice that, in particular,

CohomLB;chiLm
$$\chi(L^m) = m^g \cdot \chi(L) \tag{7}$$

for all $m \in \mathbb{Z}$.

To prove (9.12) we may assume that $k = \overline{k}$. Let $f\colon Y \to X$ be an isogeny of degree d. Then $c_1(f^*L)^g = f^*\big(c_1(L)^g\big)$ in the Chow ring of Y. (Alternatively we may use any Weil cohomology, such as ℓ-adic cohomology for some $\ell \neq \mathrm{char}(k)$, or Betti cohomology in case the ground field is $\mathbb{C}$.) But $c_1(L)^g$ is represented by a 0-cycle (a formal sum of points), so all that remains to be shown is that $\int_Y f^*[P] = d$ for every point $P \in X$. This is clear if f is separable, for then $f^{-1}(P)$ consists of d distinct points, each with multiplicity 1. It is also clear if f is purely inseparable, because then $f^{-1}(P)$ consists of one single point, say Q, and $O_{Y,Q}$ is free of rank d over $O_{X,P}$. The general result follows by combining these two cases, using (5.8). This proves Cor. (9.12).

Next we show that $\chi(L)^2 = \deg(\varphi_L)$. We first do this for non-degenerate line bundles L. The idea is to compute $\chi\big(\Lambda(L)\big)$ in two different ways.

So, assume that L is non-degenerate. As usual we write $\Lambda(L)$ for the associated Mumford bundle on $X \times X$. We have a cartesian diagram

$$\begin{array}{ccc} X \times X & \xrightarrow{\mathrm{id}_X \times \varphi_L} & X \times X^t \\ {\scriptstyle p_2}\big\downarrow & & \big\downarrow{\scriptstyle p_2'} \\ X & \xrightarrow[\varphi_L]{} & X^t \end{array} .$$

Further we know that $\Lambda(L) = (\mathrm{id}_X \times \varphi_L)^* \mathscr{P}$, and φ_L is an isogeny with kernel $\{1\} \times K(L)$. By (9.1) and flat base change,

$$R^n p_{2,*}\Lambda(L) = \varphi_L^*\big(R^n p'_{2,*}\mathscr{P}\big) = \begin{cases} 0 & \text{if } n \neq g; \\ i_* O_{K(L)} & \text{if } n = g, \end{cases}$$

where $i\colon K(L) \hookrightarrow X$ is the inclusion. Using a Leray spectral sequence, as in (9.2), we find

CohomLB;hnLam
$$h^n\big(X \times X, \Lambda(L)\big) = \begin{cases} 0 & \text{if } n \neq g; \\ \deg(\varphi_L) & \text{if } n = g. \end{cases} \tag{8}$$

Here, as usual, we write $h^n(-) := \dim H^n(-)$. In particular,

CohomLB;chiLam
$$\chi\big(\Lambda(L)\big) = (-1)^g \cdot \deg(\varphi_L)\,. \tag{9}$$

(A quicker proof of (9) is to use (9.12), but we shall need (8) later.)

For the second computation of $\chi\big(\Lambda(L)\big)$, recall that $\Lambda(L) := m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1}$. The projection formula therefore gives

$$R^n p_{2,*}\Lambda(L) = R^n p_{2,*}\big(m^*L \otimes p_1^*L^{-1}\big) \otimes L^{-1}\,.$$

We know that $R^n p_{2,*}\Lambda(L)$ is supported on the finite subscheme $K(L) \subset X$. As L can be trivialized over $K(L)$ we find that

$$R^n p_{2,*}\big(m^*L \otimes p_1^*L^{-1}\big) \otimes L^{-1} = R^n p_{2,*}\big(m^*L \otimes p_1^*L^{-1}\big)\,.$$

Once again computing cohomology via a Leray spectral sequence we conclude that

CohomLB;HnLamb
$$H^n\big(X \times X, \Lambda(L)\big) \cong H^n(X \times X, m^*L \otimes p_1^*L^{-1}) \qquad \text{for all } n. \tag{10}$$

Now remark that $(m \times p_1)\colon X \times X \to X \times X$ is an isomorphism with $(m \times p_1)^*\big(p_1^*L \otimes p_2^*L^{-1}\big) = m^*L \otimes p_1^*L^{-1}$. By the Künneth formula it follows that

CohomLB;Kunn
$$H^n(X \times X, m^*L \otimes p_1^*L^{-1}) \cong H^n(X \times X, p_1^*L \otimes p_2^*L^{-1}) \cong \bigoplus_{p+q=n} H^p(X, L) \otimes H^q(X, L^{-1})\,. \tag{11}$$

Combining (10) and (11) we find

CohomLB;chichi
$$\chi\big(\Lambda(L)\big) = \chi\big(p_1^*L \otimes p_2^*L^{-1}\big) = \chi(L) \cdot \chi(L^{-1}) = (-1)^g \cdot \chi(L)^2\,, \tag{12}$$

where the last equality follows from (7). Comparing the two answers (9) and (12) proves that $\chi(L)^2 = \deg(\varphi_L)$ for non-degenerate L.

Now suppose that L is degenerate. Then φ_L is not finite and, by convention, $\deg(\varphi_L) = 0$. We want to show that $\chi(L) = 0$ too. It is still true that $\Lambda(L) = (\mathrm{id}_X \times \varphi_L)^* \mathscr{P}$. We rewrite this as

$$m^*L \otimes p_2^*L^{-1} = (\mathrm{id}_X \times \varphi_L)^* \big(\mathscr{P} \otimes p_1^*L\big)\,.$$

The same argument as above gives that $\chi\big(m^*L \otimes p_2^*L^{-1}\big) = (-1)^g \cdot \chi(L)^2$. (Notice that this part of the above argument works without the assumption that L is non-degenerate.) If $H \subset K(L)$ is a subgroup scheme of order r then $\mathrm{id}_X \times \varphi_L$ factors through the projection $X \times X \to X \times X/H$, and by (9.12) it follows that $\chi\big(m^*L \otimes p_2^*L^{-1}\big)$ is divisible by r. But $K(L)$ contains subgroup schemes of arbitrarily large order (in fact, $K(L)^0_{\mathrm{red}}$ is an abelian subvariety of X of positive dimension), and we conclude that $\chi(L) = 0$. This finishes the proof of the theorem. □

RRAVRem **(9.13) Remark.** If F is a coherent sheaf on a g-dimensional abelian variety X then Hirzebruch-Riemann-Roch gives $\chi(F) = \int_X \mathrm{ch}_g(F)$ where ch_g is a certain polynomial in the Chern classes of F. See Fulton [1], Example 3.2.3.

Looking at the proof of (9.11) we see that for non-degenerate bundles we can draw one further conclusion.

VanishThm **(9.14) Vanishing Theorem.** *If L is a non-degenerate line bundle then there is a unique integer i (necessarily with $0 \leqslant i \leqslant g$) such that $H^i(X, L) \neq 0$.*

Proof. Combining (8), (10) and (11) we have shown that

$$\sum_{p+q=n} h^p(L) \cdot h^q(L^{-1}) = \begin{cases} 0 & \text{if } n \neq g; \\ \deg(\varphi_L) & \text{if } n = g. \end{cases}$$

As all $h^i(L)$ and $h^j(L^{-1})$ are in $\mathbb{Z}_{\geqslant 0}$ this is possible only if there are *unique* p and q (with $p + q = g$) such that $h^p(L) \neq 0$ and $h^q(L^{-1}) \neq 0$. □

IndexDef **(9.15) Definition.** If L is a non-degenerate line bundle then the unique index $i = i(L)$ such that $h^i(L) \neq 0$ is called the *index* of L.

Note that $i(L) = 0$ just means that L is effective.

DivECInd **(9.16) Example.** Let D be a divisor of degree d on an elliptic curve E. Riemann-Roch for curves gives $\chi\big(O_E(D)\big) = d$. It follows that

$$\begin{aligned} D \text{ is degenerate} &\iff d = 0 \\ D \text{ is non-degenerate of index } 0 &\iff d > 0 \\ D \text{ is non-degenerate of index } 1 &\iff d < 0 \end{aligned}$$

ThRepCor **(9.17) Corollary.** *Let X be an abelian variety over an algebraically closed field k. Let L be a non-degenerate line bundle on X with index $i = i(L)$. Then $H^i(X, L)$ is the unique irreducible weight 1 representation of the theta group $\mathscr{G}(L)$.*

Proof. That $H^i(X, L)$ is a $\mathscr{G}(L)$-representation of weight 1 is clear, for instance, using Čech cohomology. The corollary thus follows from (8.32) by a dimension count. Indeed, we have

$$\big(\dim H^i(X, L)\big)^2 = \chi(L)^2 = \deg(\varphi_L) = \operatorname{rank}\big(K(L)\big)\,,$$

as required. □

If L is a non-degenerate line bundle with index i then $\chi(L) = (-1)^i \cdot h^i(L)$. In particular, $\chi(L)$ has sign equal to $(-1)^{i(L)}$. We shall later see how the index can be read off from the Hilbert polynomial of L. As a preparation for this we collect some properties of the index as a function on the set of non-degenerate bundles.

IndexProp **(9.18) Proposition.** (i) *Let L be a non-degenerate line bundle on a g-dimensional abelian variety X. Then $i(L^{-1}) = g - i(L)$.*

(ii) *"The index is (locally) constant in algebraic families": If T is a locally noetherian k-scheme and M is a line bundle on $X \times T$ such that all $M_t := M_{|X\times\{t\}}$ are non-degenerate then the function $t \mapsto i(M_t)$ is locally constant on T. In particular, if L is as in* (i) *and L' is a line bundle on X with $[L'] \in \operatorname{Pic}^0_{X/k}$ then $i(L) = i(L \otimes L')$.*

(iii) *Let $f\colon X \to Y$ be an isogeny of degree prime to $\operatorname{char}(k)$. If M is a non-degenerate line bundle on Y then f^*M is non-degenerate too and $i(f^*M) = i(M)$.*

(iv) *If L is non-degenerate and $m \neq 0$ then L^m is non-degenerate too. Furthermore, if $m > 0$ and $\operatorname{char}(k) \nmid m$ then $i(L^m) = i(L)$.*

(v) *If L_1, L_2 and $L_1 \otimes L_2$ are all non-degenerate then $i(L_1 \otimes L_2) \leqslant i(L_1) + i(L_2)$.*

(vi) *If H is ample and L and $L \otimes H$ are both non-degenerate then $i(L \otimes H) \leqslant i(L)$.*

Notes: In (9.23) below we shall sharpen (iv), showing that $i(L^m) = i(L)$ for all $m > 0$. In (9.26) we shall show that (iii) holds without the assumption that $\deg(f)$ is prime to $\operatorname{char}(k)$. If in (ii) the scheme T is geometrically connected then it suffices to require that M_t is non-degenerate for *some* $t \in T$ (as $K(M_t)$ does not jump in such families), and the conclusion is that $t \mapsto i(M_t)$ is constant on T. The requirement that T is locally noetherian is in fact superfluous, as we can reduce to the "universal" case $T = \operatorname{Pic}_{X/k}$.

Proof. Statement (i) was already found in the proof of (9.14). Alternatively, it follows from Serre duality.

The first statement of (ii) follows from the fact (HAG, III, Thm. 12.8) that for all j the function $t \mapsto \dim_{k(t)} H^j(X \otimes k(t), M_t)$ is upper semi-continuous. The second statement follows by applying this to the Poincaré bundle over $X \times \operatorname{Pic}_{X/k}$. Alternatively, passing to an algebraic closure of k the bundles $L \otimes L'$ with $[L'] \in \operatorname{Pic}^0_{X/k}$ are precisely the line bundles of the form t_x^*L. In cohomology the translation t_x induces an isomorphism between $H^j(X, L)$ and $H^j(X, t_x^*L)$.

(iii) As shown in (7.6), f^*M is again non-degenerate. We have $f_*(f^*M) = M \otimes_{O_Y} f_*O_X$. We claim that the sheaf O_Y is a direct summand of f_*O_X, hence M is a direct summand of f_*f^*M. Indeed, if $r = \deg(f)$ then f_*O_X is locally free of rank r over O_Y and by assumption r is invertible in O_Y. If trace: $f_*O_X \to O_Y$ is the trace map then $(1/r) \cdot \text{trace}$ is a section of the natural map $O_Y \to f_*O_X$, so $f_*O_X = O_Y \oplus \operatorname{Ker}(\text{trace})$.

Since f is finite, a Leray spectral sequence shows that $H^i(X, f^*M) \cong H^i(Y, f_*f^*M)$ for all i (see also HAG, III, Exercise 4.1), and we conclude that $H^i(Y, M)$ is isomorphic to a direct summand of $H^i(X, f^*M)$. This proves (iii).

(iv) We have $K(L^m) = m^{-1}\big(K(L)\big)$. Hence L^m is non-degenerate for $m \neq 0$. Now assume that $m > 0$ is relatively prime with $\operatorname{char}(k)$. We use the notation and the results of Exercise (7.8).

Consider the line bundle $L^{\boxtimes 4}$ on X^4 given by $L^{\boxtimes 4} = L^{\boxtimes \mathrm{id}_4} = \otimes_{i=1}^4 p_i^* L$. (Here id_4 denotes the identity matrix of size 4×4.) It is readily seen that $L^{\boxtimes 4}$ is again non-degenerate (in fact, $K\big(L^{\boxtimes 4}\big) = K(L)^4$), and by the Künneth formula we have $i\big(L^{\boxtimes 4}\big) = 4 \cdot i(L)$.

We write $m > 0$ as a sum of four squares, say $m = a^2 + b^2 + c^2 + d^2$. Consider the matrix

$$A = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

which should be thought of as representing the quaternion $a+bi+cj+dk$. We have $A^t \cdot A = m \cdot \mathrm{id}_4$. Now consider the homomorphism $\alpha = \alpha_A \colon X^4 \to X^4$ associated to A, and apply part (i) of Exercise (7.8). This gives that $\alpha^*\big(L^{\boxtimes 4}\big)$ and $(L^m)^{\boxtimes 4}$ differ by something in $\mathrm{Pic}^0_{X/k}$; hence by (ii) they have the same index. But by (iii) the index of $\alpha^*\big(L^{\boxtimes 4}\big)$ equals that of $L^{\boxtimes 4}$. Putting everything together we find that

$$i(L) = 1/4 \cdot i\big(L^{\boxtimes 4}\big) = 1/4 \cdot i\big((L^m)^{\boxtimes 4}\big) = i(L^m)\,,$$

as claimed.

(v) Let i_1, i_2 and ι be the indices of L_1, L_2 and $L_1 \otimes L_2$, respectively. Consider the line bundle $N := p_1^* L_1 \otimes p_2^* L_2$ on $X \times X$, and let $\nu \colon X \times X \to X$ be given by $\nu(x, y) = x - y$. The fibre of ν over 0 is the diagonal $X \cong \Delta(X) \subset X \times X$, over which N restricts to the bundle $L_1 \otimes L_2$. By (ii) it follows that all fibres of N have index ι, so that $R^j \nu_* N = 0$ for all $j < \iota$. By a Leray spectral sequence this implies that $H^j(X \times X, N) = 0$ for all $j < \iota$. But the Vanishing Theorem together with the Künneth decomposition show that $H^{i_1}(X, L_1) \otimes_k H^{i_2}(X, L_2) \cong H^{i_1 + i_2}(X \times X, N)$.

Finally, (vi) follows from (v), as it follows from (iv) that ample bundles have index 0. □

FrobSplitRem **(9.19) Remark.** The fact used in the proof of (iii) that O_Y is a direct summand of $f_* O_X$ is not necessarily true if the degree of f is divisible by $\mathrm{char}(k)$. For instance, suppose X is an abelian variety over a field k of characteristic $p > 0$, such that X is not ordinary, i.e., $f(X) < g$. Then the relative Frobenius map $F_{X/k} \colon X \to X^{(p)}$ is an isogeny of abelian varieties, but it can be shown that $O_{X^{(p)}}$ is in this case not a direct summand of $F_{X/k,*} O_X$. In the literature one finds this as the statement that a non-ordinary abelian variety is not Frobenius split; see Mehta-Srinivas [??].

For the proof of the following proposition we need a somewhat technical, but important lemma.

hiEstLem **(9.20) Lemma.** *Let Y be a d-dimensional projective scheme over a field. Let $L_1, \cdots, L_r$ be line bundles on Y. For $\underline{a} = (a_1, \ldots, a_r) \in \mathbb{Z}^r$, set $|\underline{a}| := |a_1| + \cdots + |a_r|$ and $L^{\underline{a}} := L_1^{a_1} \otimes \cdots \otimes L_r^{a_r}$. Then there is a constant $C > 0$, only depending on Y and the bundles L_j, such that*

$$h^i(Y, L^{\underline{a}}) \leqslant C \cdot (1 + |\underline{a}|^r)$$

for all i and all $\underline{a} \in \mathbb{Z}^r$.

Proof. If all L_i are trivial then the assertion is clear; this covers the cases $d = 0$ and $r = 0$. Next we reduce to the case when all L_j are very ample. For this, choose a very ample bundle M such that each of the

$$M_j := L_j \otimes M \qquad (1 \leqslant j \leqslant r)$$

is very ample, too. Suppose we know the lemma for the line bundles $M_1, \dots, M_r$, M_{r+1}. If C is the resulting constant then for all $\underline{a} \in \mathbb{Z}^r$, putting $\sigma(\underline{a}) := a_1 + \cdots + a_r$,

$$\begin{aligned} h^i(Y, L^{\underline{a}}) = h^i(Y, M_1^{a_1} \otimes \cdots \otimes M_r^{a_r} \otimes M_{r+1}^{-\sigma(\underline{a})}) &\leqslant C \cdot \big(1 + \{|\underline{a}| + |\sigma(\underline{a})|\}^r\big) \\ &\leqslant C \cdot \big(1 + \{2|\underline{a}|\}^r\big) \leqslant (3^{r+1}C) \cdot (1 + |\underline{a}|^r)\,. \end{aligned}$$

From now on we may therefore assume all L_j to be very ample.

We proceed by induction on the integer $d + r$. The case $d + r = 0$ is already dealt with. Assume the lemma is true whenever $d + r \leqslant \nu$. As the lemma is true when $r = 0$, it suffices to do the case when we have $r + 1$ very ample bundles, say $L_1, \dots, L_r$ and M, on a d-dimensional projective scheme Y, such that $d + r + 1 = \nu + 1$.

Let $Z \subset Y$ be a hyperplane section for the projective embedding given by M. For every $\underline{a} \in \mathbb{Z}^r$ and $b \in \mathbb{Z}$ we have an exact sequence

$$0 \longrightarrow L^{\underline{a}} \otimes M^{b-1} \longrightarrow L^{\underline{a}} \otimes M^b \longrightarrow (L^{\underline{a}} \otimes M^b)_{|Z} \longrightarrow 0\,.$$

In cohomology this gives an exact sequence

$$H^{i-1}(Z, L^{\underline{a}} \otimes M^b) \longrightarrow H^i(Y, L^{\underline{a}} \otimes M^{b-1}) \longrightarrow H^i(Y, L^{\underline{a}} \otimes M^b) \longrightarrow H^i(Z, L^{\underline{a}} \otimes M^b)$$

which gives

CohomLB;LaMb
$$h^i(Y, L^{\underline{a}} \otimes M^b) \leqslant h^i(Y, L^{\underline{a}} \otimes M^{b-1}) + h^i(Z, L^{\underline{a}} \otimes M^b) \tag{13}$$

and

CohomLB;LaMb-1
$$h^i(Y, L^{\underline{a}} \otimes M^{b-1}) \leqslant h^i(Y, L^{\underline{a}} \otimes M^b) + h^{i-1}(Z, L^{\underline{a}} \otimes M^b)\,. \tag{14}$$

By induction hypothesis we have estimates for $h^i(Y, L^{\underline{a}} \otimes M^b)$ when $b = 0$ and for the terms $h^i(Z, L^{\underline{a}} \otimes M^b)$. For $b > 0$ we get the desired estimates by iterated application of (13); for $b < 0$ we do the same using (14). □

PLH **(9.21)** To obtain further results on the index function, we investigate in more detail what happens in the situation of (vi) in (9.18). We fix a non-degenerate bundle L and an ample bundle H. As remarked above, ample bundles have index 0; in other words: they are effective.

Set $l = c_1(L)$ and $h = c_1(H)$. Consider the homogeneous polynomial of degree g

$$P(s,t) := (sl + th)^g \quad \in \mathbb{Z}[s,t]\,,$$

whose coefficients are intersection numbers. Notice that $P(m,n) = g! \cdot \chi(L^m \otimes H^n)$ for all integral m and n. Further note that P is homogeneous of degree g, so $P(m,n) = m^g P(1, n/m) = g! m^g \Phi_{L,H}(n/m)$ where $\Phi_{L,H}$ is the Hilbert polynomial of L with respect to H. In other words: P is "the Hilbert polynomial made homogeneous of degree g". If we want to indicate which bundles L and H we are working with then we use the notation $P_{L,H}$. For later use let us remark that

CohomLB;PLmH
$$P_{L^m,H}(s,t) = P_{L,H}(ms,t) = m^g \cdot P_{L,H}(s, t/m) \tag{15}$$

for all integers $m \neq 0$.

P(1,t)Prop1 **(9.22) Proposition.** *Suppose that both L and $L \otimes H$ are non-degenerate, and that $i(L) \neq i(L \otimes H)$. Then $P(1,t)$ has a root in the interval $[0,1] \subset \mathbb{R}$.*

Proof. Let M be a square not divisible by $\mathrm{char}(k)$. By (iv) of (9.18) we have

$$i(L^M) = i(L) \neq i(L \otimes H) = i(L^M \otimes H^M)\,.$$

Assume that $P(1,t)$ does not vanish on $[0,1]$, so that there exists a constant $C > 0$ with $|P(1,t)| > C$ for all $t \in [0,1]$. As degenerate line bundles have zero Euler characteristic this implies that all line bundles $L^M \otimes H^n$ with $0 \leqslant n \leqslant M$ are non-degenerate. Let n be the smallest positive integer such that $i(L^M \otimes H^{n-1}) \neq i(L^M \otimes H^n)$. Set

$$\begin{aligned} i_1 = i(L) = i(L^M) = \cdots = i(L^M \otimes H^{n-1}) \\ i_2 = i(L^M \otimes H^n)\,, \end{aligned}$$

and observe that $i_2 < i_1$ by (vi) of (9.18).

Choose an effective divisor $D \in |H|$ and consider the short exact sequence

$$0 \longrightarrow L^M \otimes H^{n-1} \longrightarrow L^M \otimes H^n \longrightarrow (L^M \otimes H^n)_{|D} \longrightarrow 0\,.$$

Looking at the associated long exact cohomology sequence and using that $i_1 > i_2$ we find that

$$H^{i_2}(X, L^M \otimes H^n) \hookrightarrow H^{i_2}(D, L^M \otimes H^n)\,.$$

In particular, $h^{i_2}(D, L^M \otimes H^n) \geqslant M^g \cdot |P(1, n/M)|$, which by our choice of C is at least $M^g \cdot C$. Since this holds with arbitrarily large M, and since D has dimension $g-1$, we obtain a contradiction with (9.20). □

i(Lm)Cor **(9.23) Corollary.** *If L is non-degenerate then $i(L^m) = i(L)$ for all $m > 0$.*

Proof. Write $L = H_1 \otimes H_2^{-1}$ as the difference of two ample bundles. Choose $M \geqslant 2$ big enough such that both polynomials $P_{L,H_1}(1,t)$ and $P_{L,H_2}(1,t)$ have no zeroes in the interval $[0, 1/M]$, which is possible since $P_{L,H_j}(1,0) = g! \cdot \chi(L) \neq 0$. By (15) it follows that for $m \geqslant M$ both $P_{L^m,H_1}(1,t)$ and $P_{L^m,H_2}(1,t)$ have no zeroes in the interval $[0,1]$. By the proposition this implies

$$i(L^{m+1}) = i(L^{m+1} \otimes H_2) = i(H_1^{m+1} \otimes H_2^{-m}) = i(L^m \otimes H_1) = i(L^m)\,.$$

Hence for large enough m the index of L^m is independent of m. Using properties (i) and (iv) in (9.18) the corollary follows. □

P(1,t)Lem2 **(9.24) Lemma.** *Let L be non-degenerate, H ample, and let $P(s,t) := P_{L,H}(s,t)$ be the polynomial defined above. Suppose $P(1,t)$ has a unique root $\tau \in [0,1]$, of multiplicity μ and with $\tau \neq 1$. Then $i(L) \leqslant i(L \otimes H) + \mu$.*

Proof. As $P_{L^m,H^m}(s,t) = m^{2g} \cdot P_{L,H}(s,t)$ we may assume, using (9.23), that H is very ample. Also we may assume that $i(L) \neq i(L \otimes H)$, so that also $i(L^m) \neq i(L^m \otimes H^m)$ for all $m \neq 0$.

Let $m \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}$ with $n < m$. In the rest of the proof we shall only consider integers m which are coprime with all denominators of rational roots of $P(1,t)$. This ensures that $L^m \otimes H^n$ is non-degenerate; indeed, if $L^m \otimes H^n$ is degenerate then $P(1, n/m) = 0$.

With m and n as above, suppose that $i(L^m \otimes H^{n-1}) \neq i(L^m \otimes H^n)$. Note that

$$P_{L^m \otimes H^{n-1},H}(1,t) = m^g \cdot P_{L,H}(1, \frac{n-1+t}{m})\,,$$

so it follows from (9.22) that $P(1,t)$ has a root in the interval $[(n-1)/m, n/m]$. By the assumptions of the lemma we conclude that for given $m > 0$ there is a unique n with $1 < n \leqslant m$ (depending on m) such that

CohomLB;iLm
$$i(L^m) = \cdots = i(L^m \otimes H^{n-1}) \;>\; i(L^m \otimes H^n) = \cdots = i(L^m \otimes H^m)\,. \tag{16}$$

Let $X =: Z_0 \supset Z_1 \supset Z_2 \supset \cdots$ be obtained by taking hyperplane sections for the projective embedding given by H. So, $Z_1 \subset X$ is a hyperplane section, Z_2 is a hyperplane section of Z_1, etc. We have exact sequences

CohomLB;exseq
$$0 \longrightarrow (L^m \otimes H^{q-1})_{|Z_r} \longrightarrow (L^m \otimes H^q)_{|Z_r} \longrightarrow (L^m \otimes H^q)_{|Z_{r+1}} \longrightarrow 0\,. \tag{17}$$

Fix $m > 0$ and let $n = n(m) < m$ be determined by (16). Set $i_1 := i(L) = i(L^m)$ and $i_2 := i(L \otimes H) = i(L^m \otimes H^m)$. Note that $i_1 > i_2$ and $i(L^m \otimes H^q) \geqslant i_1$ for all $q \leqslant n-1$. Similar to what we did in the proofs of (9.20) and (9.22), we shall use the exact sequences (17) to obtain dimension estimates for cohomology groups. As a first step, take $r = 0$ in (17). Since $i_2 < i_1$ we find that $H^{i_2}(X, L^m \otimes H^n)$ injects into $H^{i_2}(Z_1, L^m \otimes H^n)$ and that $H^j(Z_1, L^m \otimes H^q) = 0$ for all $j < i_1 - 1$ and $q \leqslant (n-1)$. Next we want to take $r = 1$, in which case we have the exact sequence

$$H^{i_2}(Z_1, L^m \otimes H^{n-1}) \longrightarrow H^{i_2}(Z_1, L^m \otimes H^n) \longrightarrow H^{i_2}(Z_2, L^m \otimes H^n)\,.$$

Applying the previous conclusions we see that the first term vanishes if $i_2 < i_1 - 1$. If this holds then $H^{i_2}(Z_1, L^m \otimes H^n)$ injects into $H^{i_2}(Z_2, L^m \otimes H^n)$; further we then find that $H^j(Z_2, L^m \otimes H^q) = 0$ for all $j < i_1 - 2$ and $q \leqslant (n-1)$.

Proceeding by induction we find that if $r < i_1 - i_2$ then

$$H^{i_2}(Z_{r-1}, L^m \otimes H^n) \hookrightarrow H^{i_2}(Z_r, L^m \otimes H^n)$$

and

$$H^j(Z_r, L^m \otimes H^q) = 0 \qquad \text{for all } j < i_1 - r \text{ and } q \leqslant (n-1).$$

(The induction breaks down for $r \geqslant i_1 - i_2$.) The conclusion of this (terminating) induction is that $H^{i_2}(X, L^m \otimes H^n)$ maps injectively to $H^{i_2}(Z_{i_1-i_2}, L^m \otimes H^n)$. Comparing dimensions and using (9.20) we find that there exists a constant C such that

CohomLB;Pest
$$\bigl|m^g \cdot P(1, n/m)\bigr| \leqslant C \cdot \bigl|m^{g-(i_1-i_2)}\bigr| \tag{18}$$

for all sufficiently large m. Here $n = n(m) < m$ is a function of m.

Next we write $P(1,t) = (t-\tau)^\mu \cdot R(t)$ where $R(t)$ does not have roots in $[0,1]$. Choose a constant $C' > 0$ with $|R(t)| > C'$ for all $t \in [0,1]$. Combined with (18) this gives

CohomLB;Pest2
$$\bigl|C' \cdot (n/m - \tau)^\mu\bigr| \leqslant \bigl|P\bigl(1, n/m\bigr)\bigr| \leqslant C \cdot \bigl|m^{-(i_1-i_2)}\bigr| \tag{19}$$

for all sufficiently large m.

To finish the argument we distinguish two cases. First assume that $\tau \in \mathbb{Q}$. Let f be its denominator. Recall that we only consider integers m that are coprime with f. For all such m and all $1 \leqslant n \leqslant m$ we have $|n/m - \tau| \geqslant 1/fm$. Using this in (19) and letting m get large we find the desired estimate $i_1 \leqslant i_2 + \mu$. Similarly, if τ is irrational then it suffices to show that there is an infinite sequence of values for m, say $m_1, m_2, \ldots$, and a constant C'' such that

$|n_j/m_j - \tau| \geqslant C''/m_j$ for all j. (Note that the n's are still a function of the m's, determined by the rule that τ lies in the interval $[(n-1)/m, n/m]$.) This is achieved by a theorem of Kronecker which says that the fractional parts of the numbers $m \cdot \tau$, for $m \in \mathbb{N}$, lie dense in the interval $]0,1[$; see Hardy and Wright [1], Chap. 23. □

After all these preparations we are now ready for the main result about the relation between the index and the Hilbert polynomial of L.

IndHilbThm **(9.25) Theorem.** (Kempf-Mumford-Ramanujam) *Let L be a non-degenerate line bundle on an abelian variety X. Let H be an ample line bundle on X and write $\Phi(t) \in \mathbb{Z}[t]$ for the Hilbert polynomial of L with respect to H. (So $\Phi(n) = \chi(L \otimes H^n)$ for all n.) Then all complex roots of Φ are real, and the index $i(L)$ equals the number of positive roots, counted with multiplicities.*

Proof. Writing $P(s,t) = (sl + th)^g$ for the 2-variable polynomial as introduced before (9.22), we have $\Phi(t) = P(1,t)/g!$. For the rest of the proof we may therefore work with $P(1,t)$. Notice that this is a polynomial of degree g.

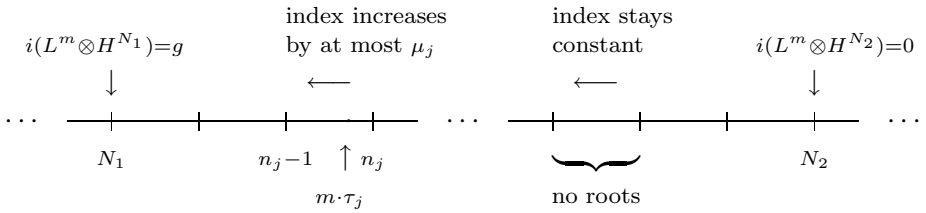
Let $\tau_1, \ldots, \tau_h$ be the real roots of $P(1,t)$, say with multiplicities $\mu_1, \ldots, \mu_h$, respectively. (It will be clear from the arguments below that $h > 0$.) Choose $m \in \mathbb{Z}_{>0}$ and $n_1, \ldots, n_h \in \mathbb{Z}$ such that τ_j lies in the interval $[(n_j - 1)/m, n_j/m]$. We can make these choices such that $P(1,t)$ has no roots of the form n/m, so that all bundles $L^m \otimes H^n$ are non-degenerate.

For $n >> 0$, say $n \geqslant N_2$, the bundle $L^m \otimes H^n$ is ample, so that $i(L^m \otimes H^n) = 0$. Similarly, for $n \leqslant N_1$ the bundle $L^m \otimes H^n$ is anti-ample, in which case $i(L^m \otimes H^n) = g$. (That $h > 0$ is now clear from (9.22).)

Applying Proposition (9.22) and Lemma (9.24) we find that for every $n \in \mathbb{Z}$,

either: $P(1,t)$ has no root in the interval $[(n-1)/m, n/m]$ and $i(L^m \otimes H^{n-1}) = i(L^m \otimes H^n)$,

or: $n = n_j$ (for some j), and $P(1,t)$ has a unique root in $[(n-1)/m, n/m]$, of multiplicity μ_j; in this case $i(L^m \otimes H^{n-1}) \leqslant i(L^m \otimes H^n) + \mu_j$.



Starting at $n = N_2$ and descending in steps of length 1 we find

$$g = i(N_1) - i(N_2) \leqslant \sum_j \mu_j \,.$$

On the other hand, as $P(1,t)$ has degree g we have $\sum_j \mu_j \leqslant g$. The conclusion is that we have equality everywhere: $P(1,t)$ has all its roots real and $i(L^m \otimes H^{n_j - 1}) = i(L^m \otimes H^{n_j}) + \mu_j$ for all j. This also gives that

$$i(L) = i(L^m) = i(L^m \otimes H^0) = \sum_{j;\tau_j > 0} \mu_j \,,$$

and the theorem is proven. □

IndHilbCor **(9.26) Corollary.** *Let $f\colon X \to Y$ be an isogeny. If L is a non-degenerate line bundle on Y then $i(L) = i(f^*L)$.*

Proof. Choose and ample line bundle H on Y. By (9.12), the Hilbert polynomial of f^*L with repsect to the ample bundle f^*H is just $\deg(f)$ times the Hilbert polynomial of L with respect to H. Now apply the theorem. □

The reason that in (9.25) we restrict ourselves to non-degenerate bundles is that only for such bundles the index is well-defined. Without this restriction we still have a quantative result, though.

0Multipl **(9.27) Theorem.** *Let L be a line bundle on an abelian variety X over a field k. Let H be an ample line bundle on X and write $\Phi(t) \in \mathbb{Z}[t]$ for the Hilbert polynomial of L with respect to H. Then the multiplicity of 0 as a root of Φ equals the dimension of $K(L)$.*

Proof. Write $Y := K(L)^0_{\mathrm{red}}$, which is an abelian subvariety of X. There exists an abelian subvariety $Z \subset X$ such that the homomorphism $\nu\colon Y \times Z \to X$ given by $(y, z) \mapsto y + z$ is an isogeny; see Exercise ?? or Theorem (12.2) below. Let $M := (\nu^*L)_{|\{0\}\times Z}$. Note that M is a non-degenerate bundle on Z. We claim that ν^*L differs from p_Z^*M by an element in $\mathrm{Pic}^0_{(Y\times Z)/k}$. Indeed, if we let $N := \nu^*L \otimes p_Z^*M^{-1}$ then $K(N)$ contains both $\{0\} \times Z$ (because $N_{|\{0\}\times Z}$ is trivial) and $Y \times \{0\}$ (because $N_{|Y\times\{0\}} = L_{|Y}$ and $Y \subset K(L)$); hence $K(N) = Y \times Z$, which by Cor. (7.22) means that the class of N lies in $\mathrm{Pic}^0_{(Y\times Z)/k}$. Writing $l = c_1(L)$ and $m = c_1(M)$ we therefore have $\nu^*l = p_Z^*m$. Let $g = \dim(X)$ and $s = \dim(Z)$, and write $h = c_1(H)$. Using Corollary (9.12) we find

$$\begin{aligned}\deg(\nu)\cdot\Phi(t) = \deg(\nu)\cdot(l + t\cdot h)^g &= \big(\nu^*(l+th)\big)^g = \big(p_Z^*m + t\cdot\nu^*h\big)^g \\ &= \sum_{j=0}^{s}\binom{g}{j}\big((p_Z^*m)^j\cdot(\nu^*h)^{g-j}\big)\cdot t^{g-j}\,,\end{aligned}$$

since $m^j = 0$ if $j > s = \dim(Z)$. Moreover, $m^s \neq 0$ because M is non-degenerate; and because ν^*h is an ample class then also $(p_Z^*m)^s \cdot (\nu^*h)^{g-s} \neq 0$. This shows that $\Phi(t)$ is exactly divisible by t^{g-s}. □

If X is an abelian variety over the complex numbers, the associated analytic manifold can be described as a complex torus V/Λ, with V a $\mathbb{C}$-vector space and $\Lambda \subset V$ a lattice. Topologically this is a product of spheres, and the fundamental group can be identified with $\Lambda \cong \mathbb{Z}^{2g}$ (with $g = \dim(X)$). Many properties of X can be expressed in terms of this lattice, and in fact we see that Λ together with the complex structure on $V = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ completely determines X.

Over an arbitrary ground field, we can no longer naturally associate a lattice of rank $2g$ to a g-dimensional abelian variety (see ??), and we have to look for a substitute for Λ. The starting point is the remark that, over $\mathbb{C}$, the fundamental group is also the group of covering transformations of the universal covering of X, and its pro-finite completion classifies the finite coverings of X. Analytically, such finite coverings can be described as $V/\Lambda' \to V/\Lambda$ where $\Lambda' \subset \Lambda$ is a subgroup of finite index; the covering group is then Λ/Λ'. In particular, one finds that any finite covering is dominated by a covering of the form $[n]_X \colon X \to X$ (which corresponds to taking $\Lambda' = n\Lambda$), which has covering group isomorphic to the n-torsion subgroup $X[n] \subset X$. This leads to a description of the pro-finite completion of $\pi_1(X, 0)$ as the projective limit of the finite groups $X[n]$. (Cf. Cor. (10.37).)

Finite coverings of X, as well as torsion points of X, can be studied over arbitrary ground fields. Restricting to the ℓ-primary part, for a prime number ℓ, we are led to consider the so-called Tate-ℓ-module $T_\ell X$ of X, which is a good ℓ-adic analogue of the fundamental group, and which can be defined in elementary terms. These Tate modules turn out to be very useful, and will play an important role in the study of endomorphisms.

If the ground field has positive characteristic p then the Tate-p-module of X has a somewhat different structure than the $T_\ell X$ for $\ell \neq p$, and there is another object, called the p-divisible group, that contains finer information. This p-divisble group, denoted $X[p^\infty]$, will be introduced in the second paragraph.

In the second half of the chapter we give a brief introduction to Grothendieck's theory of the algebraic fundamental group. We then compute the (algebraic) π_1 of an abelian variety, and show that it can indeed be expressed—as already suggested above—in terms of Tate modules.

Throughout this chapter we work over a field k. We let k_s denote a separable closure of k and $\overline{k}$ an algebraic closure. The letter ℓ is reserved for a prime number different from $\mathrm{char}(k)$.

§1. *Tate-ℓ-modules.*

Xln **(10.1)** Let X be a g-dimensional abelian variety over a field k. Let ℓ be a prime number different from $\mathrm{char}(k)$. As we have seen in (5.9) the group scheme $X[\ell^n]$ has rank ℓ^{2ng}, and since this is not divisible by $\mathrm{char}(k)$, Cor. (4.48) shows that $X[\ell^n]$ is étale-étale.

In (3.26) we have seen that a finite étale group scheme is fully described by its group of k_s-valued points equipped with its natural action of $\mathrm{Gal}(k_s/k)$. In the case of $X[\ell^n]$ this means we have to look at the group $X[\ell^n]\big(k_s\big)$ of ℓ^n-torsion points in $X(k_s)$, equipped with its natural Galois action.

Multiplication by ℓ on X induces a homomorphism of group schemes $\ell\colon X[\ell^{n+1}] \to X[\ell^n]$. Under the correspondence of (3.26) it corresponds to the homomorphism of abstract groups

TateBT:lXln
$$\ell\colon X[\ell^{n+1}]\big(k_s\big) \to X[\ell^n]\big(k_s\big)\,, \tag{1}$$

which is $\mathrm{Gal}(k_s/k)$-equivariant. For varying n these maps make the collection $\big\{X[\ell^n]\big(k_s\big)\big\}_{n\in\mathbb{Z}_{\geqslant 0}}$ into a projective system of abelian groups with $\mathrm{Gal}(k_s/k)$-action.

TlXDef **(10.2) Definition.** Let X be an abelian variety over a field k, and let ℓ be a prime number different from $\mathrm{char}(k)$. Then we define the *Tate-ℓ-module of X*, notation $T_\ell X$, to be the projective limit of the system $\big\{X[\ell^n]\big(k_s\big)\big\}_{n\in\mathbb{Z}_{\geqslant 0}}$ with respect to the transition maps (1). In other words,

$$T_\ell X := \lim\Big(\{0\} \xleftarrow{\ell} X[\ell]\big(k_s\big) \xleftarrow{\ell} X[\ell^2]\big(k_s\big) \xleftarrow{\ell} X[\ell^3]\big(k_s\big) \xleftarrow{\ell} \cdots\Big)\,.$$

If $\mathrm{char}(k) = p > 0$ then we define

$$T_{p,\text{ét}}X := \lim\Big(\{0\} \xleftarrow{p} X[p]\big(\overline{k}\big) \xleftarrow{p} X[p^2]\big(\overline{k}\big) \xleftarrow{p} X[p^3]\big(\overline{k}\big) \xleftarrow{p} \cdots\Big)\,.$$

In concrete terms this means that an element of $T_\ell X$ is a sequence $x = (0, x_1, x_2, \ldots)$ with $x_n \in X(k_s)$ an ℓ^n-torsion point, and with $\ell \cdot x_{n+1} = x_n$ for all n. The addition on $T_\ell X$ is done coordinatewise, and if we have an ℓ-adic number $a = (a_0, a_1, a_2, \ldots)$ with $a_i \in \mathbb{Z}/\ell^i\mathbb{Z}$ and $a_{i+1} \bmod \ell^i = a_i$, then $a \cdot x = (0, a_1 x_1, a_2 x_2, \ldots)$.

In practice we often simply call $T_\ell X$ the Tate module of X, especially when the choice of ℓ plays no particular role.

Note that for $\ell \neq \mathrm{char}(k)$ we get the same module $T_\ell X$ if in the definition we replace $X[\ell^n]\big(k_s\big)$ by $X[\ell^n]\big(\overline{k}\big)$; see Prop. (5.11). In fact, we prefer to state the definition using the separable closure k_s, as we usually want to consider $T_\ell X$ with its natural action of $\mathrm{Gal}(k_s/k)$; see below. For the definition of $T_{p,\text{ét}}X$, it does make a difference that we work with torsion points over $\overline{k}$ (and not k_s); see (5.24).

Though the definition of $T_{p,\text{ét}}X$ is perfectly analogous to that of $T_\ell X$, this "Tate-p-module" is not really a good analogue of the Tate-ℓ-modules. This is why we use a slightly different notation for it. See further the discussion in § 2.

TlXBasics **(10.3)** It follows from (5.11) that $T_\ell X$ is (non-canonically) isomorphic to

$$\lim\Big(\{0\} \xleftarrow{\ell} (\mathbb{Z}/\ell\mathbb{Z})^{2g} \xleftarrow{\ell} (\mathbb{Z}/\ell^2\mathbb{Z})^{2g} \xleftarrow{\ell} (\mathbb{Z}/\ell^3\mathbb{Z})^{2g} \xleftarrow{\ell} \cdots\Big) = \mathbb{Z}_\ell^{2g}\,.$$

In other words, $T_\ell X$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. We also introduce

$$V_\ell X := T_\ell X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell\,,$$

a $\mathbb{Q}_\ell$-vector space of dimension $2g$.

But T_ℓ is not just a $\mathbb{Z}_\ell$-module. We have a natural action of $\mathrm{Gal}(k_s/k)$ on the projective system $\big\{X[\ell^n]\big(k_s\big)\big\}$, and this gives rise to an integral ℓ-adic representation

$$\rho_\ell\colon \mathrm{Gal}(k_s/k) \to \mathrm{GL}(T_\ell X)\,.$$

We refer to Appendix ?? for some basic notions on ℓ-adic representations. If there is no risk of confusion we use the same notation ρ_ℓ for the ℓ-adic representation with values in $\mathrm{GL}(V_\ell X)$.

Note that we can find back the group scheme $X[\ell^n]$ from $T_\ell X$ with its Galois action, since $T_\ell X/\ell^n T_\ell X \cong X[\ell^n]\big(k_s\big)$. Therefore, knowing the Tate-ℓ-module with its action of $\mathrm{Gal}(k_s/k)$ is equivalent to knowing the full projective system of group schemes $X[\ell^n]$.

TlAltDef **(10.4)** The group $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the union of its subgroups $\ell^{-n}\mathbb{Z}_\ell/\mathbb{Z}_\ell$. Phrased differently, $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the inductive limit of the system $\{\mathbb{Z}/\ell^n\mathbb{Z}\}_{n\geqslant 0}$, where the transition maps are the homomorphisms $\mathbb{Z}/\ell^n\mathbb{Z} \hookrightarrow \mathbb{Z}/\ell^{n+1}\mathbb{Z}$ given by $(1 \bmod \ell^n) \mapsto (\ell \bmod \ell^{n+1})$.

The definition of the Tate-ℓ-module may be reformulated by saying that

$$T_\ell X = \mathrm{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big)\,,$$

where we take homomorphisms of abstract groups. Indeed,

$$\mathrm{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big) = \varprojlim_n \mathrm{Hom}\big(\mathbb{Z}/\ell^n\mathbb{Z}, X(k_s)\big) = \varprojlim_n X[\ell^n]\big(k_s\big)\,,$$

where in the last term the transition maps are given by multiplication by ℓ. Concretely, if $(0, x_1, x_2, \ldots)$ with $x_n \in X[\ell^n](k_s)$ is an element of $T_\ell X$ then the corresponding homomorphism $\mathbb{Q}_\ell/\mathbb{Z}_\ell \to X(k_s)$ sends the class of ℓ^{-n} to x_n. In this description the $\mathrm{Gal}(k_s/k)$-action on $T_\ell X$ is induced by the Galois action on $X(k_s)$.

Tlf **(10.5)** A homomorphism $f\colon X \to Y$ gives rise to a $\mathbb{Z}_\ell$-linear, $\mathrm{Gal}(k_s/k)$-equivariant map $T_\ell f\colon T_\ell X \to T_\ell Y$. It sends a point $(0, x_1, x_2, \ldots)$ of $T_\ell X$ to the point $\big(0, f(x_1), f(x_2), \ldots\big)$ of $T_\ell Y$.

Suppose f is an isogeny with kernel $N \subset X$. Applying $\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, -)$ to the exact sequence $0 \longrightarrow N(k_s) \longrightarrow X(k_s) \longrightarrow Y(k_s) \longrightarrow 0$ we obtain an exact sequence

$$\begin{aligned} 0 \longrightarrow T_\ell X \xrightarrow{T_\ell f} T_\ell Y \longrightarrow \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s)\big) \\ \longrightarrow \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big) \longrightarrow \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, Y(k_s)\big)\,, \end{aligned} \tag{2}$$

TateBT:TXTY

where the Ext terms are computed in the category Ab of abelian groups.

Let us first try to understand the term $\mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s)\big)$. We use that if A and B are abelian groups, multiplication by an integer n on $\mathrm{Ext}^1(A,B)$ equals the map induced by $[n]_A$ (multiplication by n on A), and also equals the map induced by $[n]_B$.

Write $N = N_\ell \times N^\ell$ with N^ℓ a group scheme of order prime to ℓ and N_ℓ a group scheme of ℓ-power order. If m is the order of N^ℓ then multiplication by m kills $N^\ell(k_s)$ but is a bijection on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Hence

$$\begin{aligned} \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s)\big) &= \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(k_s)\big) \times \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N^\ell(k_s)\big) \\ &= \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(k_s)\big)\,. \end{aligned}$$

Next consider the long exact sequence

$$\begin{aligned} \cdots \longrightarrow \mathrm{Hom}\big(\mathbb{Q}_\ell, N_\ell(k_s)\big) \longrightarrow \mathrm{Hom}\big(\mathbb{Z}_\ell, N_\ell(k_s)\big) \\ \longrightarrow \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N_\ell(k_s)\big) \longrightarrow \mathrm{Ext}^1\big(\mathbb{Q}_\ell, N_\ell(k_s)\big) \longrightarrow \cdots\,. \end{aligned} \tag{3}$$

TateBT:ExtN

For a sufficiently big $N_\ell(k_s)$ is killed by ℓ^a, so multiplication by ℓ^a induces the zero map on all terms in (3). On the other hand, multiplication by ℓ^a is a bijection on $\mathbb{Q}_\ell$ and therefore

induces an bijection on the terms $\mathrm{Ext}^i\big(\mathbb{Q}_\ell, N_\ell(k_s)\big)$. Hence the terms $\mathrm{Hom}\big(\mathbb{Q}_\ell, N_\ell(k_s)\big)$ and $\mathrm{Ext}^1\big(\mathbb{Q}_\ell, N_\ell(k_s)\big)$ vanish, and the conclusion is that

TateBT:Ext1N
$$\mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, N(k_s)\big) \cong \mathrm{Hom}\big(\mathbb{Z}_\ell, N_\ell(k_s)\big) \cong N_\ell(k_s)\,. \tag{4}$$

Write $E^1(f)$: $\mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big) \to \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, Y(k_s)\big)$ for the map induced by f. We claim it is injective. If the ground field k is perfect, so that $k_s = \overline{k}$, then we know from Cor. (5.10) that $X(k_s)$ is a divisible group, and is therefore an injective object in the category of abelian groups. Hence in this case $\mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big) = 0$. In the general case, we first choose an isogeny g: $Y \to X$ such that $g\circ f = [n]_X$ for some positive integer n. Then $E(g\circ f)$ is multiplication by n on $\mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big)$. Now write $n = \ell^m \cdot n'$ with $\ell \nmid n'$. Multiplication by n' is a bijection on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$; so it suffices to show that $E^1(\ell^m)$ is injective. But if we take $f = \ell^m$ then the sequence (2) becomes

$$\begin{aligned} 0 \longrightarrow T_\ell X \xrightarrow{\ell^m} T_\ell X \xrightarrow{\delta} \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X[\ell^m](k_s)\big) \\ \longrightarrow \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big) \xrightarrow{E^1(\ell^m)} \mathrm{Ext}^1\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X(k_s)\big)\,, \end{aligned}$$

and it follows from (4) that δ is surjective. This proves our claim.

Finally we remark that the maps in (2) are equivariant for the natural Galois actions on all terms. To summarize, we have the following conclusion.

TfProp **(10.6) Proposition.** *Let f: $X \to Y$ be an isogeny of abelian varieties over a field k, with kernel N. If ℓ is a prime number with $\ell \neq \mathrm{char}(k)$ then we have an exact sequence of $\mathbb{Z}_\ell\big[\mathrm{Gal}(k_s/k)\big]$-modules*

$$0 \longrightarrow T_\ell X \xrightarrow{T_\ell f} T_\ell Y \longrightarrow N_\ell(k_s) \longrightarrow 0$$

where $N_\ell(k_s)$ is the ℓ-Sylow subgroup of $N(k_s)$.

TfCor **(10.7) Corollary.** *If f: $X \to Y$ is an isogeny then for all $\ell \neq \mathrm{char}(k)$ the induced map $V_\ell f$: $V_\ell X \to V_\ell Y$ is an isomorphism.*

TlG **(10.8)** The construction of the Tate module makes sense for arbitrary group varieties. Thus, if G is a group variety over k and $\ell \neq \mathrm{char}(k)$ then we can form

$$T_\ell G := \lim\Big(\{0\} \xleftarrow{\ell} G[\ell]\big(k_s\big) \xleftarrow{\ell} G[\ell^2]\big(k_s\big) \xleftarrow{\ell} G[\ell^3]\big(k_s\big) \xleftarrow{\ell} \cdots\Big)\,.$$

In some cases the result is not very interesting. For instance, $T_\ell \mathbb{G}_a = 0$. But the Tate module of the multiplicative group $\mathbb{G}_m$ is a fundamental object; so much so that it has a special notation: we write

$$\mathbb{Z}_\ell(1) := T_\ell \mathbb{G}_m = \lim\Big(\{1\} \xleftarrow{(\ )^\ell} \mu_\ell(k_s) \xleftarrow{(\ )^\ell} \mu_{\ell^2}(k_s) \xleftarrow{(\ )^\ell} \mu_{\ell^3}(k_s) \xleftarrow{(\ )^\ell} \cdots\Big)\,.$$

(In this case we of course use multiplicative notation.) As a $\mathbb{Z}_\ell$-module, $\mathbb{Z}_\ell(1)$ is free of rank 1. The action of $\mathrm{Gal}(k_s/k)$ is therefore given by a character

$$\chi_\ell\colon \mathrm{Gal}(k_s/k) \to {\mathbb{Z}_\ell}^* = \mathrm{GL}\big(\mathbb{Z}_\ell(1)\big)\,,$$

called the ℓ-adic cyclotomic character.

As discussed in Appendix ??, if T is any ℓ-adic representation of $\mathrm{Gal}(k_s/k)$ then we define $T(n)$, called "T twisted by n", to be

$$\begin{cases} T \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1)^{\otimes n} & \text{if } n \geqslant 0, \\ T \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(-1)^{\otimes -n} & \text{if } n \leqslant 0, \end{cases}$$

where $\mathbb{Z}_\ell(-1) := \mathbb{Z}_\ell(1)^\vee$ and $\mathbb{Z}_\ell(1)^{\otimes 0}$ is defined to be $\mathbb{Z}_\ell$ with trivial Galois action. Concretely, if ρ is the Galois action on T then $T(n)$ is isomorphic to T as a $\mathbb{Z}_\ell$-module, but with $\sigma \in \mathrm{Gal}(k_s/k)$ acting via $\chi_\ell(\sigma)^n \cdot \rho(\sigma)$.

TlXt **(10.9) Proposition.** *We have a canonical isomorphism*

$$T_\ell X^t \cong (T_\ell X)^\vee\big(1\big)\,.$$

Proof. By Thm. (7.5) we have $X^t[\ell^n] \cong X[\ell^n]^D$, and therefore

$$X^t[\ell^n]\big(k_s\big) \cong \mathrm{Hom}\Big(X[\ell^n]\big(k_s\big), k_s^*\Big) = \mathrm{Hom}\Big(X[\ell^n]\big(k_s\big), \mu_{\ell^n}\big(k_s\big)\Big)$$

as groups with Galois action. Now take projective limits. □

§2. *The p-divisible group.*

If $\mathrm{char}(k) = p > 0$ then the "Tate-p-module" $T_{p,\text{ét}}X$ is in many respects not the right object to consider. For instance, whereas $T_\ell X$ (for $\ell \neq \mathrm{char}(k)$, as always) has rank $2g$ over $\mathbb{Z}_\ell$, independent of ℓ, the rank of the module $T_{p,\text{ét}}X$ equals the p-rank of X, and as we know this is an integer with $0 \leqslant f(X) \leqslant g$. In particular, $T_{p,\text{ét}}X$ could be zero.

We have seen that the Tate-ℓ-module captures the full system of group *schemes* $X[\ell^n]$. That this system can be encoded into a single $\mathbb{Z}_\ell$-module with Galois action is due to the fact that $X[\ell^n]$ is étale for every n. So we should really consider the full system of group schemes $X[p^n]$. It turns out that it is most convenient to put these into an inductive system, and in this way we arrive at the p-divisible group of an abelian variety.

Let us now first give the definition of a p-divisible group in a general setting.

BTDefGen **(10.10) Definition.** Let S be a base scheme. A p-divisible group over S, also called a Barsotti-Tate group over S, is an inductive system

$$\big\{G_n\,;\, i_n\colon G_n \to G_{n+1}\big\}_{n\in\mathbb{N}}\,, \quad \text{in other words:} \quad G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \xrightarrow{i_3} \cdots\,,$$

where:

(i) each G_n is a commutative finite locally free S-group scheme, killed by p^n, and flat when viewed as a sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules;

(ii) each $i_n\colon G_n \to G_{n+1}$ is a homomorphism of S-group schemes, inducing an isomorphism $G_n \xrightarrow{\sim} G_{n+1}[p^n]$.

Homomorphisms of p-divisible groups are defined to be the homomorphisms of inductive systems of group schemes.

The flatness condition in (i) of the definition can be rephrased in more elementary terms, as in the following lemma.

BTFlatLem **(10.11) Lemma.** *Let S be a scheme. Let p be a prime number. If H is an fppf sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules on S then the following are equivalent:*

(i) *H is flat as a sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules;*

(ii) *$\mathrm{Ker}(p^i) = \mathrm{Im}(p^{n-i})$ for all $i \in \{0, 1, \ldots, n\}$.*

Proof. We closely follow Messing [1], Chap. I, § 1. For (i) ⇒ (ii), start with the exact sequence

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{p^{n-i}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{p^i} \mathbb{Z}/p^n\mathbb{Z}\,.$$

If H is flat over $\mathbb{Z}/p^n\mathbb{Z}$ then $- \otimes H$ gives an exact sequence

TateBT:HHH
$$H \xrightarrow{p^{n-i}} H \xrightarrow{p^i} H \tag{5}$$

and we see that (ii) holds.

For the proof of (ii) ⇒ (i) we use some results of Bourbaki [2]. These results are stated in the context of modules over rings, but they carry over (with the same proofs) to the setting of sheaves.

We use the flatness criterion, loc. cit., Chap. III, § 5, Thm. 1 together with ibid., Prop. 1. This tells us that H is flat over $\mathbb{Z}/p^n\mathbb{Z}$ if and only if the following two conditions hold:

(a) H/pH is flat as a sheaf of $\mathbb{F}_p$-modules;

(b) $\mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(\mathbb{Z}/p^i\mathbb{Z}, H) = 0$ for all $i \geqslant 0$.

But (a) is trivially true, as $\mathbb{F}_p$ is a field. To see that (b) holds, start with

$$0 \longrightarrow \mathbb{Z}/p^{n-i}\mathbb{Z} \xrightarrow{p^i} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^i\mathbb{Z} \longrightarrow 0\,.$$

This gives a long exact sequence

$$0 \longrightarrow \mathrm{Tor}_1^{\mathbb{Z}/p^n\mathbb{Z}}(\mathbb{Z}/p^i\mathbb{Z}, H) \longrightarrow H/p^{n-i}H \xrightarrow{p^i} H \longrightarrow H/p^iH \longrightarrow 0\,.$$

But assumption (ii), equivalent to the exactness of (5), says precisely that $p^i\colon H/p^{n-i}H \to H$ is injective. □

BTGenRem **(10.12)** Let $\{G_n; i_n\}$ be a p-divisible group over S. If m and n are natural numbers then the composition

$$i_{m,n}\colon G_m \xrightarrow{i_m} G_{m+1} \xrightarrow{i_{m+1}} \cdots \xrightarrow{i_{m+n-1}} G_{m+n}$$

gives an identification $G_m \xrightarrow{\sim} G_{m+n}[p^m]$. Hence we may view G_m as a subgroup scheme of G_{m+n}.

On the other hand, since G_{m+n} is killed by p^{m+n} the map $[p^m]\colon G_{m+n} \to G_{m+n}$ factors through $G_{m+n}[p^n] = G_n$. If there is no risk of confusion we simply write $p^m\colon G_{m+n} \to G_n$ for the induced homomorphism. By Lemma (10.11) this last map is an epimorphism. Hence the sequence

TateBT:ExSeq
$$0 \longrightarrow G_m \xrightarrow{i_{m,n}} G_{m+n} \xrightarrow{p^m} G_n \longrightarrow 0 \tag{6}$$

is exact.

BTfppf **(10.13)** Given a p-divisible group as in the above definition, we may consider the G_n as fppf sheaves on S and form the limit

$$G := \varinjlim_n G_n \,,$$

in the category of fppf sheaves of abelian groups. We can recover G_n from G by $G_n = G[p^n]$.

If $\{G_n\}$ and $\{H_n\}$ are two p-divisible groups and we form $G := \varinjlim G_n$ and $H := \varinjlim H_n$, then the homomorphisms from $\{G_n\}$ to $\{H_n\}$ are just the homomorphisms from G to H as fppf sheaves. In other words, by passing from the inductive system $\{G_n\}$ to the limit G we can identify the category of p-divisible groups over S with a full subcategory of the category of fppf sheaves in abelian groups over S.

An fppf sheaf G is (or "comes from") a p-divisible group if and only if it satisfies the following conditions:

(i) G is p-divisible in the sense that $[p]_G\colon G \to G$ is an epimorphism;

(ii) G is p-torsion, meaning that $G = \varinjlim_n G[p^n]$;

(iii) the subsheaves $G[p^n]$ are representable by finite locally free S-group schemes.

To go back from a sheaf G satisfying these conditions to a p-divisible group as defined in (10.10), take $G_n := G[p^n]$, and let $i_n\colon G_n \to G_{n+1}$ be the natural inclusion. It follows from (i) that $[p^n]_G$ is an epimorphism for all n, and this implies that for all m and n we have an exact sequence as in (6). By Lemma (10.11), we conclude that each G_n is flat as a sheaf of $\mathbb{Z}/p^n\mathbb{Z}$-modules; hence the system $\{G_n; i_n\}_n$ is a p-divisible group. As a further simplification, it can be shown that it suffices to require (iii) for $G[p]$; see Messing [1], Chap. I, § 1.

We can go one step further by remarking that, as a consequence of (ii), a p-divisible group G has a natural structure of a sheaf in $\mathbb{Z}_p$-modules. More concretely, suppose we have a p-adic number $a = (a_1, a_2, \ldots)$ with $a_i \in \mathbb{Z}/p^i\mathbb{Z}$. Then a acts on G_n as multiplication by a_n; this gives a well-defined $\mathbb{Z}_p$-module structure on the limit G because the diagrams

$$\begin{array}{ccc} G_n & \xrightarrow{a_n\cdot} & G_n \\ {\scriptstyle i_n}\downarrow & & \downarrow{\scriptstyle i_n} \\ G_{n+1} & \xrightarrow[a_{n+1}\cdot]{} & G_{n+1} \end{array}$$

are commutative. Homomorphisms of p-divisible groups are automatically $\mathbb{Z}_p$-linear. In particular, $\mathrm{Hom}(G, H)$ has a natural structure of a $\mathbb{Z}_p$-module.

BTNameRem **(10.14) Remark.** The name "p-divisible group" refers to condition (i) in (10.13). But we see that the requirement for an fppf sheaf G to be a p-divisble group in the sense of Def. (10.10) is stronger than only this condition. Thus, strictly speaking the terminology "p-divisible group" is not correct. This is one of the reasons that some prefer the terminology "Barsotti-Tate group", after two of the pioneers in this area.

BTheight **(10.15)** If $G = \varinjlim G_n$ is a p-divisible group over a connected base scheme S then, by definition, the group scheme G_1 is locally free and killed by p. It follows that the rank of G_1 equals p^h for some integer h. (Use Exercise (4.4).) This integer $h = h(G)$ is called the *height* of G. It readily follows from (6) and Lemma (4.46) that G_n, which is again locally free, has rank p^{nh}.

Over an arbitrary basis S, we define the height of a p-divisible group G as the locally constant function $|S| \to \mathbb{Z}_{\geqslant 0}$ given by $s \mapsto h\big(G(s)\big)$.

BTAVDef **(10.16) Definition.** Let X be an abelian variety over a field k. Let p be a prime number. Then we define the *p-divisible group of X*, notation $X[p^\infty]$, to be the inductive system

$$\big\{X[p^n]\big\}_{n\geqslant 0}$$

with respect to the natural inclusion homomorphisms $X[p^n] \hookrightarrow X[p^{n+1}]$.

Note that $X[p^\infty]$ has height $2g$, where $g = \dim(X)$.

fpinftyDef **(10.17)** A homomorphism $f\colon X \to Y$ of abelian varieties over k induces a homomorphism $f[p^\infty]\colon X[p^\infty] \to Y[p^\infty]$ of p-divisible groups.

If we take $f = [n]_X$ for some integer n then the induced endomorphism of $X[p^\infty]$ is multiplication by n, which for $n \neq 0$ is surjective (as a homomorphism of fppf sheaves). Using Prop. (5.12) it follows that if f is an isogeny then $f[p^\infty]$ is an epimorphism of fppf sheaves. Hence if f is an isogeny with kernel N we find an exact sequence of fppf sheaves

$$0 \longrightarrow N_p \longrightarrow X[p^\infty] \xrightarrow{f[p^\infty]} Y[p^\infty] \longrightarrow 0\,,$$

where we write $N = N_p \times N^p$ with N_p of p-power order and N^p a group scheme of order prime to p.

SerreDual **(10.18)** Let us return to the general context of a p-divisible group G over a base scheme S. Applying Cartier duality to (6) gives an exact sequence

$$0 \longrightarrow G_n^D \longrightarrow G_{m+n}^D \longrightarrow G_m^D \longrightarrow 0\,.$$

In particular, taking $m = 1$ this gives homomorphisms $\iota_n\colon G_n^D \to G_{n+1}^D$. The inductive system $\big\{G_n^D\,;\,\iota_n\big\}$ is again a p-divisible group; it is called the Serre dual of G.

A homomorphism $f\colon G \to H$ induces a dual homomorphism $f^D\colon H^D \to G^D$; in this way $G \mapsto G^D$ gives a contravariant functor from the category of p-divisible groups over S to itself. The collection of isomorphisms $(G_n^D)^D \xrightarrow{\sim} G_n$ give a canonical isomorphism $(G^D)^D \xrightarrow{\sim} G$.

It is immediate from the defnitions that the Serre-dual of G has the same height as G.

BTXt **(10.19) Proposition.** *If X/k is an abelian variety then we have a canonical isomorphism*

$$X^t[p^\infty] \cong X[p^\infty]^D\,.$$

Proof. Immediate from Thm. (7.5) and the definition of the Serre dual. □

GmhatDef **(10.20)** Like the construction of a Tate module, the definition of a p-divisible group also makes sense for certain other commutative group varieties. Beyond abelian varieties, the main example of interest is the p-divisible group $\mathbb{G}_m[p^\infty]$ associated to $\mathbb{G}_m$. By definition, $\mathbb{G}_m[p^\infty]$ is the inductive system of group schemes μ_{p^n} with respect to the natural inclusions $\mu_{p^n} \hookrightarrow \mu_{p^{n+1}}$. If we work over a field k and view $\mathbb{G}_m[p^\infty]$ as an fppf sheaf on $\mathrm{Spec}(k)$ then we have

$$\mathbb{G}_m[p^\infty]\big(R\big) = \big\{x \in R^* \;\big|\; x^{p^n} = 1 \text{ for some } n \geqslant 0\big\}\,,$$

for any k-algebra R. The height of $\mathbb{G}_m[p^\infty]$ is 1.

The Serre-dual of $\mathbb{G}_m[p^\infty]$ is the p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$, i.e., the inductive limit of constant group schemes $\mathbb{Z}/p^n\mathbb{Z}$ with respect to the inclusion maps $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} p\mathbb{Z}/p^{n+1}\mathbb{Z} \subset \mathbb{Z}/p^{n+1}\mathbb{Z}$.

etlocBT **(10.21)** As we have seen in Prop. (4.45), a finite commutative group scheme over a field k is, in a canonical way, an extension of an étale group scheme by a local group scheme. An immediate consequence of this is that any p-divisible group $G = \varinjlim G_n$ over k is an extension

TateBT:GGGseq
$$1 \longrightarrow G_{\mathrm{loc}} \longrightarrow G \longrightarrow G_{\text{ét}} \longrightarrow 1 \tag{7}$$

of the "ind-étale" p-divisible group $G_{\text{ét}} = \varinjlim G_{n,\text{ét}}$ by the "ind-local" p-divisible group $G_{\mathrm{loc}} = \varinjlim G_{n,\mathrm{loc}}$. To simplify terminology, the prefix "ind-" is often omitted; e.g., G is called an étale p-divisible group if $G \xrightarrow{\sim} G_{\text{ét}}$.

If k is perfect then the sequence (7) splits. See Exercise (10.1).

Combining the above with the Serre-duality functor $G \mapsto G^D$ of (10.18), we can further decompose G_{loc} as an extension of a local-local p-divisble group by a local-étale one. Here we extend the terminology introduced in (4.42) in an obvious way to p-divisible groups. Similarly, $G_{\text{ét}}$ is an extension of an étale-local p-divisible group by an étale-étale one.

TpofBT **(10.22)** If G is a p-divisible group over k, viewed as an fppf sheaf, then we define its Tate-p-module by $T_pG := \mathrm{Hom}\big(\mathbb{Q}_p/\mathbb{Z}_p, G(\overline{k})\big)$. Concretely, we take the limit of the projective system

$$G_1(k_s) \xleftarrow{\pi_{1,1}} G_2(k_s) \xleftarrow{\pi_{1,2}} G_3(k_s) \xleftarrow{\pi_{1,3}} \cdots .$$

As usual, T_pG is a $\mathbb{Z}_p$-module that comes equipped with a continuous action of $\mathrm{Gal}(k_s/k)$.

It is clear from the definitions that T_pG only sees the étale part of G, i.e., the canonical map $T_pG \to T_pG_{\text{ét}}$ is an isomorphism. It follows that T_pG is a free $\mathbb{Z}_p$-module of rank $h(G_{\text{ét}})$.

If $p \neq \mathrm{char}(k)$ then clearly the Tate module of $X[p^\infty]$ is the same as the Tate-p-module of X as defined in (10.2). The Tate module of $\mathbb{G}_m[p^\infty]$ is $\mathbb{Z}_p(1)$.

BTpchark **(10.23)** Thus far we have not made any assumptions on the prime p in relation to the characteristic of the ground field k. But if $p \neq \mathrm{char}(k)$ then it follows from Prop. (4.47) that any p-divisible group G over k is étale-étale. More precisely, G_{k_s} is non-canonically isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{h(G)}$. In this case it is an easy exercise to show that the functor $G \mapsto T_pG$ gives an equivalence from the category of p-divisible groups over k to the category of free $\mathbb{Z}_p$-modules of finite rank equipped with a continuous action of $\mathrm{Gal}(k_s/k)$. This functor is compatible with duality, in the sense that $T_p(G^D)$ is canonically isomorphic to $(T_pG)^\vee(1)$.

In sum, for $p \neq \mathrm{char}(k)$, a p-divisible group carries the same information as the corresponding Tate module, and we typically work with the latter. (To stress that $p \neq \mathrm{char}(k)$ we shall use the letter ℓ rather than p.) By contrast, if $\mathrm{char}(k) = p > 0$ then a p-divisible group in general contains finer information than the associated Tate module.

BTFormGp **(10.24)** To conclude this general section on p-divisible groups, let us discuss the relation with formal groups. (??TO BE COMPLETED??)

§3. *The algebraic fundamental group—generalities.*

In Topology one defines the fundamental group $\pi_1(X,x)$ of a space X with base point $x \in X$ as the group of homotopy classes (rel. $\{0,1\}$) of paths $\gamma\colon [0,1] \to X$ with $\gamma(0) = \gamma(1) = x$. Now suppose we want to define the fundamental group of an algebraic variety over an arbitrary field. Working with the Zariski topology does not give reasonable answers—for instance, any two algebraic curves over the same field are homeomorphic as topological spaces! Further, the above topological definition via paths does not have an obvious "algebraic" analogue that works well. (In fact, an algebraic analogue of homotopy theory was developed only in the 1990's; see Morel and Voevodsky [1].)

Assuming that X is locally connected and locally simply connected, an alternative description of $\pi_1(X,x)$ is that it is the automorphism group of the universal covering $\tilde{X} \to X$. See for instance Massey [1] or Rotman [1]. In this description the fundamental group becomes the group which classifies topological coverings of X. This is similar to Galois theory of fields, and it was one of Grothendieck's fundamental insights that it is possible to develop an abstract Galois theory of which both are special instances. Using finite étale morphisms as coverings, this theory also applies to algebraic schemes and gives rise to a notion of an algebraic fundamental group.

We shall now recall the definition of the algebraic fundamental group $\pi_1(X,\bar{x})$, and some basic properties. For further introduction we refer to SGA1. On a more advanced level, but very readable, is Deligne [4], § 10. We shall write π_1 for the algebraic fundamental group and use the notation π_1^{top} for the fundamental group in the classical setting of topological spaces.

EtCovDef **(10.25) Definition.** Let X be a scheme. By an *étale covering* of X we mean a finite étale morphism $Y \to X$. (Do not confuse this with the notion of a covering for the étale topology.) We write $\mathsf{FEt}_{/X} \subset \mathsf{Sch}_{/X}$ for the full subcategory of such étale coverings. Note that the morphisms in $\mathsf{FEt}_{/X}$ are automatically again étale coverings. We say that an étale covering $f\colon Y \to X$ *dominates* the étale covering $g\colon Z \to X$ if there exists a morphism $h\colon Y \to Z$ with $f = g \circ h$.

Fix an algebraically closed field Ω and a geometric point $\bar{x}\colon \mathrm{Spec}(\Omega) \to X$. We define a functor

$$F_{\bar{x}}\colon \mathsf{FEt}_{/X} \to \mathsf{Sets}$$

by $F_{\bar{x}}(f\colon Y \to X) = \big\{y \in Y(\Omega) \;\big|\; f(y) = x\big\}$. In other words, $F_{\bar{x}}$ associates to an étale covering of X the set of geometric points lying over $\bar{x}$.

Pi1Def **(10.26) Definition.** (Grothendieck) Assume X to be locally noetherian and connected. Then the algebraic fundamental group $\pi_1(X,\bar{x})$ is defined to be the automorphism group of the functor $F_{\bar{x}}$.

Pi1Field **(10.27) Example.** Suppose $X = \mathrm{Spec}(k)$ is the spectrum of a field. The geometric point $\bar{x}$ corresponds to an embedding $\sigma\colon k \hookrightarrow \Omega$. An étale covering of X is a finite disjoint union of schemes $\mathrm{Spec}(L)$, where $k \subset L$ is a finite separable field extension. For such a scheme $Y = \mathrm{Spec}(L)$ we have

$$F_{\bar{x}}(Y) = \big\{\text{embeddings } \tau\colon L \hookrightarrow \Omega \text{ with } \tau_{|k} = \sigma\big\}\,.$$

Write k_s for the separable closure of k inside Ω. Clearly, every element of $\mathrm{Gal}(k_s/k)$ gives an automorphism of the functor $F_{\bar{x}}$. Conversely, if $\alpha \in \mathrm{Aut}(F_{\bar{x}})$ and $\xi \in k_s$ then the inclusion $k(\xi) \subset \Omega$ gives an Ω-valued point of $\mathrm{Spec}\big(k(\xi)\big)$ lying above $\bar{x}$, in other words, an element $i \in F_{\bar{x}}\big(\mathrm{Spec}(k(\xi))\big)$. Then $\alpha(i)$ is another embedding of $k(\xi)$ into Ω that extends σ. Sending ξ

to its image under $\alpha(i)$ defines an element of $\mathrm{Gal}(k_s/k)$. These two constructions are inverse to each other, so we find a canonical isomorphism of pro-finite groups

$$\pi_1\big(\mathrm{Spec}(k), \bar{x}\big) \cong \mathrm{Gal}(k_s/k)\,.$$

Notice that the elements of $\pi_1\big(\mathrm{Spec}(k), \bar{x}\big)$ do not directly appear as automorphisms of the field k_s. Rather, if $\alpha \in \pi_1\big(\mathrm{Spec}(k), \bar{x}\big)$ corresponds to $\beta \in \mathrm{Gal}(k_s/k)$ then α describes the effect that β has on all embeddings $L \hookrightarrow k_s$ (= the geometric points lying over $\bar{x}$ in the covering $\mathrm{Spec}(L) \to X$). So, to phrase it in a more topological way, the point here is that an automorphism of the "universal covering" of X is completely determined by its effect on the points in the fibre over the base point $\bar{x}$.

Pi1Thm **(10.28) Theorem.** (Grothendieck) *Assume X to be locally noetherian and connected. Then $\pi_1 = \pi_1(X, \bar{x})$ is a pro-finite group, and $F_{\bar{x}}$ induces an equivalence of categories*

$$\mathsf{FEt}_{/X} \xrightarrow{\mathrm{eq}} \begin{pmatrix} \text{finite} \\ \pi_1\text{-sets} \end{pmatrix},$$

where the right hand side denotes the category of finite sets with a continuous action of $\pi_1(X, \bar{x})$.

For the proof of this theorem we refer to SGA1, in particular Exp. V. Note that in case $X = \mathrm{Spec}(k)$ we have already seen this result in (3.25).

From now on, whenever we consider an algebraic fundamental group, it is assumed that the scheme in question is locally noetherian and connected.

We shall briefly review some basic properties of the fundamental group. Proofs may be found in SGA1. Note that some of the results discussed below are ingredients of the proof of Thm. (10.28), rather than being consequences of it.

pi1DepBP **(10.29)** *Dependence on the choice of a base point.* Suppose we have two geometric points $\bar{x}_1\colon \mathrm{Spec}(\Omega_1) \to X$ and $\bar{x}_2\colon \mathrm{Spec}(\Omega_2) \to X$; here the (algebraically closed) fields Ω_1 and Ω_2 may be different, and may even have different characteristics. The theorem implies that there is an equivalence of categories

TateBT:pi1BP
$$\begin{pmatrix} \text{finite} \\ \pi_1(X, \bar{x}_1)\text{-sets} \end{pmatrix} \xrightarrow{\mathrm{eq}} \begin{pmatrix} \text{finite} \\ \pi_1(X, \bar{x}_2)\text{-sets} \end{pmatrix}. \tag{8}$$

Notice that this equivalence is not canonical, as it depends on the choice of a quasi-inverse of the equivalence $F_{\bar{x}_2}$. Now it is not difficult to show that the equivalence in (8) is induced by an isomorphism of topological groups $\pi_1(X, \bar{x}_1) \xrightarrow{\sim} \pi_1(X, \bar{x}_2)$. Hence up to isomorphism the fundamental group of the (connected!) scheme X does not depend on the chosen base point.

As in topology, a more elegant way to express that the fundamental group does not depend on the chosen base point is to work with the fundamental groupoid. See SGA1, Exp. V, sect. 5 or Deligne [4], § 10.

pi1Funct **(10.30)** *Functoriality.* Let $f\colon Y \to X$ be a morphism between connected, locally noetherian schemes. Let $\bar{y}$ be a geometric point of Y, and write $\bar{x} = f(\bar{y})$. Associating to an étale covering $X' \to X$ its pull-back $Y' := (X' \times_X Y) \to Y$ gives a functor $f^*\colon \mathsf{FEt}_X \to \mathsf{FEt}_Y$, and $F_{\bar{x}} = F_{\bar{y}} \circ f^*$. In particular, every automorphism of the functor $F_{\bar{y}}$ induces an automorphism of $F_{\bar{x}}$, and this gives a canonical homomorphism

$$f_*\colon \pi_1(Y, \bar{y}) \to \pi_1(X, \bar{x})\,.$$

If $g\colon Z \to Y$ is a second morphism then $(f\circ g)_* = f_*\circ g_*$.

If $f\colon Y \to X$ is an étale covering (still with X and Y connected and locally noetherian), one shows that f_* gives an isomorphism

$$\pi_1(Y,\bar y) \xrightarrow{\sim} \mathrm{Stab}(\bar y) \subset \pi_1(X,\bar x)\,,$$

where $\mathrm{Stab}(\bar y)$ is the stabilizer of the point $\bar y \in f^{-1}(\bar x)$ under the natural action of $\pi_1(X,\bar x)$ on $f^{-1}(\bar x)$. Indeed, if $g\colon Z \to Y$ is an étale covering of Y, then $f\circ g$ is an étale covering of X and $g^{-1}(\bar y) \subset (f\circ g)^{-1}(\bar x)$. If $\sigma \in \mathrm{Stab}(\bar y) \subset \pi_1(X,\bar x)$ then its natural action on $(f\circ g)^{-1}(\bar x)$ preserves the subset $g^{-1}(\bar y)$; hence σ induces an automorphism of the functor $F_{\bar y}$. This gives a homomorphism $\mathrm{Stab}(\bar y) \to \pi_1(Y,\bar y)$ inverse to f_*.

Conversely, if $H \subset \pi := \pi_1(X,\bar x)$ is an open subgroup (equivalently, a subgroup of finite index) then π/H is a finite set with a natural action of π by left multiplication, so by Thm. (10.28) there exists an étale covering $f_H\colon Y_H \to X$ such that we have an isomorphism $\gamma\colon f_H^{-1}(\bar x) \xrightarrow{\sim} \pi/H$ as π-sets. Since the π-action on π/H is transitive, Y_H is connected. If we let $\bar y \in f_H^{-1}(\bar x)$ be the geometric point with $\gamma(\bar y) = (1 \bmod H)$ then $\mathrm{Stab}(\bar y) = H$ as subgroups of π, and the pair $(Y,\bar y)$ is uniquely determined up to isomorphism over X. In this way we obtain a bijective correspondence between pairs $(Y,\bar y)$ up to X-isomorphism (with connected Y) and open subgroups of $\pi_1(X,\bar x)$. As a variant, we may forget the choice of a geometric point $\bar y$ above $\bar x$; then we get a bijective correspondence between connected étale coverings $Y \to X$ up to isomorphism over X and conjugacy classes of open subgroups of $\pi_1(X,\bar x)$.

pi1GeomAr **(10.31)** *Geometric and arithmetic fundamental group.* Let X be a geometrically connected scheme of finite type over a field k. Let k_s be a separable closure of k and write $\bar X := X \times_k k_s$. Choose a geometric point $\bar x$ of $\bar X$, and write $\bar x'$ for its image in X. Then there is an exact sequence

TateBT:pi1seq
$$1 \longrightarrow \pi_1(\bar X,\bar x) \xrightarrow{p_*} \pi_1(X,\bar x') \xrightarrow{s_*} \mathrm{Gal}(k_s/k) \longrightarrow 1\,, \tag{9}$$

where the homomorphisms are induced by the projection $p\colon \bar X \to X$ and the structural morphism $s\colon X \to \mathrm{Spec}(k)$, and where we use the isomorphism of (10.27). If $\bar x\colon \mathrm{Spec}(\Omega) \to X$ factors through a k-rational point $x\colon \mathrm{Spec}(k) \to X$ then $x_*\colon \mathrm{Gal}(k_s/k) \to \pi_1(X,\bar x)$ is a section of s_*.

The group $\pi_1(\bar X,\bar x)$ is referred to as the *geometric fundamental group* of X. The "full" fundamental group $\pi_1(X,\bar x)$ is occasionally called the *arithmetic fundamental group*. If $\mathrm{char}(k) = 0$ or if X is proper over k then $\pi_1(\bar X,\bar x)$ does not change under extension of scalars to a bigger separably closed field. More precisely, if L is a separably closed field containing k_s such that $\bar x$ lifts to a geometric point $\tilde x$ of $X\times_k L$, then the natural map $\gamma\colon \pi_1^{\mathrm{alg}}(X\times_k L,\tilde x) \to \pi_1^{\mathrm{alg}}(X\times_k k_s,\bar x)$ is an isomorphism. Note however that for $\mathrm{char}(k) > 0$ and X not proper, γ need not be an isomorphism; see SGA1, Exp. X, Sect. 1.

Writing $\mathrm{Out}(\pi) := \mathrm{Aut}(\pi)/\mathrm{Inn}(\pi)$ for the group of *outer automorphisms* of a group π, the exact sequence (9) gives rise to a homomorphism

$$\mathrm{Gal}(k_s/k) \to \mathrm{Out}\big(\pi_1(\bar X,\bar x)\big)\,.$$

In the special case that $\bar x$ factors through $x\colon \mathrm{Spec}(k) \to X$, this naturally lifts (via the section x_*) to a homomorphism

$$\mathrm{Gal}(k_s/k) \to \mathrm{Aut}\big(\pi_1(\bar X,\bar x)\big)\,.$$

pi1CompTop **(10.32)** *Comparison with the topological fundamental group.* Let X be a variety over $\mathbb{C}$. Choose a base point $x \in X(\mathbb{C})$. Let us write $\pi_1^{\mathrm{top}}(X,x)$ for the usual fundamental group

of $X(\mathbb{C})$ with its analytic topology. If $Y \to X$ is an étale covering then the induced map on points $Y(\mathbb{C}) \to X(\mathbb{C})$ is a finite topological covering (taking the analytic topology on both sides). Since $\pi_1^{\mathrm{top}}(X,x)$ naturally acts on the fibre of $Y(\mathbb{C})$ over x, we obtain a homomorphism $\pi_1^{\mathrm{top}}(X,x) \to \pi_1(X,x)$. It can be shown that this map induces an isomorphism

$$\left[\pi_1^{\mathrm{top}}(X,x)\right]^{\wedge} \xrightarrow{\sim} \pi_1^{\mathrm{alg}}(X,x)\,,$$

where the left hand side denotes the pro-finite completion of π_1^{top}, that is, the projective limit of all its finite quotients. The geometric content of this statement is that every finite topological covering of X can be realised as an algebraic variety which is finite étale over X, and this algebraic structure is unique up to isomorphism over X.

Note that $\pi_1^{\mathrm{top}}(X,x)$ may not be residually finite, i.e., it may happen that the natural homomorphism $\pi_1^{\mathrm{top}} \to [\pi_1^{\mathrm{top}}]^{\wedge}$ is not injective. (For examples, see Toledo [1].) Geometrically this means that the natural map from the universal covering $\tilde{X}$ of X (in the context of topological spaces) to the "algebraic universal covering" $\tilde{X}^{\mathrm{alg}}$, obtained as the projective limit of all finite étale coverings of X, is not injective.

GalCovs **(10.33)** *Galois coverings.* As before, let X be a connected, locally noetherian scheme. Fix a geometric base point $\bar{x} \in X(\Omega)$. If we claim that the theory of the fundamental group can be viewed as an abstract Galois theory, one may expect that certain étale coverings $Y \to X$ play the role of Galois extensions.

Consider an étale covering $f\colon Y \to X$ with Y connected. Choose a base point $\bar{y} \in Y(\Omega)$ above $\bar{x}$. For simplicity of notation, write $\pi := \pi_1(X,\bar{x})$, and let $H \subset \pi$ be the stabilizer of $\bar{y}$. As discussed in (10.30), we have an isomorphism $f_*\colon \pi_1(Y,\bar{y}) \xrightarrow{\sim} H$, and we get an identification $\pi/H \xrightarrow{\sim} F_{\bar{x}}(Y)$ of finite sets with π-action. Write $N := N_\pi(H) \subset G$ for the normaliser of H.

Let $G := \mathrm{Aut}(Y/X)$ be the group of automorphisms of Y over X. Note that Y is affine over X (as $Y \to X$ is finite), so any G-equivalence class in $|Y|$ is contained in an affine subset, and there exists a quotient of Y by G.

By Theorem (10.28), G maps isomorphically to the automorphism group of $F_{\bar{x}}(Y)$ as a π-set. Using the above description we readily find that the latter group is isomorphic to $(N/H)^{\mathrm{opp}}$, the opposite group of N/H. Indeed, if $a \in N/H$ then $\varphi_a\colon \pi/H \to \pi/H$ given by $gH \mapsto gaH$ is a well-defined automorphism of π-sets, any automorphism is of this form, and $\varphi_b \circ \varphi_a = \varphi_{ab}$.

We conclude that G is finite and that its natural action on $F_{\bar{x}}(Y)$ is faithful. As this holds for any choice of the base point $\bar{x}$, it follows that G acts freely on Y. Hence the morphism $Y \to X$ factors as a composition of two étale coverings $Y \to (G\backslash Y) \to X$. From the given description of G we then see that the following conditions are equivalent:

(i) the group G acts transitively on $F_{\bar{x}}(Y)$;
(ii) the group G acts simply transitively on $F_{\bar{x}}(Y)$;
(iii) the natural map $\bar{f}\colon G\backslash Y \to X$ is an isomorphism, i.e., X is the quotient of Y under G;
(iv) the subgroup $H = f_*\pi_1(Y,\bar{y}) \subset \pi_1(X,\bar{x})$ is normal.

If these conditions are satisfied we say that $f\colon Y \to X$ is a *Galois covering* with group G, and we have an exact sequence of groups

$$1 \longrightarrow \pi_1(Y,\bar{y}) \longrightarrow \pi_1(X,\bar{x}) \longrightarrow \mathrm{Aut}(Y/X)^{\mathrm{opp}} \longrightarrow 1\,.$$

(Caution: we here only consider étale coverings. The terminology "Galois covering" is also used in the context of ramified coverings.)

Using condition (ii), it readily follows from Theorem (10.28) that every étale covering $Z \to X$ with connected Z is dominated by a Galois covering.

Suppose we have étale coverings $g\colon Z \to Y$ and $f\colon Y \to X$, where all three schemes are connected and locally noetherian. Suppose $h := f \circ g\colon Z \to X$ is a Galois covering. Then g is a Galois covering, too. Further, f is Galois if and only if $\mathrm{Aut}(Z/Y) \subset \mathrm{Aut}(Z/X)$ is a normal subgroup, and if this holds then we have a short exact sequence

$$1 \longrightarrow \mathrm{Aut}(Z/Y) \longrightarrow \mathrm{Aut}(Z/X) \longrightarrow \mathrm{Aut}(Y/X) \longrightarrow 1\,.$$

§4. *The fundamental group of an abelian variety.*

We now specialize to the case of an abelian variety. The key result of this paragraph is a theorem of Lang and Serre which says that, for an abelian variety X, the finite étale coverings $f\colon Y \to X$ with a rational point $e_Y \in f^{-1}(e_X)$ are precisely the separable isogenies with target X.

MAVApp4 **(10.34) Proposition.** *Let X be a complete variety over a field k. Suppose given a point $e \in X(k)$ and a k-morphism $m\colon X \times X \to X$ such that $m(x,e) = x = m(e,x)$ for all $x \in X$. Then X is an abelian variety with group law m and origin e.*

Proof. Let $g := \dim(X)$, and write $x \cdot y$ for $m(x,y)$. Consider the morphism $\tau\colon X \times X \to X \times X$ given by $\tau(x,y) = \big(x \cdot y, y\big)$. (If the proposition is true then τ is the universal right translation.) We have $\tau^{-1}(e,e) = \{(e,e)\}$, so the image of τ has dimension $2g$. (We use a standard result on the dimension of the fibres of a morphism; see HAG, Chap. II, Exercise 3.22.) As $X \times X$ is complete and irreducible, it follows that τ is surjective.

We reduce the problem to the case that k is algebraically closed. Namely, suppose m induces a group structure on $X(\overline{k})$, with origin e. Then for every $x \in X(\overline{k})$ the translation $\tau_x\colon y \mapsto x \cdot y$ is an automorphism of $X_{\overline{k}}$ as a variety, and by the argument of Prop. (1.5) it follows that X is non-singular. It also follows that τ induces a bijection on $\overline{k}$-valued points. Hence τ gives a purely inseparable extension on function fields. On the other hand, by looking at the restrictions of τ to $\{e\} \times X$ and $X \times \{e\}$ we see that the tangent map of τ at (e,e) is an isomorphism. The conclusion is that τ is an isomorphism. Now define $i\colon X \to X$ by $i(y) = p_1\big(\tau^{-1}(e,y)\big)$. Using that X is geometrically reduced and that we know the group axioms to hold on $X(\overline{k})$, it follows that m, i and e define the structure of an abelian variety on X. Hence to complete the proof of the proposition, we may assume that $k = \overline{k}$ and it suffices to prove that m gives a group structure on $X(k)$.

Consider the closed subscheme $\Gamma \subset X \times X$ given by $\Gamma := \big\{(x,y) \;\big|\; x \cdot y = e\big\}$. Then $\Gamma = \tau^{-1}\big(\{e\} \times X\big)$, so the surjectivity of τ implies that the second projection $p_2\colon \Gamma \to X$ is surjective. Let $\Gamma_1 \subset \Gamma$ be an irreducible component with $p_2(\Gamma_1) = X$. Notice that Γ_1 is complete, and that $\dim(\Gamma_1) \geqslant g$. Further note that $p_1^{-1}(e) \cap \Gamma = \big\{(e,e)\big\} = p_2^{-1}(e) \cap \Gamma$; this implies that $(e,e) \in \Gamma_1$. Again by comparing dimensions it follows that $p_1\colon \Gamma_1 \to X$ is surjective, too.

Define $f\colon \Gamma_1 \times X \times X \to X$ by $f\big((x,y),z,w\big) = x \cdot \big((y \cdot z) \cdot w\big)$. We have $f\big(\Gamma_1 \times \{e\} \times \{e\}\big) = \{e\}$. Applying the rigidity lemma we find

TateBT:xyzw $$x \cdot \big((y \cdot z) \cdot w\big) = z \cdot w \qquad \text{for all } (x,y) \in \Gamma_1 \text{ and } z,\, w \in X. \tag{10}$$

As a particular case, taking $w = e$, we have

TateBT:xyz=z
$$x \cdot (y \cdot z) = z \qquad \text{for all } (x, y) \in \Gamma_1 \text{ and } z \in X. \tag{11}$$

Now fix $y \in X(k)$. Choose any $x \in X(k)$ with $(x, y) \in \Gamma_1$, and any $z \in X(k)$ with $(y, z) \in \Gamma_1$. (Such x and z exist, as we have shown the two projections $p_i\colon \Gamma_1 \to X$ to be surjective.) Then (11) gives $x = x \cdot (y \cdot z) = z \cdot e = z$. The conclusion is that y has a unique left and right inverse in $X(k)$. Finally, multiplying (10) from the left by $y = x^{-1}$, and using (11) gives

$$y \cdot (z \cdot w) = y \cdot \big(x \cdot \big((y \cdot z) \cdot w\big)\big) = (y \cdot z) \cdot w\,,$$

which shows that the group law on $X(k)$ is associative. □

LSLem **(10.35) Lemma.** *Let Z be a k-variety, let Y be an integral k-scheme of finite type, and let $f\colon Y \to Z$ be a smooth proper morphism of k-schemes. If there exists a section $s\colon Z \to Y$ of f then all fibres of f are irreducible.*

Proof. As the fibres of f are non-singular, it suffices to show that they are connected. Write $Z' := \mathrm{Spec}(f_* O_Y)$, and consider the Stein factorization

$$f = g \circ f'\colon Y \xrightarrow{f'} Z' \xrightarrow{g} Z\,.$$

By Zariski's connectedness theorem (EGA III, Thm. 4.3.1) the morphism f' has connected fibres. The composition $f' \circ s$ is a proper section of g, hence it induces an isomorphism of Z with a closed subscheme of Z'. As g is finite and Z' is integral, it follows that g is an isomorphism. □

LangSer **(10.36) Theorem.** (Lang-Serre) *Let X be an abelian variety over a field k. Let Y be a k-variety and $e_Y \in Y(k)$. If $f\colon Y \to X$ is an étale covering with $f(e_Y) = e_X$ then Y has the structure of an abelian variety such that f is a separable isogeny.*

Proof. With Proposition (10.34) at our disposal, the main point of the proof is to construct the group law $m_Y\colon Y \times Y \to Y$. Let $\Gamma_X \subset X \times X \times X$ be the graph of the multiplication on X, and write $\Gamma'_Y \subset Y \times Y \times Y$ for the pull-back of Γ_X via $f \times f \times f$. Let $\Gamma_Y \subset \Gamma'_Y$ be the connected component containing the point (e_Y, e_Y, e_Y), and if $I \subseteq \{1, 2, 3\}$ write q_I for the restriction of the projection $p_I\colon Y^3 \to Y^I$ to Γ_Y. We want to show that the projection $q_{12}\colon \Gamma_Y \to Y \times Y$ is an isomorphism—if this is true then we can define the desired group law by taking $m_Y := q_3 \circ q_{12}^{-1}\colon Y \times Y \to Y$. Note that q_{12} has a section s_1 over $\{e_Y\} \times Y$ and a section s_2 over $Y \times \{e_Y\}$, given on points by $s_1(e_Y, y) = (e_Y, y, y)$ and $s_2(y, e_Y) = (y, e_Y, y)$. This readily implies that the proposed group law m_Y satisfies the conditions of (10.34).

By construction we have a commutative diagram

$$\begin{array}{ccc} \Gamma_Y & \longrightarrow & \Gamma_X \\ {\scriptstyle q_{12}}\big\downarrow & & \big\downarrow{\scriptstyle p_{12}} \\ Y \times Y & \xrightarrow{f \times f} & X \times X \end{array}\,,$$

in which both the upper arrow $\Gamma_Y \to \Gamma_X$ and the morphism $f \times f$ are étale coverings, and the right hand arrow $p_{12}\colon \Gamma_X \to X \times X$ is an isomorphism. Hence $q_{12}\colon \Gamma_Y \to Y \times Y$ is an étale covering, too.

The projection $q_2\colon \Gamma_Y \to Y$ is a smooth proper morphism, being the composition of q_{12} and $p_2\colon Y \times Y \to Y$. As s_1 gives a section of q_2 we conclude from the above lemma that all fibres of q_2 are irreducible. In particular, $Z := q_2^{-1}(e_Y) = q_{12}^{-1}\big(Y \times \{e_Y\}\big)$ is irreducible. Further, q_{12} restricts to an étale covering $r\colon Z \to Y = Y \times \{e_Y\}$ of the same degree. But s_2 gives a section of r. Hence r is an isomorphism. It follows that the étale covering q_{12} has degree 1 and is therefore an isomorphism. □

LangSerCor **(10.37) Corollary.** *Let X be an abelian variety over a field k. Let Ω be an algebraically closed field containing k, and regard $0 = e_X$ as an Ω-valued point of X. Write k_s for the separable closure of k inside Ω. Then there are canonical isomorphisms*

$$\pi_1^{\mathrm{alg}}(X_{k_s}, 0) \cong \varprojlim_n X[n](k_s) \cong \begin{cases} \prod_\ell T_\ell X & \text{if } \mathrm{char}(k) = 0, \\ T_{p,\text{ét}} X \times \prod_{\ell \neq p} T_\ell X & \text{if } \mathrm{char}(k) = p > 0, \end{cases}$$

where the projective limit runs over all maps $X[nm](k_s) \to X[n](k_s)$ given by $P \mapsto m \cdot P$, and where ℓ runs over the prime numbers. In particular, $\pi_1^{\mathrm{alg}}(X_{k_s}, 0)$ is abelian. Further there is a canonical isomorphism

$$\pi_1^{\mathrm{alg}}(X, 0) \cong \pi_1^{\mathrm{alg}}(X_{k_s}, 0) \rtimes \mathrm{Gal}(k_s/k)\,,$$

where $\mathrm{Gal}(k_s/k)$ acts on $\pi_1^{\mathrm{alg}}(X_{k_s}, 0)$ through its natural action on the groups $X[n](k_s)$.

Proof. For the proof of the first assertion we may assume that $k = k_s$. Write $\pi := \pi_1^{\mathrm{alg}}(X_{k_s}, 0)$. We have $\pi = \varprojlim (\pi/H)$ where H runs over the open subgroups of π. By (10.30), each H corresponds to an étale covering $f_H\colon Y_H \to X$ together with the choice of a point $e_H \in Y_H(\Omega)$ above 0, the pair (Y_H, e_H) being unique up to isomorphism over X. By the Lang-Serre theorem, we have the structure of an abelian variety on Y_H with origin e_H such that f_H is a separable isogeny. Further, it is clear that a separable isogeny $f\colon Y \to X$ is a Galois covering (in the sense of (10.33)) with group $\mathrm{Ker}(f)\big(k\big)$. (Recall that we assume $k = k_s$.) By what was explained in (10.33) we find that $\pi/H \cong \mathrm{Ker}(f_H)\big(k\big)^{\mathrm{opp}} = \mathrm{Ker}(f_H)\big(k\big)$, for any open subgroup $H \subset \pi$.

Let $\mathscr{I}$ be the set of isomorphism classes of separable isogenies $f\colon Y \to X$, where we call $f\colon Y \to X$ and $f'\colon Y' \to X$ isomorphic if there is an isomorphism of abelian varieties $\alpha\colon Y \xrightarrow{\sim} Y'$ with $f' \circ \alpha = f$. We partially order $\mathscr{I}$ by dominance; so $f \geqslant f'$ if there is a homomorphism of abelian varieties $\alpha\colon Y \to Y'$ with $f' \circ \alpha = f$. If $f \geqslant f'$ then we get a homomorphism $\mathrm{Ker}(f) \twoheadrightarrow \mathrm{Ker}(f')$, independent of the choice of α. In this way we have a projective system of finite groups $\big\{\mathrm{Ker}(f)\big(k\big)\big\}_{f \in \mathscr{I}}$, and the conclusion of the above discussion is that

$$\pi \xrightarrow{\sim} \varprojlim_{f \in \mathscr{I}} \mathrm{Ker}(f)\big(k\big) \tag{12}$$

TateBT:piKerf

as pro-finite groups.

If n is a positive integer then $[n] = [n]_X$ factors as $X \xrightarrow{f} X/X[n]_{\mathrm{loc}} \xrightarrow{g} X$ where f is purely inseparable and g is separable. Of course, if $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p > 0$ and $p \nmid n$ then f is the identity and $g = [n]$. For the purpose of this discussion, write $g = [n]_{\mathrm{sep}}$. The Galois group of $[n]_{\mathrm{sep}}$ is $X[n]\big(k\big)$. Let $\mathscr{I}' \subset \mathscr{I}$ be the subset of all isogenies $[n]_{\mathrm{sep}}$ for $n \in \mathbb{Z}_{\geqslant 1}$. Then $\mathscr{I}'$ is cofinal in $\mathscr{I}$; indeed, if $f\colon Y \to X$ is any separable isogeny, say of degree d, then by Prop. (5.12) there is an isogeny $g\colon X \to Y$ with $[d]_X = f \circ g$, and then it follows from Cor. (5.8) that $[d]_{\mathrm{sep}}$ dominates f. Hence we may restrict the limit in (12) to the terms $f \in \mathscr{I}'$; this gives the desired isomorphism

$$\pi \xrightarrow{\sim} \varprojlim_{f \in \mathscr{I}'} \mathrm{Ker}(f)\big(k\big) = \varprojlim_n X[n]\big(k\big)\,,$$

where n runs over the set $\mathbb{Z}_{\geqslant 1}$, partially ordered by divisibility.

The last assertion of the theorem (now again over an arbitrary ground field) follows by using what was explained in (10.31), noting that $0 \in X(\Omega)$ factors through a k-rational point. □

HetXGen **(10.38)** As an application of this theorem, let us now discuss how the ℓ-adic cohomology of an abelian variety can be described in terms of its Tate-ℓ-module.

First let X be any complete variety over a field k, say with $\dim(X) = g$. Let k_s be a separable closure of k, and let ℓ be a prime number different from $\mathrm{char}(k)$. The ℓ-adic cohomology $H^\bullet(X_{k_s}, \mathbb{Z}_\ell) = \oplus_{i=0}^{2g} H^i(X_{k_s}, \mathbb{Z}_\ell)$ is a graded-commutative $\mathbb{Z}_\ell$-algebra of finite type that comes equipped with a continuous action of $\mathrm{Gal}(k_s/k)$. If $\bar{x} \in X(k_s)$ then the first ℓ-adic cohomology and the fundamental group of X_{k_s} are related by

TateBT:H1pi1
$$H^1(X_{k_s}, \mathbb{Z}_\ell) \cong \mathrm{Hom}_{\mathrm{cont}}\big(\pi_1(X_{k_s}, \bar{x}), \mathbb{Z}_\ell\big)\,, \tag{13}$$

where the right hand side is the group of continuous homomorphisms $\pi_1(X_{k_s}, \bar{x}) \to \mathbb{Z}_\ell$. The homomorphism $\mathrm{Gal}(k_s/k) \to \mathrm{Out}\big(\pi_1(X_{k_s}, \bar{x})\big)$ of (10.31) induces a homomorphism $\mathrm{Gal}(k_s/k) \to \mathrm{Aut}\big(\pi_1(X_{k_s}, \bar{x})^{\mathrm{ab}}\big)$, and this gives a continuous Galois action on $\mathrm{Hom}_{\mathrm{cont}}\big(\pi_1(X_{k_s}, \bar{x}), \mathbb{Z}_\ell\big) = \mathrm{Hom}_{\mathrm{cont}}\big(\pi_1(X_{k_s}, \bar{x})^{\mathrm{ab}}, \mathbb{Z}_\ell\big)$. The isomorphism (13) is equivariant for the Galois actions on the two sides.

Now we specialize this to the case where X is an abelian variety. As we shall prove later, $H^\bullet(X_{k_s}, \mathbb{Z}_\ell)$ is then the exterior algebra on $H^1(X_{k_s}, \mathbb{Z}_\ell)$; see Cor. (13.32). Admitting this, we find the following result.

HetXCor **(10.39) Corollary.** *Let X be an abelian variety over a field k, let $k \subset k_s$ be a separable algebraic closure, and let ℓ be a prime number with $\ell \neq \mathrm{char}(k)$. Then we have*

$$H^1(X_{k_s}, \mathbb{Z}_\ell) \cong (T_\ell X)^\vee := \mathrm{Hom}(T_\ell X, \mathbb{Z}_\ell)$$

as $\mathbb{Z}_\ell$-modules with continuous action of $\mathrm{Gal}(k_s/k)$. Further we have an isomorphism of graded-commutative $\mathbb{Z}_\ell$-algebras with continuous $\mathrm{Gal}(k_s/k)$-action

$$H^\bullet(X_{k_s}, \mathbb{Z}_\ell) \cong \wedge^\bullet \left[(T_\ell X)^\vee\right].$$

Exercises.

Ex:BTSplit **(10.1)** Let G be a p-divisible group over a perfect field k. Show that for every n the square

$$\begin{array}{ccc} G_{n,\mathrm{red}} & \longrightarrow & G_{n+1,\mathrm{red}} \\ \big\downarrow & & \big\downarrow \\ G_n & \xrightarrow{i_n} & G_{n+1} \end{array}$$

is Cartesian. Conclude that the exact sequence (7) splits.

Ex:WeilResEtGS **(10.2)** Let K be a field, $K \subset K_s$ a separable algebraic closure. Let $K \subset L$ be a finite extension inside K_s.

(i) Let H be a finite étale group scheme over L, and consider $G := \mathrm{Res}_{L/K}(H)$, the K-group scheme obtained by Weil restriction of scalars from L to K. By definition of the Weil restriction, G represents the functor $\mathsf{Sch}_{/K}^{\mathrm{opp}} \to \mathsf{Gr}$ given by $T \mapsto H(T_L)$. Show that G is again a finite étale group scheme.

(ii) Assume (for simplicity) that H is commutative. Write $\Gamma_L := \mathrm{Gal}(K_s/L) \subset \Gamma_K := \mathrm{Gal}(K_s/K)$. Show that $G(K_s) \cong \mathrm{Ind}_{\Gamma_L}^{\Gamma_K} H(K_s)$ as representations of $\mathrm{Gal}(K_s/K)$.

(iii) Let X be an abelian variety over L, and write $Y := \mathrm{Res}_{L/K}(X)$, which is an abelian variety over K of dimension $\dim(X) \cdot [L : K]$. If ℓ is a prime number different from $\mathrm{char}(K)$, show that $T_\ell(Y) \cong \mathrm{Ind}_{\Gamma_L}^{\Gamma_K} T_\ell(X)$ as $\mathbb{Z}_\ell\big[\mathrm{Gal}(K_s/K)\big]$-modules.

In the study of higher dimensional varieties and their moduli, one often considers polarized varieties. Here a polarization is usually defined as the class of an ample line bundle modulo a suitable equivalence relation, such as algebraic or homological equivalence. If X is an abelian variety then, as we have seen in (7.24), the class of an ample bundle L modulo algebraic equivalence carries the same information as the associated homomorphism $\lambda = \varphi_L\colon X \to X^t$. And it is in fact this homomorphism that we shall put in the foreground. One reason for this is that λ usually has somewhat better arithmetic properties; for instance, it may be defined over a smaller field than any line bundle representing it. The positivity of an ample bundle shall later be translated into the positivity of the Rosati involution associated to λ; this is an important result that shall be given in the next chapter.

The first Chern class of L only depends on L modulo algebraic equivalence, and we therefore expect that it can be expressed directly in terms of the associated homomorphism $\lambda = \varphi_L$. This is indeed the case. As we have seen before (cf. ??), the ℓ-adic cohomology of X can be described in more elementary terms via the Tate-ℓ-module. The class $c_1(L)$ then takes the form of an alternating pairing $E_\ell^\lambda\colon T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1)$, usually referred to as the Riemann form of L (or of λ). It is obtained, by a limit procedure, from pairings $e_n^\lambda\colon X[n] \times X[n] \to \mu_n$, called the Weil pairing.

§1. *Polarizations.*

Idlambda*P **(11.1) Proposition.** *Let X be an abelian variety. Let $\lambda\colon X \to X^t$ be a homomorphism, and consider the line bundle $M := (\mathrm{id}, \lambda)^*\mathscr{P}_X$ on X. Then $\varphi_M = \lambda + \lambda^t$. In particular, if λ is symmetric then $\varphi_M = 2\lambda$.*

Proof. Immediate from Proposition (7.6) together with Exercise (7.5). □

lambdasymm **(11.2) Proposition.** *Let X be an abelian variety over a field k. Let $\lambda\colon X \to X^t$ be a homomorphism. Then the following properties are equivalent:*

(a) *λ is symmetric;*
(b) *there exists a field extension $k \subset K$ and a line bundle L on X_K such that $\lambda_K = \varphi_L$;*
(c) *there exists a finite separable field extension $k \subset K$ and a line bundle L on X_K such that $\lambda_K = \varphi_L$.*

Proof. Assume (a) holds. Let $M := (\mathrm{id}, \lambda)^*\mathscr{P}_X$ and $N := M^2$. By the previous proposition we know that $\varphi_M = 2\lambda$, so $\varphi_N = 4\lambda$. In particular, $X[4] \subset K(N) = \mathrm{Ker}(\varphi_N)$. We claim that $X[2] \subset X[4]$ is totally isotropic with respect to the commutator pairing e^N. Indeed, if x, $x' \in X[2]\big(T\big)$ for some k-scheme T then possibly after passing to an fppf covering of T we can write $x = 2y$ and $x' = 2y'$ for some y, $y' \in X[4]\big(T\big)$. Our claim now follows by noting that the restriction of e^N to $X[4] \times X[4]$ takes values in μ_4. By Corollary (8.11) we can find a line bundle L on $X_{\overline{k}}$ such that $N \cong [2]^*L$ on $X_{\overline{k}}$. But then $4\lambda_{\overline{k}} = \varphi_{[2]^*L} = 4\varphi_L$, using Corollary (7.25). As $[4]_X$ is an epimorphism, it follows that $\lambda_{\overline{k}} = \varphi_L$. So (b) holds with $K = \overline{k}$.

To see that the apparently stronger condition (c) holds, view λ as a k-valued point of $Hom_{\mathsf{AV}}(X, X^t)$. Let $P(\lambda) \subset \mathrm{Pic}_{X/k}$ be the inverse image of λ under the homomorphism $\varphi\colon \mathrm{Pic}_{X/k} \to Hom_{\mathsf{AV}}(X, X^t)$. As $P(\lambda)$ is a closed subscheme of $\mathrm{Pic}_{X/k}$, it is locally of finite type. If T is a k-scheme then the T-valued points of $P(\lambda)$ are the classes of line bundles M on X_T such that $\varphi_M = \lambda$. Note that $P(\lambda)$ inherits a natural action of $X^t = \mathrm{Pic}^0_{X/k}$ by translations. The exact sequence of (7.22) tells us that for every k-scheme T the set $P(\lambda)(T)$ is either empty or it is a principal homogeneous space under $X^t(T)$. Hence if L is a line bundle on $X_{\overline{k}}$ with $\varphi_L = \lambda_{\overline{k}}$ then $x \mapsto [t_x^* L]$ defines an isomorphism of $\overline{k}$-schemes $(X^t)_{\overline{k}} \xrightarrow{\sim} P(\lambda)_{\overline{k}}$. In particular, $P(\lambda)$ is a geometrically integral k-scheme, so it has points with values in some finite separable extension $k \subset K$.

Finally, it is clear that (c) implies both (a) and (b). □

NSSymHomCor **(11.3) Corollary.** *Let X/k be an abelian variety. Then the homomorphism $\psi\colon \mathrm{NS}_{X/k} \to Hom^{\mathrm{sym}}(X, X^t)$ of (7.26) is an isomorphism.*

Proof. Both group schemes are étale and we already know that ψ is injective. Hence it suffices to show that ψ is surjective on k_s-valued points, and this follows from the preceding Proposition. □

PolPrepare **(11.4) Proposition.** *Let X/k be an abelian variety. Let $\lambda\colon X \to X^t$ be a symmetric homomorphism, and write $M := (\mathrm{id}, \lambda)^* \mathscr{P}_X$. Let $k \subset K$ be a field extension and let L be a line bundle on X_K with $\lambda_K = \varphi_L$.*

(i) *We have: λ is an isogeny $\Leftrightarrow$ L is non-degenerate $\Leftrightarrow$ M is non-degenerate.*

(ii) *If λ is an isogeny then L is effective if and only if M is effective.*

(iii) *We have: L is ample $\Leftrightarrow$ M is ample.*

Proof. By Proposition (11.1) $\varphi_{M_K} = 2\varphi_L = \varphi_{L^2}$, so M_K and L^2 are algebraically equivalent. Now (i) is clear, and (ii) follows from Corollary (9.23) and part (ii) of Proposition (9.18). For (iii), recall that a line bundle N on X is ample if and only if N is non-degenerate and effective; this is just Proposition (2.22). □

Putting Propositions (2.22), (11.2) and (11.4) together we obtain the following corollary.

PolConditions **(11.5) Corollary.** *Let X/k be an abelian variety. Let $\lambda\colon X \to X^t$ be a homomorphism. Then the following properties are equivalent:*

(a1) *λ is a symmetric isogeny and the line bundle $(\mathrm{id}, \lambda)^* \mathscr{P}$ on X is ample;*

(a2) *λ is a symmetric isogeny and the line bundle $(\mathrm{id}, \lambda)^* \mathscr{P}$ on X is effective;*

(b1) *there exists a field extension $k \subset K$ and an ample line bundle L on X_K such that $\lambda_K = \varphi_L$;*

(b2) *there exists a finite separable field extension $k \subset K$ and an ample line bundle L on X_K such that $\lambda_K = \varphi_L$.*

PolDef **(11.6) Definition.** Let X be an abelian variety over a field k. A *polarization* of X is an isogeny $\lambda\colon X \to X^t$ that satisfies the equivalent conditions in (11.5).

By the Riemann-Roch Theorem (9.11) the degree of a polarization is always a square: $\deg(\lambda) = d^2$ with $d = \chi(L)$ if $\lambda_{\overline{k}} = \varphi_L$. If λ is an isomorphism (equivalent: λ has degree 1) then we call it a *principal polarization*.

It is clear that the sum of two polarizations is again a polarization. But of course the polarizations do not form a subgroup of $\mathrm{Hom}_{\mathsf{AV}}(X, X^t)$.

We also remark that if λ is a polarization, then for any line bundle L on X_K with $\lambda_K = \varphi_L$ we have that L is ample. In fact, ampleness of a line bundle N on an abelian variety only depends on the associated homomorphism φ_N, as is clear for instance from Proposition (11.4).

phiLObstr **(11.7)** Let X be an abelian variety over a field k. We have an exact sequence of fppf sheaves

$$0 \longrightarrow X^t \longrightarrow \mathrm{Pic}_{X/k} \longrightarrow \mathit{Hom}^{\mathrm{sym}}(X, X^t) \longrightarrow 0$$

which gives a long exact sequence in fppf cohomology

$$0 \longrightarrow X^t(k) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{Hom}^{\mathrm{sym}}(X, X^t) \xrightarrow{\partial} H^1_{\mathrm{fppf}}(k, X^t) \longrightarrow \cdots \quad .$$

For $\lambda\colon X \to X^t$ a symmetric homomorphism, $\partial(\lambda)$ is the obstruction for finding a line bundle L on X (over k) with $\varphi_L = \lambda$. Now we know from Proposition (11.2) that $\partial(2\lambda) = 0$; hence $\partial(\lambda)$ lies in the image of

$$H^1_{\mathrm{fppf}}\big(k, X^t[2]\big) \to H^1_{\mathrm{fppf}}(k, X^t)\,.$$

(NOG VERDERE OPM OVER MAKEN, BV VGL MET GALOIS COHOM?)

PolPullback **(11.8) Proposition.** *Let $f\colon X \to Y$ be an isogeny. If $\mu\colon Y \to Y^t$ is a polarization of Y, then $f^*\mu := f^t \circ \mu \circ f$ is a polarization of X of degree* $\deg(f^*\mu) = \deg(f)^2 \cdot \deg(\mu)$.

Proof. It is clear that $f^*\mu$ is an isogeny of the given degree. By assumption there is a field extension $k \subset K$ and an ample line bundle M on Y_K such that $\mu_K = \varphi_M$. Then $f^*\mu_K = \varphi_{f^*M}$ and because f is finite f^*M is an ample line bundle on X_K. □

See Exercise (11.1) for a generalization.

CorDef **(11.9) Definition.** Let X and Y be abelian varieties over k. A *(divisorial) correspondence* between X and Y is a line bundle L on $X \times Y$ together with rigidifications $\alpha\colon L_{|\{0\}\times Y} \xrightarrow{\sim} O_Y$ and $\beta\colon L_{|X\times\{0\}} \xrightarrow{\sim} O_X$ that coincide on the fibre over $(0,0)$.

Correspondences between X and Y form a group $\mathrm{Corr}_k(X, Y)$, with group structure obtained by taking tensor products of line bundles. (Cf. the definition of $P_{X/S,\varepsilon}$ in Section (6.2).)

Note that the multiplicative groep $\mathbb{G}_m$ acts (transitively) on the choices of the rigidifications (α, β). Moreover, if $Y = X$ we can speak of symmetric correspondences.

The Poincaré bundle $\mathscr{P} = \mathscr{P}_X$ on $X \times X^t$ comes equipped with a rigidification along $\{0\} \times X^t$. There is a unique rigidification along $X \times \{0\}$ such that the two rigidifications agree at the origin $(0,0)$. We thus obtain an element

$$[\mathscr{P}_X] = (\mathscr{P}_X, \alpha_{\mathscr{P}}, \beta_{\mathscr{P}}) \in \mathrm{Corr}_k(X, X^t)\,.$$

The following proposition makes an alternative definition of the notion of polarization possible.

ternativedefpol **(11.10) Proposition.** *Let X/k be an abelian variety. Then we have a bijection*

$$\{\textit{polarizations } \lambda\colon X \to X^t\} \xrightarrow{\sim} \left\{ \begin{array}{c} \textit{symmetric divisorial correspondences} \\ (L, \alpha, \beta) \textit{ on } X \times X \textit{ such that } \Delta_X^* L \textit{ is ample} \end{array} \right\}$$

by associating to a polarization λ the divisorial correspondence (L, α, β) with $L = (\mathrm{id}_X \times \lambda)^* \mathscr{P}_X$ and α and β the pull-backs under $\mathrm{id}_X \times \lambda$ of the rigidifications $\alpha_{\mathscr{P}}$ and $\beta_{\mathscr{P}}$.

Proof. This is essentially contained in Corollary (11.5). The inverse map is obtained by associating to (L, α, β) the unique homomorphism $\lambda\colon X \to X^t$ such that $(L, \alpha) = (\mathrm{id}_X \times \lambda)^*(\mathscr{P}_X, \alpha_{\mathscr{P}})$ as rigidified line bundles on $X \times X$. The assumption that (L, α, β) is symmetric implies that λ_X is symmetric, and because $(\mathrm{id}_X, \lambda)^* \mathscr{P}_X = \Delta_X^* (\mathrm{id}_X \times \lambda)^* \mathscr{P}_X = \Delta_X^* L$ is ample, λ is a polarization. This establishes the correspondence. □

The alternative definition of a polarization suggested by Proposition (11.10) as "a symmetric self-correspondence such that restriction to the diagonal is ample" is evidently similar in appearance to the definition of a positive definite symmetric bilinear form in linear algebra. But, whereas in linear algebra one dominantly views a bilinear form b as a map $V \times V \to k$ rather than as a map $V \to V^*$ given by $v \mapsto \big(w \mapsto b(v, w)\big)$, in the theory of abelian varieties the latter point of view dominates. Note further that the role of the evaluation map $V \times V^* \to k$ with $(v, w) \mapsto w(v)$ is played in our context by the Poincaré bundle $\mathscr{P}$.

§2. *Pairings.*

We now turn to the study of some bilinear forms attached to isogenies. In its most general form, any isogeny f gives a pairing e_f between $\mathrm{Ker}(f)$ and $\mathrm{Ker}(f^t)$; this is an application of the duality result Theorem (7.5). Of particular interest is the case $f = [n]_X$. If we choose a polarization λ we can map $X[n]$ to $X^t[n]$, and we obtain a bilinear form e_n^λ on $X[n]$, called the Weil pairing. The pairings that we consider satisfy a number of compatibilities, which, for instance, allow us to take the limit of the pairings $e_{\ell^m}^\lambda$, obtaining a bilinear form E^λ with values in $\mathbb{Z}_\ell(1)$ on the Tate module $T_\ell X$. In cohomological terms this pairing is the first Chern class of λ (or rather, of any line bundle representing it). It is the ℓ-adic analogue of what over $\mathbb{C}$ is called the Riemann form associated to a polarization. (See also ???)

WeilpDef **(11.11) Definition.** Let $f\colon X \to Y$ be an isogeny of abelian varieties over a field k. Write $\beta\colon \mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$ for the isomorphism of Theorem (7.5).

(i) Define

$$e_f\colon \mathrm{Ker}(f) \times \mathrm{Ker}(f^t) \longrightarrow \mathbb{G}_{m,k}$$

to be the perfect bilinear pairing given (on points) by $e_f(x, y) = \beta(y)(x)$. Note that if $\mathrm{Ker}(f)$ is killed by $n \in \mathbb{Z}_{\geqslant 1}$ then e_f takes values in $\mu_n \subset \mathbb{G}_m$. In the particular case that $f = n_X\colon X \to X$ we obtain a pairing

$$e_n\colon X[n] \times X^t[n] \to \mu_n$$

which we call the *Weil pairing*.

(ii) Let $\lambda\colon X \to X^t$ be a homomorphism. We write

$$e_n^\lambda\colon X[n] \times X[n] \to \mu_n$$

for the bilinear pairing given by $e_n^\lambda(x_1, x_2) = e_n\big(x_1, \lambda(x_2)\big)$. If $\lambda = \varphi_L$ for some line bundle L then we also write e_n^L instead of e_n^λ.

Recall that if A and B are finite commutative group schemes (written additively), a pairing $e\colon A \times B \to \mathbb{G}_m$ is said to be bilinear if $e(a+a', b) = e(a, b) \cdot e(a', b)$ and $e(a, b+b') = e(a, b) \cdot e(a, b')$ for all points a and a' of A and b and b' of B. (Points with values in an arbitrary k-scheme.) The

pairing e is said to be perfect if sending a to $e(a,-)\colon B \to \mathbb{G}_m$ gives an isomorphism $A \xrightarrow{\sim} B^D$. This is equivalent to the condition that $b \mapsto e(-,b)$ gives an isomorphism $B \xrightarrow{\sim} A^D$. It is clear from the construction that the pairings e_f, in particular also the Weil pairings, are perfect bilinear pairings. If n is relatively prime to the degree of λ then the pairing e_n^λ is perfect, too.

There are various ways in which we can make the pairings defined above more explicit. We shall give a couple of different points of view.

WpExpl1 **(11.12)** Let us first try to unravel the definition of e_f by going back to the proof of (7.5). This leads to the following description. Let T be a k-scheme. Let L be a rigidified line bundle on Y_T that represents a class $\eta \in \mathrm{Ker}(f^t)(T)$. Then $f^*L \cong O_{X_T}$. Hence the geometric line bundle $\mathbb{L}$ corresponding to L can be described as a quotient of $X_T \times_T \mathbb{A}^1_T$ by an action of $\mathrm{Ker}(f)_T$. More precisely, by what was explained in (7.3) there exists a character $\chi\colon \mathrm{Ker}(f)_T \to \mathbb{G}_{m,T}$ such that the action of a point x of $\mathrm{Ker}(f)$ on $X_T \times_T \mathbb{A}^1_T$ is given (on points) by

$$(z,a) \mapsto \big(z+x, \chi(x)\cdot a\big)\,.$$

The isomorphism $\mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$ of Theorem (7.5) sends η to χ. Hence the pairing e_f is given by $e_f(x,\eta) = \chi(x)$.

WpExpl2 **(11.13)** Next let us give a more geometric description of the Weil pairings e_n. Suppose D is a divisor on X such that nD is linearly equivalent to zero. Write $L = O_X(D)$. As $n^*L \cong O_X$ (cf. Exercise (7.2)), there exists a rational function g on X with divisor $(g) = n^*D$. But also $L^n \cong O_X$, so there exists a rational function f with divisor $(f) = nD$. Then n^*f and g^n both have divisor $n\cdot n^*D = n^*(nD)$, so there is a constant $c \in k^*$ with $g^n = c\cdot(n^*f)$.

Let $x \in X[n](k)$ be a k-rational n-torsion point. We find that

$$g(\xi)^n = c\cdot f(n\xi) = c\cdot f\big(n(\xi+x)\big) = g(\xi+x)^n = \big((t_x^*g)(\xi)\big)^n$$

for all $\xi \in X(\overline{k})$. So $g/t_x^*(g)$ is an n-th root of unity. We claim that in fact $e_n\big(x,[D]\big) = g/t_x^*(g)$.

To see this, note that we have an isomorphism of line bundles $n^*L \xrightarrow{\sim} O_X$ given by $g \mapsto 1$. As described in (11.12), there is a character $\chi\colon X[n] \to \mathbb{G}_m$ such that the natural action of $X[n]$ on n^*L becomes the action of $X[n]$ on O_X given by the character χ. Note that $x \in X[n](k)$ acts on the identity section $1 \in \Gamma(X,O_X)$ as multiplication by $\chi(x)^{-1}$. Hence $g/t_x^*(g) = \chi(x) = e_n\big(x,[D]\big)$, as claimed.

WpExaE/F2 **(11.14) Example.** We calculate the Weil pairing e_3 on the elliptic curve E over $\mathbb{F}_2$ given by the affine equation $y^2+y = x^3$. This curve has 9 points over $\mathbb{F}_4$ which realise an isomorphism $E[3]\big(\mathbb{F}_4\big) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $O = P_\infty$ be the point at ∞, which we take as the identity element on E. The bundle $L = O_E(P_\infty)$ is ample. The associated principal polarization $\lambda\colon E \xrightarrow{\sim} E^t = \mathrm{Pic}^0_{E/\mathbb{F}_2}$ is given on points by $R \mapsto O_E(O-R)$. (Note that this is *minus* the map given by $R \mapsto O_E(R-O)$; see Remark (2.11).)

Let us calculate $e_3^\lambda(Q,P)$ for $P = (0,0)$ and $Q = (1,\alpha)$, where α is an element of $\mathbb{F}_4$ not in $\mathbb{F}_2$. First we note that the function y has divisor $(y) = 3\cdot(P-O)$. Next we compute a function g with divisor $[3]^*(O-P)$. For this we compute the "triplication formula" on E which expresses for a point $R = (\xi,\eta)$ on E the coordinates of $3R$ in those of R. As we have seen in Example (5.26), E is supersingular. The relative Frobenius $\pi = F_{E/\mathbb{F}_2}\colon E \to E$ is an endomorphism of E. One can show that it satisfies $\pi^2 = -2$, for example by verifying

that for $T \in E$ the point $\pi^2(T)$ lies on the tangent line to E in T. As -1 on E is given by $(x,y) \mapsto (x, y+1)$ we find that $2R$ has coordinates (ξ^4, η^4+1). Next one calculates that the coordinates of $3R$ are $\big((\xi^9+\xi^3+1)/(\xi+\xi^4)^2, (\eta\xi^3+1)^3/(\xi+\xi^4)^3\big)$. Hence the function

$$g = \frac{x^4+x}{yx^3+1}$$

has divisor $(g) = [3]^*(O-P)$. (Use that $3\cdot(g) = [3]^*(y) = 3\cdot[3]^*(O-P)$.)

Now we know that g/t_Q^*g is constant and this constant can be computed by evaluating g and t_Q^*g at a suitable point T; so

$$g/t_Q^*g = g(T)/g(T+Q)\,.$$

For T we take a point rational over $\mathbb{F}_{64}$. Let γ be a generator of $\mathbb{F}_{64}^*$ with $\gamma^{21} = \alpha$ and such that $\delta := \gamma^9 \in \mathbb{F}_8^*$ satisfies $\delta^3+\delta = 1$. Then the point $T = (\gamma^3, \gamma^{18})$ is in $E(\mathbb{F}_{64})$. One easily verifies that $(\gamma^{24}, \gamma^{18}+1)$ is again a point of E, and that it lies on the line through T and Q; hence $T+Q = (\gamma^{24}, \gamma^{18})$. By (11.13) we conclude that $e_3^\lambda(Q,P) = e_3\big(Q, (O-P)\big)$ equals $(\gamma^{12}+\gamma^3)/(\gamma^{33}+\gamma^{24}) = 1/\gamma^{21} = 1/\alpha = \alpha^2$.

The value of $e_3^\lambda(P',Q')$ for any pair $(P',Q') \in E[3]\times E[3]$ can be computed from this using the fact that e_3 is bilinear and alternating; see Cor. (11.22) below.

KerKerAction **(11.15)** Let $f\colon X \to Y$ be an isogeny of abelian varieties over a field k. By definition, $f^t\colon Y^t \to X^t$ is the unique map such that $(f\times \mathrm{id}_{Y^t})^*\mathscr{P}_Y \cong (\mathrm{id}_X \times f^t)^*\mathscr{P}_X$ as line bundles on $X\times Y^t$ with rigidification along $\{0\}\times Y^t$. Note that this isomorphism is unique, so without ambiguity we can define $\mathscr{Q} := (f\times\mathrm{id}_{Y^t})^*\mathscr{P}_Y = (\mathrm{id}_X\times f^t)^*\mathscr{P}_X$. The diagram to keep in mind is

PolWp:Bundles
$$\begin{array}{ccccc} \mathscr{P}_X & & \mathscr{Q} & & \mathscr{P}_Y \\ X\times X^t & \xleftarrow{\mathrm{id}\times f^t} & X\times Y^t & \xrightarrow{f\times\mathrm{id}} & Y\times Y^t \end{array} \tag{1}$$

On the line bundle $\mathscr{Q}$ we have an action of $\mathrm{Ker}(f)\times\{0\}$, lifting the action on $X\times Y^t$ by translations. This action is given by isomorphisms $\sigma_x\colon \mathscr{Q}_T \xrightarrow{\sim} t_{(x,0)}^*\mathscr{Q}_T$, for any k-scheme T and $x \in \mathrm{Ker}(f)\big(T\big)$. Likewise, we have an action of $\{0\}\times\mathrm{Ker}(f^t)$, given by isomorphisms $\tau_q\colon \mathscr{Q}_T \xrightarrow{\sim} t_{(0,q)}^*\mathscr{Q}_T$ for $q \in \mathrm{Ker}(f^t)\big(T\big)$. Unless f is an isomorphism, these two group scheme actions on $\mathscr{Q}$ do not commute, for if they did it would give us an action of $\mathrm{Ker}(f)\times\mathrm{Ker}(f^t)$ and $\mathscr{Q}$ would descend to a line bundle L on $(X\times Y^t)/\mathrm{Ker}(f)\times\mathrm{Ker}(f^t) = Y\times X^t$. But then we had $(-1)^g = \chi(\mathscr{P}_X) = \deg(f)\cdot\chi(L)$, which is possible only if $\deg(f) = 1$. We shall prove that the extent to which the two actions fail to commute is measured by the pairing e_f.

Let $\mathscr{Q}'$ be the restriction of $\mathscr{Q}$ to $X\times\mathrm{Ker}(f^t)$. We have $\mathscr{Q}' = (\mathrm{id}_X\times f^t)^*\big((\mathscr{P}_X)_{|X\times\{0\}}\big)$, so the natural rigidification of $\mathscr{P}_X$ along $X\times\{0\}$ (see (7.7)) gives us a trivialisation $\mathscr{Q}' \xrightarrow{\sim} O_{X\times\mathrm{Ker}(f^t)}$. The action of $\{0\}\times\mathrm{Ker}(f^t)$ on $\mathscr{Q}$ restricts to the trivial action on $\mathscr{Q}'$. It will be useful to think of $\mathscr{Q}'$ as being the sheaf of sections of $\mathbb{A}^1$ over $X\times\mathrm{Ker}(f^t)$. Writing $\mathbb{A}^1_{X\times\mathrm{Ker}(f^t)} = X\times\mathrm{Ker}(f^t)\times\mathbb{A}^1$, the action of a point $(0,q)\in\{0\}\times\mathrm{Ker}(f^t)$ on $\mathscr{Q}'$ corresponds to the action on $X\times\mathrm{Ker}(f^t)\times\mathbb{A}^1$ given by $\tau_q\colon (t,u,a)\mapsto(t,u+q,a)$.

Note that also the action of $\mathrm{Ker}(f)\times\{0\}$ restricts to an action on $\mathscr{Q}'$. To describe this action we apply what was explained in (11.12) in the "universal case", i.e., with $T = \mathrm{Ker}(f^t)$ and $\eta = \mathrm{id}_T$. The corresponding line bundle L on $Y_T = Y\times\mathrm{Ker}(f^t)$ is just the restriction of $\mathscr{P}_Y$ to $Y\times\mathrm{Ker}(f^t)$, so f^*L is precisely our bundle $\mathscr{Q}'$. If we write a point of $\mathrm{Ker}(f)_T =$

$\mathrm{Ker}(f)\times_k\mathrm{Ker}(f^t)$ as a pair (x,u) then the conclusion of (11.12) is that the character $\chi\colon \mathrm{Ker}(f)\times_k \mathrm{Ker}(f^t) \to \mathbb{G}_{m,k}\times_k \mathrm{Ker}(f^t)$ is given by $(x,u)\mapsto \big(e_f(x,u),u\big)$. Hence the action of a point $(x,0)\in\mathrm{Ker}(f)\times\{0\}$ on $\mathscr{Q}'$ corresponds to the action on $X\times\mathrm{Ker}(f^t)\times\mathbb{A}^1$ given by $\sigma_x\colon (t,u,a)\mapsto \big(t+x,u,e_f(x,u)\cdot a\big)$.

Now we can start drawing some conclusions. The first result is an interpretation of the pairing e_f as a measure for the extent to which the two group scheme actions on $\mathscr{Q}$ fail to commute.

ef2Actions **(11.16) Proposition.** *Let $f\colon X\to Y$ be an isogeny of abelian varieties over a field k, and consider the line bundle $\mathscr{Q} := (f\times \mathrm{id}_{Y^t})^*\mathscr{P}_Y = (\mathrm{id}_X\times f^t)^*\mathscr{P}_X$ on $X\times Y^t$. Let T be a k-scheme, $x\in\mathrm{Ker}(f)\big(T\big)$ and $q\in\mathrm{Ker}(f^t)\big(T\big)$. Let $\sigma_x\colon \mathscr{Q}_T\xrightarrow{\sim} t_{(x,0)}^*\mathscr{Q}_T$ be the isomorphism that gives the action of $(x,0)\in\mathrm{Ker}(f)\times\{0\}$ on $\mathscr{Q}_T$, and let $\tau_q\colon \mathscr{Q}_T\xrightarrow{\sim} t_{(0,q)}^*\mathscr{Q}_T$ be the isomorphism that gives the action of $(0,q)\in\{0\}\times\mathrm{Ker}(f^t)$. Then we have a commutative diagram*

$$\begin{array}{ccccc}
\mathscr{Q}_T & \xrightarrow{\sigma_x} & t_{(x,0)}^*\mathscr{Q}_T & \xrightarrow{t_{(x,0)}^*\tau_q} & t_{(x,q)}^*\mathscr{Q}_T \\
\| & & & & \downarrow{\scriptstyle \text{multiplication by } e_f(x,q)} \\
\mathscr{Q}_T & \xrightarrow{\tau_q} & t_{(0,q)}^*\mathscr{Q}_T & \xrightarrow{t_{(0,q)}^*\sigma_x} & t_{(x,q)}^*\mathscr{Q}_T
\end{array}$$

Proof. A priori it is clear that there exists a constant $c\in\mathbb{G}_m(T)$ such that $(t_{(0,q)}^*\sigma_x)\circ\tau_q = c\cdot(t_{(x,0)}^*\tau_q)\circ\sigma_x$, so all we need to show is that $c=e_f(x,q)$. For this we may restrict everything to $X\times\mathrm{Ker}(f^t)$. As in the above discussion, we think of $\mathscr{Q}'$ as the sheaf of sections of $\mathbb{A}^1$ over $X\times\mathrm{Ker}(f^t)$. We have seen that $(t_{(x,0)}^*\tau_q)\circ\sigma_x$ is given on points by $(t,u,a)\mapsto\big(t+x,u+q,e_f(x,u)\cdot a\big)$, whereas $(t_{(0,q)}^*\sigma_x)\circ\tau_q$ is given by $(t,u,a)\mapsto\big(t+x,u+q,e_f(x,u+q)\cdot a\big)$. Because e_f is bilinear, the result follows. □

Next we prove a compatibility result among the two main duality theorems that we have proved in Chapter 7.

DualDualProp **(11.17) Proposition.** *Let $f\colon X\to Y$ be an isogeny of abelian varieties. Let $\kappa_X\colon X\to X^{tt}$ be the canonical isomorphism.*

(i) *For any k-scheme T and points $x\in\mathrm{Ker}(f)\big(T\big)$ and $\eta\in\mathrm{Ker}(f^t)\big(T\big)$ we have the relation $e_{f^t}\big(\eta,\kappa_X(x)\big) = e_f(x,\eta)^{-1}$.*

(ii) *Let $\beta_1\colon \mathrm{Ker}(f^t)\xrightarrow{\sim}\mathrm{Ker}(f)^D$ and $\beta_2\colon \mathrm{Ker}(f^{tt})\xrightarrow{\sim}\mathrm{Ker}(f^t)^D$ be the canonical isomorphisms as in* Theorem (7.5)*, and let $\gamma\colon \mathrm{Ker}(f)^{DD}\xrightarrow{\sim}\mathrm{Ker}(f)$ be the isomophism of* Theorem (3.22)*. Then the isomorphism $\mathrm{Ker}(f)\xrightarrow{\sim}\mathrm{Ker}(f^{tt})$ induced by κ_X equals $-\beta_2^{-1}\circ\beta_1^D\circ\gamma^{-1}$.*

Proof. (i) Consider the commutative diagram

$$\begin{array}{ccccc}
X\times X^t & \xleftarrow{\mathrm{id}\times f^t} & X\times Y^t & \xrightarrow{f\times\mathrm{id}} & Y\times Y^t \\
{\scriptstyle \kappa_X\times\mathrm{id}}\downarrow & & {\scriptstyle \kappa_X\times\mathrm{id}}\downarrow & & \downarrow{\scriptstyle \kappa_Y\times\mathrm{id}} \\
X^{tt}\times X^t & \xleftarrow{\mathrm{id}\times f^t} & X^{tt}\times Y^t & \xrightarrow{f^{tt}\times\mathrm{id}} & Y^{tt}\times Y^t
\end{array} \qquad (2)$$

PolWp:fftftt

If we read the lower row from right to left (term by term!), we get the row

$$Y^t\times Y^{tt} \xleftarrow{\mathrm{id}\times f^{tt}} Y^t\times X^{tt} \xrightarrow{f^t\times\mathrm{id}} X^t\times X^{tt}$$

which is precisely (1) for the morphism $f^t\colon Y^t \to X^t$. Now the result follows from the previous proposition, with the -1 in the exponent coming from the fact that we are reading the lower row in (2) from right to left, thereby switching factors.

(ii) This follows from (i) using the relations $e_f(x,\eta) = \beta_1(\eta)\big(x\big) = (\beta_1^D \circ \gamma^{-1})(x)\big(\eta\big)$ and $e_{f^t}\big(\eta, \kappa_X(x)\big) = \beta_2\big(\kappa_X(x)\big)\big(\eta\big)$. □

PXonSlices **(11.18) Example.** Let X be an abelian variety over k. Let $\mathscr{P} = \mathscr{P}_X$ be its Poincaré bundle. Let n be a positive integer, and let $e_n\colon X[n] \times X^t[n] \to \mu_n$ be the Weil pairing.

The geometric line bundle on $X \times X^t[n]$ that corresponds to $\mathscr{P}_{|X\times X^t[n]}$ is the quotient of $\mathbb{A}^1_{X\times X^t[n]} = X\times X^t[n]\times\mathbb{A}^1$ under the action of $X[n]\times\{0\}$, with $x \in X[n]$ acting on $X\times X^t[n]\times\mathbb{A}^1$ by $\sigma_x\colon (t,u,a) \mapsto \big(t+x, u, e_n(x,u)\cdot a\big)$.

To make this completely explicit, suppose $k = \overline{k}$ and $\mathrm{char}(k) \nmid n$, so that $X[n]$ and $X^t[n]$ are constant group schemes, each consisting of n^{2g} distinct points. Then for $\xi \in X^t[n](k)$, the restriction of the Poincaré bundle to $X \times \{\xi\}$ is given by

$$\mathscr{P}_{|X\times\{\xi\}}\big(U\big) = \big\{ f \in O_X(n^{-1}U) \;\big|\; f(v+x) = e_n(x,\xi)\cdot f(v) \text{ for all } v \in n^{-1}U \text{ and } x \in X[n]\big\}\,.$$

For the restriction of $\mathscr{P}_X$ to $X[n] \times X^t$ we have an analogous description; namely, the corresponding geometric line bundle is the quotient of $\mathbb{A}^1_{X[n]\times X^t} = X[n] \times X^t \times \mathbb{A}^1$ under the action of $\{0\} \times X^t[n]$, with $\xi \in X^t[n]$ acting on $X[n] \times X^t \times \mathbb{A}^1$ by $\tau_\xi\colon (t,u,a) \mapsto \big(t, u + \xi, e_n(t,\xi)^{-1}\cdot a\big)$. Note, however, that whereas our description of $\mathscr{P}_{|X\times X^t[n]}$ is essentially a reformulation of the definition of the Weil pairing, to arrive at our description of $\mathscr{P}_{|X[n]\times X^t}$ we use (i) of Proposition (11.17).

eLeGLIntr **(11.19)** Let L be a non-degenerate line bundle on an abelian variety X. As the associated isogeny $\varphi_L\colon X \to X^t$ is symmetric, we have $K(L) = \mathrm{Ker}(\varphi_L) = \mathrm{Ker}(\varphi_L^t)$, and we obtain a pairing

$$e_{\varphi_L}\colon K(L) \times K(L) \to \mathbb{G}_m\,.$$

On the other hand we have the theta group $1 \longrightarrow \mathbb{G}_m \longrightarrow \mathscr{G}(L) \longrightarrow K(L) \longrightarrow 0$, and this, too, gives a pairing

$$e^L\colon K(L) \times K(L) \to \mathbb{G}_m\,.$$

eLeGLProp **(11.20) Proposition.** *We have $e_{\varphi_L} = e^L$.*

Proof. We apply what was explained in (11.15) to the isogeny $\varphi_L\colon X \to X^t$. We identify $X \times X^{tt}$ with $X \times X$ via the isomorphism $\mathrm{id} \times \kappa_X\colon X \times X \xrightarrow{\sim} X \times X^{tt}$. The line bundle $\mathscr{Q} := (\varphi_L \times \kappa_X)^*\mathscr{P}_{X^t} = (\mathrm{id}\times\varphi_L)^*\mathscr{P}_X$ is none other than the Mumford bundle $\Lambda(L)$ associated to L. Let $\mathscr{Q}' := \mathscr{Q}_{|X\times K(L)} = \Lambda(L)_{|X\times K(L)}$ which, as we already knew from Lemma (2.17), is trivial.

Let T be a k-scheme, and consider T-valued points $x, y \in K(L)\big(T\big)$. Possibly after replacing T by a covering we can choose isomorphisms $\varphi\colon L_T \xrightarrow{\sim} t_x^*L_T$ and $\psi\colon L_T \xrightarrow{\sim} t_y^*L_T$. Then (x,φ) and (y,ψ) are T-valued points of $\mathscr{G}(L)$, and by definition of the pairing e^L we have the relation

PolWp:eLformula
$$(t_y^*\varphi)\circ\psi = e^L(x,y)\cdot(t_x^*\psi)\circ\varphi\,. \tag{3}$$

We can also view ψ as the trivialisation

$$\psi\colon O_{X_T\times\{y\}} \xrightarrow{\sim} \Lambda(L_T)_{X_T\times\{y\}} = t_y^*L_T \otimes L_T^{-1}$$

that sends $1 \in \Gamma(X_T, O_{X_T \times \{y\}})$ to the global section ψ of $t_y^* L_T \otimes L_T^{-1}$. If $\sigma_x \colon \mathscr{Q}_T \to t_{(x,0)}^* \mathscr{Q}_T$ is the isomorphism that gives the action of $(x,0) \in K(L) \times \{0\}$ on $\mathscr{Q}$ then it follows from what we have seen in (11.15) that we have a commutative diagram

$$\begin{array}{ccc} \Lambda(L)_{X_T \times \{y\}} & \xrightarrow{(\sigma_x)_{|X_T \times \{y\}}} & t_{(x,0)}^* \Lambda(L)_{|X_T \times \{y\}} \\ {\scriptstyle \psi}\uparrow & & \uparrow{\scriptstyle e_{\varphi_L}(x,y) \cdot \left(t_{(x,0)}^* \psi\right)} \\ O_{X_T \times \{y\}} & \xrightarrow{\quad\text{can}\quad} & t_{(x,0)}^* O_{X_T \times \{y\}} \quad . \end{array}$$

We have $t_{(x,0)}^* \Lambda(L_T) = m^*(t_x^* L_T \otimes L_T^{-1}) \otimes p_1^*(t_x^* L_T \otimes L_T^{-1})^{-1} \otimes \Lambda(L_T)$. Taking this as an identification, σ_x is given on sections by $s \mapsto m^*\varphi \otimes p_2^*\varphi^{-1} \otimes s$. (Note that this does not depend on the choice of φ.) Now restrict to $X_T \times \{y\}$ and use the natural identification

$$t_{(x,0)}^* \Lambda(L_T)_{|X_T \times \{y\}} = t_{x+y}^* L_T \otimes t_x^* L_T^{-1} = \mathit{Hom}(t_x^* L_T, t_{x+y}^* L_T) \,.$$

we find that $\sigma_x \circ \psi$ maps $1 \in \Gamma(X_T, O_{X_T \times \{y\}})$ to the homomorphism $t_y^*\varphi \circ \psi \circ \varphi^{-1} \colon t_x^* L_T \to t_{x+y}^* L_T$. On the other hand, the composition $(t_{(x,0)}^* \psi) \circ \text{can}$ sends 1 to $t_x^* \psi$. Hence we have

$$t_y^*\varphi \circ \psi \circ \varphi^{-1} = e_{\varphi_L}(x,y) \cdot t_x^* \psi$$

and comparison with (3) now gives the result. □

efRulesProp **(11.21) Proposition.** (i) *Let $f \colon X \to Y$ be a homomorphism of abelian varieties over k. Then for any integer $n \geqslant 1$ the diagram*

$$\begin{array}{ccc} X[n] \times Y^t[n] & \xrightarrow{1 \times f^t} & X[n] \times X^t[n] \\ {\scriptstyle f \times 1}\downarrow & & \downarrow{\scriptstyle e_n} \\ Y[n] \times Y^t[n] & \xrightarrow{e_n} & \mu_n \end{array}$$

is commutative. In other words: if T is a k-scheme, $x \in X[n]\big(T\big)$ and $\eta \in Y^t[n]\big(T\big)$ then $e_n\big(f(x), \eta\big) = e_n\big(x, f^t(\eta)\big)$.

(ii) *Let $f \colon X \to Y$ and $g \colon Y \to Z$ be isogenies, and write $h := g \circ f \colon X \to Z$. Then we have "commutative diagrams"*

$$\begin{array}{ccc} \mathrm{Ker}(f) \times \mathrm{Ker}(f^t) & \xrightarrow{e_f} & \mathbb{G}_m \\ {\scriptstyle i}\downarrow \quad \uparrow{\scriptstyle g^t} & & \| \\ \mathrm{Ker}(h) \times \mathrm{Ker}(h^t) & \xrightarrow{e_h} & \mathbb{G}_m \end{array} \qquad \textit{and} \qquad \begin{array}{ccc} \mathrm{Ker}(g) \times \mathrm{Ker}(g^t) & \xrightarrow{e_g} & \mathbb{G}_m \\ {\scriptstyle f}\uparrow \quad \downarrow{\scriptstyle i} & & \| \\ \mathrm{Ker}(h) \times \mathrm{Ker}(h^t) & \xrightarrow{e_h} & \mathbb{G}_m \end{array}$$

where the maps labelled "i" are the natural inclusion homomorphisms. By our assertion that the first diagram is commutative we mean that if T is a k-scheme, $x \in \mathrm{Ker}(f)\big(T\big)$ and $\eta \in \mathrm{Ker}(h^t)\big(T\big)$ then $e_f\big(x, g^t(\eta)\big) = e_h\big(i(x), \eta\big)$; similarly for the second diagram.

Proof. (i) Let $\chi \colon Y[n]_T \to \mathbb{G}_{m,T}$ be the character corresponding to η, as in (11.12). Then the character corresponding to $h^t(\eta)$ is $\chi \circ h \colon X[n]_T \to \mathbb{G}_{m,T}$. By (11.12) we find

$$e_n\big(h(x), \eta\big) = \chi\big(h(x)\big) = \chi \circ h(x) = e_n\big(x, h^t(\eta)\big) \,.$$

(ii) Let $\chi \colon \mathrm{Ker}(h)_T \to \mathbb{G}_{m,T}$ be the character corresponding to η. Then the character $\mathrm{Ker}(f)_T \to \mathbb{G}_{m,T}$ corresponding to $g^t(\eta)$ is simply $\chi \circ i$. Hence by what was explained in (11.12),

$e_h\big(i(x),\eta\big) = \chi\big(i(x)\big) = \chi\circ i(x) = e_f\big(x, g^t(\eta)\big)$. This gives the first commutative diagram. For the second, apply the first diagram to the composition $f^t\circ g^t\colon Z^t \to Y^t \to X^t$; then apply (i) of Proposition (11.17). □

elambdanAlt **(11.22) Corollary.** *Let $\lambda\colon X \to X^t$ be a polarization, and let n be a positive integer. Then the pairing $e_n^\lambda\colon X[n]\times X[n] \to \mu_n$ is alternating: for any $x \in X[n]\big(T\big)$ with T a k-scheme we have $e_n^\lambda(x,x) = 1$.*

Proof. Without loss of generality we may assume that $k = \overline{k}$ and write $\lambda = \varphi_L$ for some ample L. Consider the composition $n\lambda = \lambda\circ[n]_X$. Applying (ii) of Proposition (11.21) we find a commutative diagram

$$\begin{array}{ccc} X[n]\times X^t[n] & \xrightarrow{e_n} & \mathbb{G}_m \\ {\scriptstyle i}\big\downarrow \quad \big\uparrow{\scriptstyle \lambda} & & \big\| \\ \mathrm{Ker}(n\lambda)\times \mathrm{Ker}(n\lambda) & \xrightarrow{e_{n\lambda}} & \mathbb{G}_m \end{array}$$

This gives $e_n^\lambda(x,x) = e_n\big(x, \lambda\circ i(x)\big) = e_{n\lambda}\big(i(x), i(x)\big) = 1$, where in the last step we use Proposition (11.20) together with the remark that $n\lambda = \varphi_{L^n}$. □

In particular, we find that the pairing e_n^λ is skew-symmetric: $e_n^\lambda(x,y) = e_n^\lambda(y,x)^{-1}$. Note, however, that skew-symmetry is weaker in general than the property of being alternating.

ElambdaDef **(11.23)** Let X be an abelian variety over a field k. Fix a separable closure $k \subset k_s$. As usual, ℓ denotes a prime number different from $\mathrm{char}(k)$. Let $x = (0, x_1, x_2, \ldots)$ be an element of $T_\ell X$ and $\xi = (0, \xi_1, \xi_2, \ldots)$ and element of $T_\ell X^t$. Applying (ii) of Proposition (11.21) we find that

$$e_{\ell^m}(x_m, \xi_m) = e_{\ell^{m+1}}(\ell\cdot x_{m+1}, \xi_{m+1}) = e_{\ell^{m+1}}(x_{m+1}, \xi_{m+1})^\ell\,.$$

This means precisely that

$$E(x,\xi) = \big(1, e_\ell(x_1,\xi_1), e_{\ell^2}(x_2,\xi_2), \ldots\big)$$

is a well-defined element of $\mathbb{Z}_\ell(1) = T_\ell\mathbb{G}_m$. The map $(x,\xi)\mapsto E(x,\xi)$ defines a perfect bilinear pairing

$$E\colon T_\ell X \times T_\ell X^t \to \mathbb{Z}_\ell(1)\,.$$

If $\beta\colon T_\ell X^t \xrightarrow{\sim} (T_\ell X)^\vee(1)$ is the canonical isomorphism as in Proposition (10.9) then the pairing E is nothing else but the composition

$$T_\ell X \times T_\ell X^t \xrightarrow{\mathrm{id}\times\beta} T_\ell X \times (T_\ell X)^\vee(1) \xrightarrow{\mathrm{ev}} \mathbb{Z}_\ell(1)$$

where the map "ev" is the canonical pairing, or "evaluation pairing". Note that the pairing E is equivariant with respect to the natural action of $\mathrm{Gal}(k_s/k)$ on all the terms involved.

If $\lambda\colon X \to X^t$ is a polarization, we obtain a pairing

$$E^\lambda\colon T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1) \qquad \text{by} \qquad E^\lambda(x,x') := E\big(x, T_\ell\lambda(x')\big)\,.$$

If $\lambda = \varphi_L$ we also write E^L for E^λ. It readily follows from Corollary (11.22) that the pairing E^λ is alternating.

Putting everything together, E^λ is a $\mathrm{Gal}(k_s/k)$-invariant element in $\big(\wedge^2(T_\ell X)^\vee\big)(1)$. The cohomological interpretation is that E^λ is the first Chern class of λ, or rather of any line bundle representing λ. Note that $\big(\wedge^2(T_\ell X)^\vee\big)(1) = H^2\big(X_{k_s}, \mathbb{Z}_\ell(1)\big)$, see Corollary (10.39).

AVnoPP **(11.24)** Suppose we have an abelian variety X of dimension g over a field k. If $g = 1$ then X is an elliptic curve, and the origin O (as a divisor on X) gives a principal polarization (via $Q \mapsto O - Q$). If $g \geqslant 2$ then in general X does not carry a principal polarization, not even if we allow an extension of the base field. Let us explain why this is so.

Fix $g \geqslant 2$. We shall use the fact that there exists an algebraically closed field k and an abelian variety Y of dimension g over k such that $\mathrm{End}(Y) = \mathbb{Z}$. A proof of this shall be given later; see ??. Note that this does not work for arbitrary k; for instance, every abelian variety over $\overline{\mathbb{F}}_p$ has $\mathbb{Z} \subsetneq \mathrm{End}(Y)$, as we shall see in ??.

If Y carries no principal polarization then we have the desired example. Hence we may assume there is a principal polarization $\lambda\colon Y \to Y^t$. As $k = \overline{k}$ there is a line bundle L with $\lambda = \varphi_L$. Because λ is principal and $\mathrm{End}(X) = \mathbb{Z}$ the only polarizations of Y are those of the form $\varphi_{L^n} = n \cdot \lambda$, of degree n^{2g}.

On the other hand, if ℓ is any prime number different from $\mathrm{char}(k)$ then $Y[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ as group schemes. Hence Y has a subgroup scheme H of order ℓ. Let $q\colon Y \to X := Y/H$ be the quotient. If $\mu\colon X \to X^t$ is a polarization then $q^*\mu$ is a polarization of Y, with $\deg(q^*\mu) = \ell^2 \cdot \deg(\mu)$. But as just explained, any polarization of Y has degree equal to n^{2g} for some $n \in \mathbb{N}$. Hence μ cannot be principal.

With a similar construction we shall see later that an abelian variety of dimension $g \geqslant 2$ over a field of characteristic p in general does not even carry a separable polarization; see ??.

To arrive at some positive results, we shall now first give a very useful criterion for when a polarization $\lambda\colon X \to X^t$ descends over an isogeny $f\colon X \to Y$. If L is a line bundle on X then by Theorem (8.10) there exists a line bundle M on Y with $L \cong f^*M$ if and only if the following conditions are satisfied:

(a) $\mathrm{Ker}(f)$ is contained in $K(L)$ and is totally isotropic with respect to the pairing $e_{\mathscr{G}(L)} = e_{\varphi_L}$;
(b) the inclusion map $\mathrm{Ker}(f) \hookrightarrow K(L)$ can be lifted to a homomorphism $\mathrm{Ker}(f) \hookrightarrow \mathscr{G}(L)$.

(The second condition in (a) is in fact implied by (b).) As we shall prove now, in order for a polarization to descend, it suffices that the analogue of condition (a) holds.

PolDesc **(11.25) Proposition.** *Let $\lambda\colon X \to X^t$ be a symmetric isogeny, and let $f\colon X \to Y$ be an isogeny.*

(i) *There exists a symmetric isogeny $\mu\colon Y \to Y^t$ such that $\lambda = f^*\mu := f^t \circ \mu \circ f$ if and only if* $\mathrm{Ker}(f)$ *is contained in* $\mathrm{Ker}(\lambda)$ *and is totally isotropic with respect to the pairing $e_\lambda\colon \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mathbb{G}_m$. If such an isogeny μ exists then it is unique.*

(ii) *Assume that an isogeny μ as in* (i) *exists. Then μ is a polarization if and only if λ is a polarization.*

Note that the "only if" in (ii) was already proven in Proposition (11.8). For this implication the assumption that f is an isogeny can be weakened; see Exercise (11.1).

Proof. (i) If $\lambda = f^t \circ \mu \circ f$ then $\mathrm{Ker}(f) \subset \mathrm{Ker}(\lambda)$ and it follows from (ii) of Proposition (11.21), applied with $g = (f^t \circ \mu)$ and $h = \lambda$, that $\mathrm{Ker}(f)$ is totally isotropic for the pairing e_λ.

For the converse, assume $\mathrm{Ker}(f)$ is contained in $\mathrm{Ker}(\lambda)$ and is totally isotropic with respect to e_λ. Consider the line bundle $M := (1 \times \lambda)^* \mathscr{P}_X$ on $X \times X$. Recall from Example (8.26) that the theta group $\mathscr{G}(M)$ is naturally isomorphic to the Heisenberg group associated to the group scheme $\mathrm{Ker}(\lambda)$. We have natural actions of $\mathrm{Ker}(\lambda) \times \{0\}$ and $\{0\} \times \mathrm{Ker}(\lambda)$ on M; for the first action note that M can also be written as $(\lambda \times 1)^* \mathscr{P}_{X^t}$. The assumption that $\mathrm{Ker}(f) \subset \mathrm{Ker}(\lambda)$

is totally isotropic for e_λ means precisely that the actions of $\mathrm{Ker}(f) \times \{0\}$ and of $\{0\} \times \mathrm{Ker}(f)$ commute, and therefore define an action of $\mathrm{Ker}(f) \times \mathrm{Ker}(f)$ on M. This gives us a line bundle N on $Y \times Y$ such that $M \cong (f \times f)^* N$. If $\mu\colon Y \to Y^t$ is the (unique) homomorphism such that $N = (1 \times \mu)^* \mathscr{P}_Y$ then we get the desired relation $\lambda = f^t \circ \mu \circ f$. The uniqueness of μ is immediate from Lemma (5.4). But we also have $\lambda = \lambda^t = (f^t \circ \mu \circ f)^t = f^t \circ \mu^t \circ f$. Hence $\mu = \mu^t$.

(ii) By Proposition (11.2) there exists a field extension $k \subset K$ and a line bundle L on Y_K with $\mu_K = \varphi_L$, and then $\lambda_K = \varphi_{f^*L}$. Because f is finite, L is effective if and only if f^*L is effective. □

IsogtoPPAV **(11.26) Corollary.** *Let X be an abelian variety over an algebraically closed field. Then X is isogenous to an abelian variety that admits a principal polarization.*

Proof. Start with any polarization $\lambda\colon X \to X^t$. By Lemma (8.22) there exists a Lagrangian subgroup $H \subset \mathrm{Ker}(\lambda)$. (There clearly exists a subgroup $H \subset \mathrm{Ker}(\lambda)$ satisfying condition (i) of that Lemma.) By the previous Proposition, λ descends to a principal polarization on X/H. □

The conclusion of the Corollary no longer holds in general if we drop the assumption that the ground field is algebraically closed. For examples, see e.g. Howe [1], [2] and Silverberg-Zarhin [1].

[alpha]XDef **(11.27)** Before we turn to Zarhin's trick, we recall from Exercise (7.8) some notation.

Suppose X is an abelian variety and $\alpha = (a_{ij})$ is an $r \times s$ matrix with integral coefficients. Then we denote by $[\alpha]_X\colon X^s \to X^r$ the homomorphism given by

$$[\alpha]_X\big(x_1, \ldots, x_s\big) = \big(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1s}x_s, \ldots, \sum_{j=1}^{s} a_{ij}x_j, \ldots, a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rs}x_s\big)\,.$$

For $r = s = 1$ this just gives our usual notation $[n]_X$ for the "multiplication by n" maps. As another example, the 1×2 matrix $(1\,1)$ gives the group law on X while the 2×1 matrix $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ gives the diagonal.

If β is a $q \times r$ matrix with integral coefficients then $[\beta \cdot \alpha]_X = [\beta]_X \circ [\alpha]_X\colon X^s \to X^q$. It follows that if α is an invertible $r \times r$ matrix then $[\alpha]_X$ is an automorphism of X^r. Further, if $f\colon X \to Y$ is a homomorphism of abelian varieties then for any integral $r \times s$ matrix α,

$$[\alpha]_Y \circ \underbrace{(f, \ldots, f)}_{s} = \underbrace{(f, \ldots, f)}_{r} \circ [\alpha]_X\colon X^s \to Y^r\,.$$

[alpha]XProp **(11.28) Proposition.** *Let X be an abelian variety of dimension g.*

(i) *If $\alpha \in M_r(\mathbb{Z})$ then $[\alpha]_X\colon X^r \to X^r$ has degree $\det(\alpha)^{2g}$.*

(ii) *Let β be an $r \times s$ matrix with integral coefficients. Then $\big([\beta]_X\big)^t = \big[{}^t\beta\big]_{X^t}$, where ${}^t\beta$ is the transposed matrix.*

Proof. (i) If $\det(\alpha) = 0$ then it is readily seen that $[\alpha]_X$ has infinite kernel, so by convention we have $\deg\big([\alpha_X]\big) = 0$. Now assume $\det(\alpha) \neq 0$, and let $\{e_1, \ldots, e_r\}$ be the standard ordered basis of $\mathbb{Z}^r$. By the theory of elementary divisors, there is an ordered basis $\{f_1, \ldots, f_r\}$ for $\mathbb{Z}^r$ and a sequence of nonzero integers $(n_1, \ldots, n_r)$ such that $\alpha(e_i) = n_i \cdot f_i$. Let $\beta \in \mathrm{GL}_r(\mathbb{Z})$ be the matrix with $\beta(e_i) = f_i$, and let $\gamma = \mathrm{diag}(n_1, \ldots, n_r)$ be the diagonal matrix with coefficients n_i. Then $[\beta]_X$ is an automorphism of X^r and it is clear that $[\gamma]_X\colon X^r \to X^r$, which is given by

$(x_1, \ldots, x_r) \mapsto (n_1 x_1, \ldots, n_r x_r)$, has degree $(n_1 \cdots n_r)^{2g} = \det(\alpha)^{2g}$. As $[\alpha]_X = [\gamma]_X \circ [\beta]_X$ the claim follows.

(ii) Write $\beta = (b_{ij})$. Any line bundle L on X^r with class in Pic^0 can be written as $L = p_1^* L_1 \otimes \cdots \otimes p_r^* L_r$, where the p_i: $X^r \to X$ are the projection maps and the L_i are line bundles on X with class in Pic^0. Because $(X^s)^t \cong (X^t)^s$ (cf. Exercise (6.2)) it suffices to know the restriction of $[\beta]_X^* L$ to each of the coordinate axes $\{0\} \times \cdots \times \{0\} \times X \times \{0\} \times \cdots \times \{0\}$. But the restriction of $[\beta]_X$ to the j-th coordinate axis is the map $X \to X^r$ given by $x \mapsto (b_{1j}x, b_{2j}x, \ldots, b_{rj}x)$ and the pull-back of L under this map is

$$b_{1j}^* L_1 \otimes \cdots \otimes b_{rj}^* L_r = L_1^{\otimes b_{1j}} \otimes \cdots \otimes L_r^{\otimes b_{rj}} .$$

This means precisely that $[\beta]_X^t$: $(X^r)^t = (X^t)^r \to (X^s)^t = (X^t)^s$ is the map given by the matrix

$$\begin{pmatrix} b_{11} & \cdots & b_{i1} & \cdots & b_{r1} \\ \vdots & & \vdots & & \vdots \\ b_{1j} & \cdots & b_{ij} & \cdots & b_{rj} \\ \vdots & & \vdots & & \vdots \\ b_{1s} & \cdots & b_{is} & \cdots & b_{rs} \end{pmatrix} = {}^{\mathrm{t}}\beta ,$$

as claimed. □

ZarTrick **(11.29) Theorem.** (Zarhin's trick) *Let X be an abelian variety over a field k. Then $X^4 \times (X^t)^4$ carries a principal polarization.*

Proof. Suppose we have an abelian variety Y, a polarization μ: $Y \to Y^t$, and an endomorphism α: $Y \to Y$. Consider the isogeny f: $Y \times Y \to Y \times Y^t$ given by $(y_1, y_2) \mapsto \big(y_1 - \alpha(y_2), \mu(y_2)\big)$. The kernel is given by $\mathrm{Ker}(f) = \big\{(\alpha(y), y) \;\big|\; y \in \mathrm{Ker}(\mu)\big\}$. In particular, $\deg(f) = \deg(\mu)$. Proposition (11.25) tells us under what conditions the polarization $\mu \times \mu$: $(Y \times Y) \to (Y^t \times Y^t)$ descends to a polarization on $Y \times Y^t$ via the isogeny f. Namely: there exists a polarization ν on $Y \times Y^t$ with $f^*\nu = (\mu \times \mu)$ if and only if
(a) $\alpha\big(\mathrm{Ker}(\mu)\big) \subseteq \mathrm{Ker}(\mu)$, and
(b) $e_\mu\big(\alpha(y_1), \alpha(y_2)\big) \cdot e_\mu(y_1, y_2) = 1$ for all (scheme valued) points y_1, y_2 of $\mathrm{Ker}(\mu)$.
Note that if such a descended polarization ν exists then it is principal.

Condition (a) means that there exists an endomorphism β: $Y^t \to Y^t$ such that $\beta \circ \mu = \mu \circ \alpha$. By (ii) of Proposition (11.21),

$$e_\mu\big(\alpha(y_1), \alpha(y_2)\big) = e_{\mu \circ \alpha}\big(y_1, \alpha(y_2)\big) = e_{\beta \circ \mu}\big(y_1, \alpha(y_2)\big) = e_\mu\big(y_1, \beta^t\alpha(y_2)\big) ,$$

so (b) is equivalent to the condition that $e_\mu\big(y_1, (1 + \beta^t\alpha)(y_2)\big) = 1$ for all y_1, y_2 in $\mathrm{Ker}(\mu)$. As e_μ is a pefect pairing on $\mathrm{Ker}(\mu)$, this is equivalent to the condition that $(1 + \beta^t\alpha) \in \mathrm{End}(Y)$ kills $\mathrm{Ker}(\mu)$.

We now apply this with $Y = X^4$. Choose any polarization λ on X, and take $\mu = \lambda^4$ (so $\mu = \lambda \times \lambda \times \lambda \times \lambda$). For α we take the endomorphism $[\alpha]_X$ given by a 4×4 matrix α with integral coefficients. As $\lambda^4 \circ [\alpha]_X = [\alpha]_{X^t} \circ \lambda^4$, condition (a) is automatically satisfied, and we have $\beta = [\alpha]_{X^t}$ in the above. Using (ii) of Proposition (11.28) we find that the only condition that remains is that $[\mathrm{id}_4 + {}^{\mathrm{t}}\alpha\alpha]_X$ kills $\mathrm{Ker}(\mu) = \mathrm{Ker}(\lambda)^4$, where id_4 is the 4×4 identity matrix.

Choose an integer m such that $\mathrm{Ker}(\lambda) \subset X[m]$. We are done if we can find an integral 4×4 matrix α such that $\mathrm{id}_4 + {}^{\mathrm{t}}\alpha\alpha \equiv 0 \bmod m$. To see that such a matrix can be found we use the

fact that every integer can be written as a sum of four squares. In particular there exist integers a, b, c, d with $a^2+b^2+c^2+d^2 = m-1$. Now take

$$\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}, \tag{4}$$

PolWp:ZarTrMat

for which we have $\mathrm{id}_4 + {}^{\mathrm{t}}\alpha\alpha = m \cdot \mathrm{id}_4$. □

ZarTrickRem **(11.30) Remarks.** (i) The choice of the matrix α can be explained as follows. Consider the Hamiltonian quaternion algebra $\mathbb{H} = \mathbb{R}\cdot 1 + \mathbb{R}\cdot i + \mathbb{R}\cdot j + \mathbb{R}\cdot k$, which is a central simple algebra over $\mathbb{R}$. For $x = a\cdot 1 + b\cdot i + c\cdot j + d\cdot k$ we define its complex conjugate by $\bar{x} = a\cdot 1 - b\cdot i - c\cdot j - d\cdot k$. The reduced trace and norm of $\mathbb{H}$ over $\mathbb{R}$ are given by

$$\mathrm{Trd}_{\mathbb{H}/\mathbb{R}}(x) = x + \bar{x} = 2a \qquad \text{and} \qquad \mathrm{Nrd}_{\mathbb{H}/\mathbb{R}}(x) = x\bar{x} = a^2+b^2+c^2+d^2\,.$$

Further, taking $\{1, i, j, k\}$ as a basis of $\mathbb{H}$, left multiplication by x is given precisely by the matrix (4). The map $h\colon \mathbb{H} \to M_4(\mathbb{R})$ sending x to this matrix is an injective homomorphism of $\mathbb{R}$-algebras, and we have $h(\bar{x}) = {}^{\mathrm{t}}h(x)$ and $\mathrm{Nrd}_{\mathbb{H}/\mathbb{R}}(x) = \det\big(h(x)\big)$. Further it is clear that h maps the subring $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot i + \mathbb{Z}\cdot j + \mathbb{Z}\cdot k$ into $M_4(\mathbb{Z})$. In sum, we can think of α as being the (left) multiplication by $a\cdot 1 + b\cdot i + c\cdot j + d\cdot k$, where a, b, c, d are chosen such that $a^2+b^2+c^2+d^2 = m-1$.

(ii) In general there is no positive n such that for any abelian variety X the nth power X^n admits a principal polarization. To see this we go back to the example in (11.24). We start with an abelian variety Y of dimension $g \geqslant 2$ over a field $k = \overline{k}$ such that $\mathrm{End}(Y) = \mathbb{Z}$ and such that Y does admit a principal polarization; see ?? for the existence. Any homomorphism $Y^n \to (Y^t)^n$ is of the form $\lambda^n \circ [\alpha]_Y = [\alpha]_{Y^t} \circ \lambda^n$ for some $\alpha \in M_n(\mathbb{Z})$, and it easily follows from (ii) of Proposition (11.28) that this homomorphism is symmetric if and only if $\alpha = {}^{\mathrm{t}}\alpha$. Now choose a prime number ℓ different from $\mathrm{char}(k)$, and choose a subgroup $H \subset Y$ of order ℓ, generated by a point of order ℓ. Let $\pi\colon Y \to X := Y/H$ be the quotient.

Let μ be any polarization on X^n. By what was just explained we have $(\pi^n)^*\mu = \lambda^n \circ [\alpha]_Y$ for some $\alpha \in M_n(\mathbb{Z})$. Moreover, $H \times \cdots \times H \subset \mathrm{Ker}\big([\alpha]_Y\big)$, which readily implies that α is divisible by ℓ, say $\alpha = \ell\cdot\beta$. Further we have $\deg(\mu)\cdot\ell^{2n} = \deg\big([\alpha]_Y\big) = \ell^{2ng}\cdot\det(\beta)^{2g}$, so $\deg(\mu) = \ell^{2n(g-1)}\cdot\det(\beta)^{2g}$. In particular, X^n does not carry a principal polarization.

Exercises.

Ex:f*Pol **(11.1)** Let $f\colon X \to Y$ be a homomorphism of abelian varieties with finite kernel. If $\mu\colon Y \to Y^t$ is a polarization, show that $f^*\mu := f^t \circ \mu \circ f$ is a polarization of X.

Ex:ZarhOdd **(11.2)** Let X be an abelian variety over a field k. Suppose there exists a polarization $\lambda\colon X \to X^t$ with $\deg(\lambda) = m$ odd.

(i) Show that there exist integers a and b with $1 + a^2 + b^2 \equiv 0 \bmod m$. [*Hint:* Use the Chinese remainder theorem. First find a solution modulo p for any prime p dividing m. Then use the fact that the curve $C \subset \mathbb{A}^2$ given by $1 + x^2 + y^2 = 0$ is smooth over $\mathbb{Z}_p$ ($p \neq 2$!) to see that the solutions can be lifted to solutions modulo arbitrarily high powers of p.]

(ii) Adapting the proof of Zarhin's trick, show that $X^2 \times (X^t)^2$ admits a principal polarization.

Ex:q*MmodPic0 **(11.3)** Let L be a line bundle on an abelian variety X over a perfect field k. Write $Y := K(L)^0_{\mathrm{red}}$, which is an abelian subvariety of X, and let $q\colon X \to Z := X/Y$ be the quotient.

(i) Show that $\varphi_L\colon X \to X^t$ factors as $\varphi_L = q^t \circ \psi \circ q$ for some homomorphism $\psi\colon Z \to Z^t$.

(ii) Show that there is a finite separable field extension $k \subset K$ and a line bundle M on Z_K such that $\psi_K = \varphi_M$.

(iii) With K and M as in (ii), conclude that the class of $L \otimes q^*M^{-1}$ lies in $\mathrm{Pic}^0_{X/k}(K)$.

We begin this section by extending the definition of an action of a group scheme G on a scheme P to the situation where G and P are only assumed to be fppf sheaves. This is a straightforward generalization of the definitions given in Chapter ?? and mainly serves to recall the notation. Unless indicated otherwise, "fppf sheaf" in this section means "fppf sheaf of sets", and group actions are actions from the left.

fppfGrActSetup **(11.31)** Let S be a scheme. We recall from ?? that an S-scheme defines an fppf sheaf on $\mathsf{Sch}_{/S}$, and that this gives an embedding of the category $\mathsf{Sch}_{/S}$ as a full subcategory of the category $\mathrm{FPPF}(S)$. If an fppf sheaf X is isomorphic to the sheaf defined by a scheme then we shall simply say that X is a scheme.

If X and Y are fppf sheaves on S then we have a product sheaf $X \times_S Y$, whose set of sections over an S-scheme T is the product set $X(T) \times Y(T)$. If X and Y are both S-schemes then the sheaf $X \times_S Y$ is of course just the sheaf defined by the scheme $X \times_S Y$. Note that the category $\mathrm{FPPF}(S)$ has (the sheaf defined by) S as a final object, so $X \times_S Y$ is the ordinary product of X and Y in the category $\mathrm{FPPF}(S)$.

fppfGrActDef **(11.32) Definition.** Let G be a sheaf of groups for the fppf topology, and suppose given an fppf sheaf P.

(i) An action of G on P is a morphism of fppf sheaves

$$\rho\colon G \times_S P \to P$$

such that for every S-scheme T the map $\rho(T)\colon (G \times_S P)\big(T\big) = G(T) \times P(T) \to P(T)$ defines an action of the group $G(T)$ on the set $P(T)$. If there is no risk of confusion, we simply write $g \cdot p$ for $\rho(T)\big((g,p)\big)$

(ii) If we have actions of G on sheaves P_1 and P_2 then a sheaf morphism $f\colon P_1 \to P_2$ is said to be G-equivariant (with respect to the given actions), if $f(T)\colon P_1(T) \to P_2(T)$ is $G(T)$-equivariant for all S-schemes T.

(iii) Given an action ρ as in (i), we define the graph morphism

$$\Psi = \Psi_\rho\colon G \times_S P \to P \times_S P$$

to be the morphism of sheaves with $\Psi(T)\colon G(T)\times P(T) \to P(T)\times P(T)$ given by $(g,p) \mapsto (g\cdot p, p)$.

TorsorDef **(11.33) Definition.** Let S be a scheme. Let G be an fppf sheaf of groups over S.

(i) Consider an fppf sheaf $P\colon \mathsf{Sch}_{/S}^{\mathrm{opp}} \to \mathsf{Sets}$ with a left action $\rho\colon G\times_S P \to P$ of G. Then P, or more precisely the pair (P,ρ), is called a *G-torsor* if the following two conditions are satisfied:

(a) the unique morphism of fppf sheaves $P \to S$ is an epimorphism;

(b) the graph morphism $\Psi\colon G \times_S P \to P \times_S P$ is an isomorphism.

(ii) If P_1 and P_2 are G-torsors then a morphism of torsors $P_1 \to P_2$ is a G-equivariant morphism of sheaves.

TorsorDefRem **(11.34) Remarks.** (i) Condition (a) is satisfied, in particular, when P is an S-scheme such that the structural morphism $P \to S$ is faithfully flat and of finite presentation. This will usually be the case in the examples that we want to consider later. On the other hand, as we shall see in (11.37) below, if we want to set up the general theory there is some advantage in allowing P to be a sheaf.

(ii) We have chosen here to work with sheaves on the fppf site of S. The same definition of a G-torsor can be made for other topologies. For a comprehensive treatment we refer to Giraud [1].

(iii) In practise, when we refer to a torsor we often do not specify the G-action, leaving it implicit or assuming it is clear which action is meant.

TrivTorsor **(11.35)** Assume $G \to S$ is an epimorphism of fppf sheaves. The simplest example of a G-torsor is to take $P = G$, with G acting on itself by left translations. In this case ρ: $G \times_S G \to G$ is just the group law. The graph morphism Ψ is indeed an isomorphism; its inverse is the morphism $G \times_S G \to G \times_S G$ given on points by $(g_1, g_2) \mapsto (g_1 g_2^{-1}, g_2)$. We refer to this G-torsor as the trivial G-torsor. More generally, we say that a G-torsor is trivial is if it isomorphic, as a G-torsor, to the trivial G-torsor.

If $T \to S$ is a morphism of schemes then we can pull-back torsors. Namely, if P is a G-torsor, write P_T for the restriction of P to Sch_T. (See ??) The T-group scheme G_T acts on P_T and one easily checks that this makes P_T into a G_T-torsor. We shall usually refer to P_T as the restriction of P to T.

Condition (b) in the definition of a torsor can be interpreted by saying that locally for the fppf topology, P is trivial. Namely,.... As we shall see in Prop. (11.39) below, if G is smooth over S (which is usually the case in the situations we want to consider) then P is trivial even étale locally on S.

TorsorHomProp **(11.36) Proposition.** (i) *Let P_1 and P_2 be G-torsors over S. If f: $P_1 \to P_2$ is a morphism of G-torsors, it is an isomorphism.*

(ii) *A G-torsor P is trivial if and only if P has a global section, i.e., if $P(S) \neq \emptyset$.*

Proof.(To be written) □

Part (i) of the proposition shows that the category G-Tors of G-torsors over S is a groupoid, i.e., all morphisms in this category are isomorphisms.

Twisting **(11.37)** Twisting .... (to be written)

TorsorExa **(11.38) Proposition.** (i) line bundles and Gm-torsors

(ii) vector bundles and GL-torsors

(iii) Jac^n is a torsor under $J = \mathrm{Pic}^0$.

TorsorEtTriv **(11.39) Proposition.** *Suppose $G \to S$ is a smooth S-group scheme. If P is a G-torsor then there exists an étale covering $\{S_\alpha\}_{\alpha \in A}$ of S such that that the restrictions of P to S_α are trivial for all $\alpha \in A$.*

Proof.(To be written) □

TorsorAV **(11.40)** Let X be an abelian variety over a field k. If P is an X-torsor then P is automatically a scheme; for a proof of this we refer to Raynaud [3], Chap. XIII, Prop. 2.6. It follows from Prop. (11.39) that $P_{\overline{k}} \cong X_{\overline{k}}$. The general results mentioned in ?? therefore imply that $\mathrm{Pic}_{P/k}$ exists as a k-scheme.

We define a morphism of schemes

$$\tilde{\alpha}\colon \mathrm{Pic}_{X/k} \times P \to \mathrm{Pic}_{P/k}$$

as follows. Let T be a k-scheme, and suppose we have a line bundle L on X_T and a T-valued point $p \in P(T)$. As we have seen in ??, the point p gives rise to an isomorphism $\tau_p\colon X_T \xrightarrow{\sim} P_T$, and $\tau_p^{-1,*}(L)$ is a line bundle on P_T. The map given by $(L,p) \mapsto \tau_p^{-1,*}(L)$ defines a morphism of presheaves $P_{X/k} \times P \to P_{P/k}$, and we define $\tilde{\alpha}$ as the induced morphism on associated sheaves.

Let X act on $\mathrm{Pic}_{X/k}$ by sending (x,L) to $t_x^*(L)$. We claim that $\tilde{\alpha}$ induces a morphism

$$\alpha\colon \mathrm{Pic}_{X/k} \times^X P \to \mathrm{Pic}_{P/k}\,.$$

To see this, suppose we have $p \in P(T)$, a line bundle L on X_T and a point $x \in X(T)$. (To be written).

PicPicIsom **(11.41) Proposition.** *Let X be an abelian variety over a field k, and let P be an X-torsor. Then the morphism $\alpha\colon \mathrm{Pic}_{X/k} \times^X P \to \mathrm{Pic}_{P/k}$ defined above is an isomorphism, and it induces isomorphisms*

$$\alpha^0\colon \mathrm{Pic}^0_{X/k} \xrightarrow{\sim} \mathrm{Pic}^0_{P/k} \qquad \textit{and} \qquad \alpha_{\mathrm{NS}}\colon \mathrm{NS}_{X/k} \xrightarrow{\sim} \mathrm{NS}_{P/k}\,.$$

Proof.(To be written) □

phiLTorsor **(11.42)** In the earlier chapters we have made heavy use of the homomorphism $\varphi_L\colon X \to X^t$ associated to a line bundle L on X. Prop. (11.41) allows us to generalize the construction of this homomorphism, where now as input we no longer need a line bundle on X itself but we can associate a homomorphism φ_L to any line bundle on an X-torsor.

To explain the idea of the construction, suppose P is an X-torsor and L is a line bundle on P. If $x \in X(k)$ then we have the action $\rho_x\colon P \to P$ of x on P. Then the line bundle $\rho_x^*(L) \otimes L^{-1}$ defines a class in $\mathrm{Pic}^0_{P/k}$, and we can define $\varphi_L\colon X \to X^t = \mathrm{Pic}^0_{X/k}$ by composing the map $x \mapsto [\rho_x^*(L) \otimes L^{-1}]$ with the inverse of the canonical isomorphism α^0.

The quickest way to give a formal definition is to consider the homomorphism

$$\psi_P := \psi \circ \alpha_{\mathrm{NS}}^{-1}\colon \mathrm{NS}_{P/k} \to \mathit{Hom}^{\mathrm{sym}}(X, X^t) \subset \mathit{Hom}(X, X^t)$$

obtained by composing the inverse of α_{NS} with the homomorphism ψ of ??.

phiLDefTorsor **(11.43) Definition.** Let X be an abelian variety over a field k. Let P be an X-torsor. If L is a line bundle on P_T for some k-scheme T we define

$$\varphi_L\colon X_T \to X_T^t$$

to be the symmetric homomorphism corresponding to the image of $[L] \in \mathrm{NS}_{P/k}(T)$ under the homomorphism ψ_P of ??.

Of course, we may also describe φ_L by elaborating on the pointwise construction given above. For this, we again start with a line bundle L on X_T, and we associate to this the line bundle $M := \rho^*(L) \otimes \mathrm{pr}_2^*(L)^{-1}$ on $X_T \times_T P_T$. Viewing M as a family of line bundles on P_T parametrized by X_T, it defines a morphism $X_T \to \mathrm{Pic}_{P_T/T} = \big(\mathrm{Pic}_{P/k} \times_k T\big)$. Because it sends the zero section of X_T to the identity section of $\mathrm{Pic}_{P_T/T}$, we in fact have a homomorphism $X_T \to \mathrm{Pic}^0_{P/k} \times T$, and φ_L is now obtained by composing with the inverse of α^0.

In view of the isomorphism α_{NS} in Prop. (11.41), it may seem that we have gained nothing. However, in practise the easiest way to define a point of a Néron-Severi group scheme, is to

give a line bundle. But in general, not all points of $\mathrm{NS}_{X/k}(k)$ can be obtained by giving a line bundle on X over the given ground field. So it may be that a given point of $\mathrm{NS}_{X/k}(k)$ cannot be represented by a line bundle on X, while it can be defined by a line bundle on an X-torsor. Better still, we claim that for every point $\xi \in \mathrm{NS}_{X/k}(k)$ we can find an X-torsor P and a line bundle L on P such that $\alpha_{\mathrm{NS}}(\xi) = [L]$. ??????

SymmLBDef **(11.44)** Let L be a line bundle on an abelian variety X. Recall that L is called a symmetric line bundle if $[-1]^*L \cong L$. If L is symmetric then, by definition, there exists an isomorphism $r\colon L \xrightarrow{\sim} [-1]^*L$. The set of all such isomorphisms is then a torsor under the group $\mathrm{Aut}(L) = \Gamma(X, O_X)^* = k^*$, and this allows us to rescale r in a unique way such that on the fibres over 0 it is the identity. (Here, of course, we use the canonical identification $0^*[-1]^*L = 0^*L$.) So we find that there is a unique isomorphism $s\colon L \xrightarrow{\sim} [-1]^*L$ such that s is the identity on the fibres over the origin $0 \in X(k)$; we call this s the normalized symmetry of L.

Let L again be a symmetric line. As $[-1]_X$ is the identity on the 2-torsion subscheme $X[2] \subset X$, the normalized symmetry $s\colon L \xrightarrow{\sim} [-1]^*L$ restricts to an automorphism of the line bundle $L_{|X[2]}$ over $X[2]$. Such an automorphism is the multiplication by a global section $\varepsilon_L \in \Gamma\big(X[2], O^*_{X[2]}\big)$. In concrete terms, if $x \in X[2]\big(k\big)$ is a k-rational 2-torsion point then on the fibre over x the normalized symmetry s is multiplication by $\varepsilon_L(x)$. (More generally, this holds for scheme-valued points.)

We know that $X[2]$ is a finite (and hence affine) group scheme; if $A = \Gamma\big(X[2], O_{X[2]}\big)$ is the corresponding k-algebra then ε_L is an element of A^*. If $\mathrm{char}(k) \neq 2$ then $X[2]$ is an étale group scheme, so over $k = k_s$ we can view ε_L as a function $X[2]\big(k\big) \to k^*$. Note that this function will not, in general, be a homomorphism.

SymmLBLem **(11.45) Lemma.** *Let X be an abelian variety over a field k.*

(i) *If L is a symmetric line bundle on X with normalized symmetry $s\colon L \xrightarrow{\sim} [-1]^*L$ then $[-1]^*(s) \circ s$ is the identity on L. (Here we identify $[-1]^*[-1]^*L = L$.)*

(ii) *The section $\varepsilon_L \in \Gamma\big(X[2], O^*_{X[2]}\big)$ defined above satisfies $\varepsilon_L^2 = 1$, and $\varepsilon_L(0) = 1$.*

(iii) *If L and M are symmetric line bundles on X then so is $L \otimes M$, and $\varepsilon_{L\otimes M} = \varepsilon_L \cdot \varepsilon_M$.*

(iv) *If $f\colon X \to Y$ is a homomorphism of abelian varieties and M is a symmetric line bundle on Y then f^*M is a symetric line bundle on X and $\varepsilon_{f^*M} = f^{\#}(\varepsilon_M)$.*

(v) *Suppose $L^{\otimes 2} \cong O_X$, so that L defines a 2-torsion point $[L] \in X^t[2]\big(k\big)$. Consider the corresponding character $e_2(-, L)\colon X[2] \to \mathbb{G}_m$. Then ε_L is the image of $1 \in \Gamma\big(\mathbb{G}_m, O^*_{\mathbb{G}_m}\big)$ under $e_2(-, L)^{\#}\colon \Gamma\big(\mathbb{G}_m, O^*_{\mathbb{G}_m}\big) \to \Gamma\big(X[2], O^*_{X[2]}\big)$.*

In order to make some of the statements a little more concrete, it is useful to consider the case where $k = k_s$ and $\mathrm{char}(k) \neq 2$. As explained, ε_L can in that case be viewed as a function $X[2]\big(k\big) \to k^*$. Point (ii) of the lemma says that $\varepsilon_L(x) \in \{\pm 1\}$ for all 2-torsion points x, and (v) says that if $L^{\otimes 2} \cong O_X$ then $\varepsilon_L(x) = e_2(x, L)$.

Proof. To be written. □

TotSymmLBDef **(11.46) Definition.** A line bundle L on an abelian variety X is said to be *totally symmetric* if it is symmetric and if moreover $\varepsilon_L = 1$.

In other words, total symmetry is defined by the requirement that the normalized symmetry $s\colon L \xrightarrow{\sim} [-1]^*L$ restricts to the identity on the line bundle $L_{|X[2]}$ over $X[2]$.

It is in fact easy to write down examples of totally symmetric line bundles. Namely, if M is any line bundle on X then $M \otimes [-1]^*M$ is totally symmetric.

KummerVarDef **(11.47) Definition.** Let X be an abelian variety over a field k. The *Kummer variety* of X is the quotient $\mathrm{Kum}_X := X/\langle \pm 1 \rangle$ of X modulo the action of the group $\big\{\mathrm{id}_X, [-1]_X\big\}$.

If there is no risk of confusion we shall usually simply write $\langle \pm 1 \rangle$ for the group $\{\mathrm{id}_X, [-1]_X\}$. The action of this group is not free (unless $X = 0$); the fixed point subscheme is the 2-torsion subscheme $X[2] \subset X$. If X is an elliptic curve then $\mathrm{Kum}_X \cong \mathbb{P}^1$. If $g = \dim(X) > 1$ then Kum_X is singular.

TotSymmLBKummer **(11.48) Proposition.** *Let L be a line bundle on an abelian variety X. Let $q\colon X \to \mathrm{Kum} - X$ be the quotient morphism of X to its Kummer variety. Then L is totally symmetric if and only if there exists a line bundle M on Kum_X such that $L \cong q^*M$.*

Proof. To be written. □

§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 $\mathrm{Hom}(X,Y)$ of homomorphisms $X \to Y$ the structure of an abelian group. For $Y = X$ we find that $\mathrm{End}(X)$ has a natural ring structure, with composition of endomorphisms as the ring multiplication.

Note that $\mathrm{Hom}(X,Y)$ and $\mathrm{End}(X)$ always refer to the homomorphisms and endomorphisms, respectively, over the given ground field. If the context requires it, we shall use the notation $\mathrm{Hom}_k(X,Y)$ and $\mathrm{End}_k(X)$. Let us also recall (see (1.17)) that for the larger set of all morphisms of schemes $X \to Y$, which is just $\mathrm{Hom}(X,Y)\times Y(k)$, the notation $\mathrm{Hom}_{\mathsf{Sch}/k}(X,Y)$ is used. (This larger set rarely ever plays a role in our discussions, though.)

If $n \in \mathbb{Z}$ and $f \in \mathrm{Hom}(X,Y)$ 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 $\mathrm{Hom}(X,Y)$ is torsion-free. We write

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

By definition, $\mathrm{End}^0(X)$ is a $\mathbb{Q}$-algebra. If there is no risk of confusion one simply refers to $\mathrm{End}^0(X)$ as the endomorphism algebra of X. (The term *algebra* is supposed to distinguish it from the endomorphism *ring* $\mathrm{End}(X)$.)

EndkRem **(12.1) Remark.** If $k \subset K$ is a field extension, we have a natural inclusion $\mathrm{Hom}_k(X,Y) \subset \mathrm{Hom}_K(X_K,Y_K)$, which in general is strict. The K-homomorphisms $\mathrm{Hom}_K(X_K,Y_K)$ are the K-valued points of the k-group scheme $\mathit{Hom}(X,Y)$, which, as 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.

PoincSpl **(12.2) Theorem.** (Poincaré Splitting Theorem) *Let X be an abelian variety over a field k. If $Y \subset X$ is an abelian subvariety, 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. (So, $Y+Z = X$ 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. □

PoincSplRem **(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. □

SimpleDef **(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 $k \subset L$.

PoincCor **(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*

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

Up to a permutation of the factors, the abelian varieties Y_i that appear 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 Poincaré Splitting Theorem. The uniqueness statement is an easy exercise—note that a homomorphism between two simple abelian varieties is either zero or an isogeny. □

QAV/k **(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

$$\mathrm{Hom}_{\mathbb{Q}\mathsf{AV}_{/k}}(X,Y) = \mathrm{Hom}^0(X,Y) := \mathrm{Hom}_{\mathsf{AV}_{/k}}(X,Y) \otimes_{\mathbb{Z}} \mathbb{Q}\,.$$

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 $\mathbb{Q}\mathsf{AV}_{/k}$. qua iso

To explain the terminology, notice that 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. In particular, two abelian varieties give isomorphic objects of $\mathbb{Q}\mathsf{AV}_{/k}$ if and only if they are k-isogenous.

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

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

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

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

lmDivLem **(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 is zero 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 $g[p^\infty] = \varphi$.

BilFormLem **(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. □

TlInjThm **(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

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

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 $f_1, \dots, f_r \in \mathrm{End}(X)$ and non-zero ℓ-adic integers $c_1, \dots, c_r$ such that

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

We may assume that r is minimal, i.e., 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 considered in Lemma (12.9). In (2) we may assume that $B(f_1, f_j) = 0$ for all $j \in \{2, \dots, r\}$; 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. □

TlInjCor **(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 $4 \dim(X) \dim(Y)$. □

NSfinite **(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 $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{sym}}(X, X^t)$. □

HomDefField **(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, by which we mean 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 $Hom(X, Y)$ is an étale group scheme, this assertion is just a matter of Galois theory. Choose generators $f_1, \dots, f_r$ 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 $Hom(X, Y)$ 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.*

DegQDef **(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: $\mathrm{End}(X) \to \mathbb{Q}$, 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: $\mathrm{End}^0(X) \to \mathbb{Q}$, with $\deg(q \cdot f) = q^{2g} \cdot \deg(f)$ for $q \in \mathbb{Q}$ and $f \in \mathrm{End}(X)$.

DegisPol **(12.15) Proposition.** *The map* deg: $\mathrm{End}^0(X) \to \mathbb{Q}$ *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. □

CharPolDef **(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, which is uniquely determined, 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, $\mathrm{Norm}(f) := \deg(f) = a_0$.

NormsLemma **(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

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

Endoms:deltac

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. □

Plf=Pf **(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. □

PlfPfCor1 **(12.19) Corollary.** *For any $f \in \mathrm{End}^0(X)$ we have $P_f(f) = 0$.*

PfIntegral **(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. □

PlfPfCor2 **(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??)

VlXfreeQlf **(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.

Ros

inv

§3. *The Rosati involution.*

RosatiDef **(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 $f^\dagger := \lambda^{-1} \circ f^t \circ \lambda$:

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

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 with 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 $\mathrm{trace}(f^\dagger) = \mathrm{trace}(f)$.

dagEladjLem **(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 with the pairing E^λ, 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 $E(V_\ell f(x), V_\ell \lambda(y)) = E^\lambda(V_\ell f(x), y)$. □

dagSymmElts **(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 $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{sym}}(X, X^t)$; hence also $\mathrm{NS}(X) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{Hom}^{0,\mathrm{sym}}(X, X^t)$. 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 $\mathrm{Hom}^0(X, X^t)$. □

TracePos **(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 with 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

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

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). □

can
inv

§4. *The Albert classification.*

AlbertTypes **(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 $(A_1, \ldots, A_{e_0}) \mapsto (\overline{A}_1^t, \ldots, \overline{A}_{e_0}^t)$.

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

Endos:ee0m
$$e_0 := [K_0 : \mathbb{Q}]\,, \qquad e := [K : \mathbb{Q}]\,, \quad \text{and} \quad m := [D : K]^{1/2}\,. \tag{5}$$

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

Write $D^{\mathrm{sym}} := \{d \in D \mid d^\dagger = d\}$. 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

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

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 $\operatorname{char}(k) = 0$ the restrictions are a little stronger than when $\operatorname{char}(k) = p > 0$.

AlbertNumRestr **(12.29) Proposition.** *Let (X, λ) be a simple polarized abelian variety of dimension g over a field k. Let $D = \mathrm{End}^0(X)$ be the endomorphism algebra and let $\dagger$ be the Rosati involution associated with λ. Let K be the center of D, let $K_0 := \{x \in K \mid x^\dagger = x\}$, and define e_0, e and m as in* (5) *above.*

(i) *We have $em \mid 2g$.*

(ii) *If $\operatorname{char}(k) = 0$ then $\dim_{\mathbb{Q}}(D) = em^2$ divides $2g$.*

(iii) *If $L \subset D$ is a $\mathbb{Q}$-subalgebra such that $L \subset D^{\mathrm{sym}}$ then L is a field and $[L : \mathbb{Q}]$ divides g.*

Proof. (i) We know that the norm map Norm: $D \to \mathbb{Q}$ is multiplicative and is a homogeneous polynomial map of degree $2g$. By Lemma (12.17) it follows that $\mathrm{Norm} = \mathrm{Nrd}^n_{D/\mathbb{Q}}$ for some natural number n. But $\mathrm{Nrd}_{D/\mathbb{Q}}$ is polynomial of degree em; hence em divides $2g$.

(ii) For the proof of (ii) we first reduce to the case $k = \mathbb{C}$. Let $\{f_1, \ldots, f_d\}$ be a $\mathbb{Q}$-basis of D. By EGA IV, Prop. (8.9.1), there exists a subfield $k_0 \subset k$ such that k_0 is finitey generated (as a field) over the prime field $\mathbb{Q}$, and such that X and the endomorphisms f_i are defined over k_0. Concretely, this means we have an abelian variety X_0 over k_0 together with endomorphisms $f_{i,0}$ such that there exists an isomorphism $X_0 \otimes_{k_0} k \xrightarrow{\sim} X$ via which $f_{i,0}$ corresponds to f_i. As the f_i form a basis of D and the natural map $\mathrm{End}^0(X_0) \to \mathrm{End}^0(X)$ is injective, we have $\mathrm{End}^0(X_0) \cong D$.

Because k_0 is finitely generated over $\mathbb{Q}$, there exists an embedding $\iota\colon k_0 \to \mathbb{C}$. Then $\mathrm{End}^0(X_{0,\mathbb{C}})$ is a finitely generated module over $D = \mathrm{End}^0(X_0)$, and because D is a divison algebra it follows that $\dim_{\mathbb{Q}}(D)$ divides $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X_{0,\mathbb{C}})\big)$. Hence it suffices to prove (ii) over $k = \mathbb{C}$.

Assume then that $k = \mathbb{C}$. In this case the first homology $H := H_1\big(X(\mathbb{C}), \mathbb{Q}\big)$ is a $\mathbb{Q}$-vector space of dimension $2g$ that has the structure of a D-module. Because D is a division algebra, H is a free D-module; hence $\dim_{\mathbb{Q}}(D)$ divides $\dim_{\mathbb{Q}}(H) = 2g$.

(iii) For f, $g \in L$ we have $fg = f^\dagger g^\dagger = (gf)^\dagger = gf$, so L is a field.

We have a well-defined function $\chi\colon \mathrm{NS}(X)_{\mathbb{Q}} \to \mathbb{Q}$ that sends the class of a line bundle M to $\chi(M)$. By the Riemann-Roch Theorem (9.11), this function χ is multiplicative and is a homogeneous polynomial function of degree g. (Note that we usually write $\mathrm{NS}(X)$ additively, so the assertion that χ is multiplicative then means that $\chi(y_1 + y_2) = \chi(y_1) \cdot \chi(y_2)$ for all y_1, $y_2 \in \mathrm{NS}(X)_{\mathbb{Q}}$.) Because $L \subset D^{\mathrm{sym}}$, we can use the isomorphism i of Prop. (12.25) to define $\chi \circ i^{-1}\colon L \to \mathbb{Q}$, which is a multiplicative and homogeneous polynomial function of degree g on L. By Lemma (12.17) it follows that $\chi \circ i^{-1} = \mathrm{Nrd}^n_{L/\mathbb{Q}}$ for some n, and because $\mathrm{Nrd}_{L/\mathbb{Q}}$ is polynomial of degree $[L : \mathbb{Q}]$ we find that $[L : \mathbb{Q}]$ divides g. □

lbertRestrTable **(12.30)** As a corollary of the Proposition, we obtain that the following divisibility relations are satisfied.

	$\mathrm{char}(k) = 0$	$\mathrm{char}(k) = p$
Type I	$e \mid g$	$e \mid g$
Type II	$2e \mid g$	$2e \mid g$
Type III	$2e \mid g$	$e \mid g$
Type IV	$e_0 m^2 \mid g$	$e_0 m \mid g$

Table (12.30.1): numerical restrictions on the endomorphism algebra

Note that if X is of Type II, there exists a subfield $L \subset D$ with $L \subset D^{\mathrm{sym}}$ and $[L : K] = 2$. Indeed, as discussed in (12.28) we have $\dim_K(D^{\mathrm{sym}}) = 3$, and for any $\alpha \in D^{\mathrm{sym}} \setminus K$ we can take $L = K[\alpha]$. Now we apply (iii) of the Proposition with this L.

XlambdaDdagger **(12.31)** Still with the assumptions and notation of (12.29), the Albert type of $(D, \dagger)$ does not depend on the choice of a polarization λ, and we often say that X is of Type N, with $N \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}\}$, when $(D, \dagger)$ is. If X is of Type I or III then the isomorphism class of the pair $(D, \dagger)$ is independent of the choice of λ, simply because $\dagger$ is the canonical involution on D. In general, however, ????

The question arises if the conditions on the pair $(D, \dagger)$ that we have obtained are exhaustive. In other words, suppose we are given a characteristic $p \geqslant 0$, an integer $g > 0$, and a finite dimensional simple $\mathbb{Q}$-algebra D with a positive involution $\dagger$. Assume the condition given in Table (12.30.1) is satisfied. Then one may wonder if there exists a g-dimensional polarized abelian variety (X, λ) over a field k of the given characteristic such that the pair $\big(\mathrm{End}^0(X), \dagger\big)$ is isomorphic to the given pair $(D, \dagger)$. Though no complete answer is known in this generality, several further results are known, and in characteristic zero the picture is fairly complete. In particular, it is known that in characteristic 0 there always exists a polarized abelian variety

(X, λ) with the given $(D, \dagger)$, except possibly when X has Type III and $g/2e \in \{1, 2\}$ or when X has Type IV and $(g/e_0 m^2) \in \{1, 2\}$.

We refer to Oort [4] for a detailed overview. Over $\mathbb{C}$ the main results on this question are obtained in Shimura [1].

Let us here, by way of example, only show that an abelian surface X cannot be of Type III.

ngeofAlbertType **(12.32) Remark.** If $k \subset K$ is a field extension, X_K may be of a different type than X. For instance, the elliptic curve E over $\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 - x$ has $\mathrm{End}^0(E) = \mathbb{Q}$, whereas over $K = \mathbb{Q}[i]$ we have $\mathrm{End}^0(E_K) \cong \mathbb{Q}[i]$. So in this example, the type of E changes from I to IV. In general, if we start with a simple abelian variety X over k then X_K may no longer be simple. When X_K is again simple, it is clear that only certain changes of type are possible; e.g., if X is of Type II, III or IV then X_K cannot be of Type I. See Exercise 12.3.

Exercises.

Ex:Vlqisog **(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 $V_\ell(f)\colon V_\ell X \to V_\ell Y$ 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 $f[p^\infty]\colon X[p^\infty] \to Y[p^\infty]$ is an isogeny.

Ex:HomK/Homk **(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 $\mathrm{End}_k(X) = \mathrm{End}_K(X_K)$.

Ex:TypekTypeK **(12.3)** Let X be a simple abelian variety over a field k. Let $k \subset K$ be a field extension, and suppose X_K is again simple. If X has Type M in the Albert clasification and X_K has Type N (with M, $N \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}\}$) then we say we have the change of type $M \to N$.

(i) Show that a change of type $M \to \mathrm{I}$ is possible only if $M = \mathrm{I}$.

(i) Show that a change of type $M \to \mathrm{II}$ or $M \to \mathrm{III}$ is possible only if either $M = \mathrm{I}$ or $M = \mathrm{IV}$ and $m = 1$.

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; cf. Milne [1], proof of 12.1, for instance.

In this chapter we study the Chow ring of an abelian variety. For a nonsingular variety over a field the classes of cycles modulo rational equivalence form a ring with respect to the intersection product of cycles. For an abelian variety the Chow ring carries a second product, called the Pontryagin or convolution product. Here the product cycle is obtained, loosely speaking, by adding the points on the two cycles. These two aspects of the Chow ring are related by duality. The transition is provided by the Fourier transform, a transformation from the Chow ring of an abelian variety to the Chow ring of the dual abelian variety, under which the intersection product on the abelian variety corresponds to the convolution product on the dual. This Fourier transform is a wonderful tool for investigating the structure of the Chow ring of an abelian variety X. Using the Fourier transform one can decompose the diagonal correspondence in $X \times X$ as a sum of orthogonal idempotents. In the motivic language this gives a decomposition of the Chow motive of an abelian variety as $R(X) = \oplus_{i=0}^{2g} R^i(X)$, analogous to the decomposition $H^*(X) = \oplus_{i=0}^{2g} H^i(X)$ in cohomology. We close the chapter with a theorem of Künnemann which says that $R(X) \cong \wedge^* R^1(X)$.

Along the way we need some properties of the Chern classes of the Hodge bundle. These properties, like the so-called Key Formula and the vanishing of the top Chern class are of independent interest and are proved in section 2.

§1. *The Chow ring.*

We review some properties of the Chow ring and correspondences. An excellent reference book is Fulton [1]. Note that we are mainly interested in intersection theory on non-singular varieties, hence we do not need the theory developed in Fulton's book in its full strength.

CHdef **(13.1)** Let X be a variety over a field k. The group $Z_r(X)$ of r-cycles on X is defined as the free abelian group on the r-dimensional closed subvarieties of X. We usually write $[V] \in Z_r(X)$ for the element corresponding to a subvariety $V \subset X$. Thus, an r-cycle on X is a finite formal sum $\sum n_i \cdot [V_i]$ where the $V_i \subset X$ are closed subvarieties of dimension r and $n_i \in \mathbb{Z}$. For $r = \dim(X) - 1$ an r-cycle is the same as a Weil divisor.

In general, $Z_r(X)$ is a very big group. We arrive at a much more manageable group by taking the quotient modulo rational equivalence. This is done as follows. (Further details and proofs of some properties can be found in Fulton [1], Chap. 1.)

Let W be an $(r+1)$-dimensional subvariety of X. Let $V \subset W$ be a subvariety of codimension 1. The local ring $O_{W,V}$ of W along V is a 1-dimensional local domain with fraction field $k(W)$, the field of rational functions on W. (Note: V corresponds to a single point $x \in |W|$, and $O_{W,V}$ is just the stalk $O_{W,x}$ of O_W at x.) For $0 \neq a \in O_{W,V}$, define the order of vanishing of a along V to be the integer

$$\mathrm{ord}_V(a) := \mathrm{length}_{O_{W,V}} \Big(O_{W,V}/(a) \Big) .$$

We can extend this to a homomorphism $\mathrm{ord}_V\colon k(W)^* \to \mathbb{Z}$ by writing $f \in k(W)^*$ as $f = a/b$ with $a,\, b \in O_{W,V}$; then let $\mathrm{ord}_V(f) := \mathrm{ord}_V(a) - \mathrm{ord}_V(b)$. Note that if V is not contained in the singular locus of W then $O_{W,V}$ is a discrete valuation ring, and ord_V is just the valuation homomorphism.

Given $f \in k(W)^*$, there are only finitely many codimension 1 subvarieties $V \subset W$ such that $\mathrm{ord}_V(f) \neq 0$. This allows us to define an r-cycle on X, called the divisor of f on $W \subset X$, by

$$\mathrm{div}(f) := \sum_V \mathrm{ord}_V(f) \cdot [V]\,,$$

where the sum runs over the subvarieties $V \subset W$ of codimension 1.

An r-cycle $\alpha \in Z_r(X)$ is said to be rationally equivalent to zero, notation $\alpha \sim 0$ or $\alpha \sim_{\mathrm{rat}} 0$, if there exist $(r+1)$-dimensional subvarieties $W_1, \ldots, W_n$ of X and rational functions $f_i \in k(W_i)^*$ such that $\alpha = \sum_{i=1}^n \mathrm{div}(f_i)$. The cycles rationally equivalent to zero form a subgroup $\mathrm{Rat}_r(X)$ of $Z_r(X)$ and one defines the Chow group of r-cycles to be the factor group

$$\mathrm{CH}_r(X) := Z_r(X)/\mathrm{Rat}_r(X)\,.$$

We set $\mathrm{CH}^r(X) := \mathrm{CH}_{\dim(X)-r}(X)$; this is called the Chow group of codimension r cycles. Let

$$\mathrm{CH}^*(X) := \oplus_r \mathrm{CH}^r(X)\,, \qquad \text{and} \qquad \mathrm{CH}^*_{\mathbb{Q}}(X) := \mathrm{CH}^*(X) \otimes_{\mathbb{Z}} \mathbb{Q}\,.$$

It is a fundamental fact that for X a non-singular variety, there exists an intersection pairing

$$\mathrm{CH}^r(X) \times \mathrm{CH}^s(X) \to \mathrm{CH}^{r+s}(X)\,, \qquad (\alpha, \beta) \mapsto \alpha \cdot \beta$$

which makes $\mathrm{CH}^*(X)$ into a commutative graded ring with identity. This ring is called the *Chow ring* of X. The identity element is $1_X = [X] \in \mathrm{CH}^0(X)$. (If X is singular, there is still a good intersection theory, but this may not give a ring structure on $\mathrm{CH}^*(X)$. See Fulton [1].)

f*f*CH **(13.2)** Let $f\colon X \to Y$ be a morphism of k-varieties. Then we have a pull-back homomorphism $f^*\colon \mathrm{CH}^*(Y) \to \mathrm{CH}^*(X)$. If f is flat then f^* is given by $f^*[V] = [f^{-1}(V)]$. The definition in the general case requires a little more care; we refer to Fulton [1], Chap. 8 for details. If X and Y are non-singular then f^* is a homomorphism of graded rings.

Now assume that f is proper. Let V be a closed subvariety of X. Then $W = f(V)$ is a closed subvariety of Y. If $\dim(W) = \dim(V)$, let $\deg(V/W)$ be the degree of the function field extension $\big[k(V) : k(W)\big]$ defined by f; if $\dim(W) < \dim(V)$ let $\deg(V/W) := 0$. We set $f_*[V] = \deg(V/W)\cdot[W]$. By extending this linearly, we get a homomorphism $f_*\colon Z_r(X) \to Z_r(Y)$ which induces a homomorphism $f_*\colon \mathrm{CH}_r(X) \to \mathrm{CH}_r(Y)$.

For a proper morphism $f\colon X \to Y$ we have the *projection formula*

$$f_*(f^*\eta \cdot \xi) = \eta \cdot f_*\xi \qquad \text{for all } \xi \in \mathrm{CH}^*(X) \text{ and } \eta \in \mathrm{CH}^*(Y).$$

Furthermore, if

$$\begin{array}{ccc} X' & \xrightarrow{g} & X \\ {\scriptstyle f'}\big\downarrow & & \big\downarrow{\scriptstyle f} \\ Y' & \xrightarrow{h} & Y \end{array}$$

is a Cartesian square with h flat and f proper ("flat base change of a proper morphism"), then g is flat and f' is proper, and for all $\alpha \in \mathrm{CH}^*(X)$ we have

Chow:h*f*
$$f'_* g^* \alpha = h^* f_* \alpha. \tag{1}$$

Chernchar **(13.3)** Let X be a variety. Let $K^0(X)$ be the Grothendieck group of vector bundles on X. Then $K^0(X)$ has a natural structure of a commutative ring, with product $[E_1]\cdot[E_2] = [E_1 \otimes E_2]$. Let $K_0(X)$ be the Grothendieck group of coherent sheaves on X. Then $K_0(X)$ has a natural structure of a $K^0(X)$-module, by $[E]\cdot[F] = [E \otimes_{O_X} F]$. If $f\colon X \to Y$ is a morphism of varieties then we have a natural ring homomorphism $f^*\colon K^0(Y) \to K^0(X)$. If f is proper then we have a homomorphism $f_*\colon K_0(X) \to K_0(Y)$ given by $f_*[F] = \sum_{i\geqslant 0}(-1)^i\big[R^i f_* F\big]$.

Now assume X is non-singular. The natural homomorphism $K^0(X) \to K_0(X)$, sending a vector bundle to the corresponding O_X-module, is in this case an isomorphism. If there is no risk of confusion we simply write $K(X)$ for $K^0(X)$. Just as for the Chow ring, we have pull-backs f^* for arbitrary morphisms f between non-singular varieties, and push-forwards f_* for proper morphisms. We write $K_{\mathbb{Q}}(X) := K(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

There is a ring homomorphism

$$\mathrm{ch}\colon K(X) \to \mathrm{CH}^*_{\mathbb{Q}}(X),$$

called the *Chern character*. For a line bundle L with associated divisor class $\ell = c_1(L) \in \mathrm{CH}^1_{\mathbb{Q}}(X)$, it is given by

$$[L] \mapsto e^{\ell} := 1 + \ell + \frac{1}{2}\ell^2 + \frac{1}{3!}\ell^3 + \cdots .$$

(Note that e^{ℓ} only involves a finite sum, as $\mathrm{CH}^i(X) = 0$ for $i > \dim(X)$.) For further details about the definition of the Chern character, see Fulton [1], sections 3.2 and 15.1.

Still assuming that X is non-singular, the homomorphism $K_{\mathbb{Q}}(X) \to \mathrm{CH}^*_{\mathbb{Q}}(X)$ induced by the Chern character is an isomorphism. See Fulton [1], Example 15.2.16.

If $f\colon X \to Y$ is a morphism between non-singular varieties then the Chern character commutes with f^*, in the sense that $f^*\big(\mathrm{ch}(\alpha)\big) = \mathrm{ch}\big(f^*(\alpha)\big)$ for all $\alpha \in K(Y)$. But if f is proper then "ch" does *not*, in general, commute with f_*. The difference between $f_* \circ \mathrm{ch}$ and $\mathrm{ch} \circ f_*$ is made precise by the Grothendieck-Riemann-Roch theorem; see Fulton [1], Thm. 15.2.

Corresp **(13.4)** Let X and Y be non-singular varieties. Elements in $\mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ are called *correspondences* from X to Y. For a correspondence $\xi \in \mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ the transpose correspondence ${}^{\mathrm{t}}\xi$ from Y to X is defined as ${}^{\mathrm{t}}\xi := s_*(\xi)$, where $s\colon X \times Y \to Y \times X$ is the morphism reversing the factors.

Assume Y is complete. If Z is a third non-singular variety then we can compose correspondences: Given $\varphi \in \mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ and $\psi \in \mathrm{CH}^*_{\mathbb{Q}}(Y \times Z)$ we define their composition, which is a correspondence from X to Z, by

$$\psi \circ \varphi = p_{XZ,*}\big(p^*_{XY}(\varphi) \cdot p^*_{YZ}(\psi)\big) \quad \in \mathrm{CH}^*_{\mathbb{Q}}(X \times Z)\,.$$

Here p_{XZ} denotes the projection $X \times Y \times Z \to X \times Z$, and similarly for the other projections. We have ${}^{\mathrm{t}}(\psi \circ \varphi) = {}^{\mathrm{t}}\varphi \circ {}^{\mathrm{t}}\psi$.

If $f\colon X \to Y$ is a morphism with graph map $\gamma_f\colon X \to X \times Y$, then the correspondence $\Gamma_f = \big[\gamma_f(X)\big]$ in $\mathrm{CH}^*_{\mathbb{Q}}(X \times Y)$ is called the graph correspondence of f. Note that $\Gamma_f = \gamma_{f,*}[X]$. If $f\colon X \to Y$ and $g\colon Y \to Z$ then $\Gamma_g \circ \Gamma_f = \Gamma_{gf}$.

Assume X is complete. A correspondence Γ from X to Y gives rise to a homomorphism of groups $\gamma\colon \mathrm{CH}^*(X) \to \mathrm{CH}^*(Y)$ by

Chow:gammaDef
$$\gamma(\alpha) = p_{Y,*}\big(p_X^*(\alpha)\cdot\Gamma\big)\,, \tag{2}$$

where p_X and p_Y are the projections from $X\times Y$ to X and Y, respectively. If $\Gamma = \Gamma_f$ for some morphism f then $\gamma = f_*$. (Note that f is automatically proper, as we have assumed that X is complete.) If $\Gamma = {}^{\mathrm{t}}\Gamma_f$ then $\gamma = f^*$. If $\Gamma = \Gamma'\circ\Gamma''$ then for the associated homomorphisms we have $\gamma = \gamma'\circ\gamma''$.

We have a similar construction with Chow rings replaced by K-groups. So, if X is complete then an element $\Gamma\in K(X\times Y)$ gives rise to a homomorphism $\gamma_K\colon K(X)\to K(Y)$ by the same formula as in (2). Further we write $\gamma_{\mathrm{CH}}\colon \mathrm{CH}^*(X)\to\mathrm{CH}^*(Y)$ for the homomorphism associated to the correspondence $\mathrm{ch}(\Gamma)$ from X to Y.

CHoverS **(13.5)** We shall need a variant of the above relative to a given base variety. For this, let k be a field and let S be a smooth quasi-projective k-scheme. Consider the category $\mathscr{V}(S)$ of smooth projective S-schemes. Note that if $X\to S$ and $Y\to S$ are in $\mathscr{V}(S)$ then so is the fibre product $X\times_S Y\to S$. Note further that if $X\to S$ is in $\mathscr{V}(S)$ then X itself is again a smooth quasi-projective k-scheme. In particular this implies that X is geometrically regular. If $X = \amalg X_i$ is the decomposition of X as a union of its connected components then the X_i are k-varieties in the sense of Fulton [1] (but not in our sense, as they may not be geometrically irreducible) and we set $\mathrm{CH}^*(X) := \oplus\mathrm{CH}^*(X_i)$.

Let X and Y be two smooth projective S-schemes. Elements in $\mathrm{CH}^*_{\mathbb{Q}}(X\times_S Y)$ are called *relative correspondences* between X and Y. As before we can compose correspondences.

We shall make repeated use of the following lemma.

CorrIds **(13.6) Lemma.** *Suppose given morphisms $f\colon X\to Y$ and $g\colon Y\to Z$ in $\mathscr{V}(S)$ and classes $\alpha\in\mathrm{CH}^*_{\mathbb{Q}}(X\times_S Y)$ and $\beta\in\mathrm{CH}^*_{\mathbb{Q}}(Y\times_S Z)$. Then we have the identities of correspondences*

$$[\Gamma_g]\circ\alpha = (\mathrm{id}_X\times g)_*(\alpha)\,,\qquad \textit{and}\qquad \beta\circ[\Gamma_f] = (f\times\mathrm{id}_Z)^*(\beta)\,.$$

Similarly, if $f'\colon Y\to X$ and $g'\colon Z\to Y$ are also morphisms in $\mathscr{V}(S)$ then

$$[{}^{\mathrm{t}}\Gamma_{g'}]\circ\alpha = (\mathrm{id}_X\times g')^*(\alpha)\,,\qquad \textit{and}\qquad \beta\circ[{}^{\mathrm{t}}\Gamma_{f'}] = (f'\times\mathrm{id}_Z)_*(\beta)\,.$$

Proof. The first identities are proven as in Fulton [1], Prop. 16.1.1(c); the last two follow by transposition. □

The Grothendieck-Riemann-Roch theorem has a variant for correspondences. As usual we write $\mathrm{Td}(E)$ for the Todd class of a vector bundle E; see Fulton [1], Example 3.2.4.

GRRCorr **(13.7) Proposition.** (GRR) *Let X and Y be in $\mathscr{V}(S)$, with $X\to S$ proper. For $\Gamma\in K(X\times_S Y)$ with associated homomorphisms γ_K and γ_{CH}, we have*

$$\mathrm{ch}\big(\gamma_K(\alpha)\big) = p_{Y,*}\Big[p_X^*\big(\mathrm{ch}(\alpha)\big)\cdot\mathrm{ch}(\Gamma)\cdot\mathrm{Td}\big(p_X^*T_{X/S}\big)\Big]\,.$$

Proof. This follows from the usual GRR theorem (see Fulton [1], 15.2.8) applied to the morphism $p_Y\colon X \times Y \to Y$ and the element $p_X^*(\alpha)\cdot\Gamma$ of $K(X \times_S Y)$. One gets

$$\mathrm{ch}\big[p_{Y,*}\big(p_X^*(\alpha)\cdot\Gamma\big)\big] = p_{Y,*}\big[\mathrm{ch}\big(p_X^*(\alpha)\cdot\Gamma\big)\cdot\mathrm{Td}(T_{X\times Y/Y})\big]\,.$$

Now use the definition of $\gamma_K(\alpha)$, the fact that ch is a ring homomorphism, and that $T_{X\times Y/Y} = p_X^*T_{X/S}$. □

For an abelian scheme $\pi : X \to S$ the cotangent bundle Ω^1_X/S is a pull-back from a bundle $\mathbb{E}$ of rank g from the base S as it is trivial on the fibres. This is the Hodge bundle which we will consider more thoroughly in the next section.

GRRCorrAV **(13.8) Corollary.** *With S as in* (13.5)*, let $\xi\colon X \to S$ and $\eta\colon Y \to S$ be abelian schemes over S. Let $\mathbb{E}$ be the Hodge bundle of X/S. Let Γ be an element of $K(X \times_S Y)$ with associated homomorphisms γ_K and γ_{CH}. Then for $\alpha \in \mathrm{CH}^*_{\mathbb{Q}}(X)$ we have*

$$\mathrm{ch}\big(\gamma_K(\alpha)\big) = \gamma_{\mathrm{CH}}\big(\mathrm{ch}(\alpha)\big)\cdot\eta^*\mathrm{Td}(\mathbb{E}^\vee)\,.$$

In particular, if $S = \mathrm{Spec}(k)$ then the diagram

$$\begin{array}{ccc} K(X) & \xrightarrow{\mathrm{ch}} & \mathrm{CH}^*_{\mathbb{Q}}(X) \\ {\scriptstyle\gamma_K}\big\downarrow & & \big\downarrow{\scriptstyle\gamma_{\mathrm{CH}}} \\ K(Y) & \xrightarrow{\mathrm{ch}} & \mathrm{CH}^*_{\mathbb{Q}}(Y) \end{array}$$

is commutative.

Proof. We have $T_{X/S} = \xi^*\mathbb{E}^\vee$, so $p_X^*T_{X/S} = p_Y^*\eta^*\mathbb{E}^\vee$. The corollary now follows from (13.7) using the projection formula. □

§2. *The Hodge bundle.*

In this section we consider the Hodge bundle of an abelian scheme and prove several basic properties of its Chern classes.

HodgeBun **(13.9) Definition.** Let S be a quasi-projective non-singular variety over a field k. Let $\pi\colon X \to S$ be an abelian scheme over S of relative dimension g and with zero section s. The *Hodge bundle* $\mathbb{E} = \mathbb{E}_X$ of X is the vector bundle (locally free sheaf) $\pi_*(\Omega^1_{X/S})$ of rank g on S. By $\mathbb{E}^t$ we mean the Hodge bundle of the dual abelian scheme X^t. For $i = 1, \ldots, g$ we denote by $\lambda_i \in \mathrm{CH}^i(S)$ the i-th Chern class of $\mathbb{E}$ and by λ_i^t the i-th Chern class of $\mathbb{E}^t$.

Alternatively, the Hodge bundle $\mathbb{E}$ may be defined as $\mathbb{E} = s^*\omega_{X/S}$ and we can view it as the cotangent bundle to the zero section s. It satisfies $\pi^*(\mathbb{E}) \cong \Omega^1_{X/S}$. Note that we have

$$(\mathbb{E}^t)^\vee = \mathrm{Lie}(X^t) \cong R^1\pi_*O_X.$$

(13.9) Lemma. *We have* $\det(\mathbb{E}) \cong \det(\mathbb{E}^t)$*, i.e.* $\lambda_1^t = \lambda_1$.

Proof. Note that $R^g\pi_*O_X \cong \wedge^g R^1\pi_*O_X$, and by Grothendieck duality (see [1], Thm. ?? or ??) we have $R^g\pi_*O_X \cong R^0\pi_*(\Omega^g_{X/S})^\vee$, i.e., we get $\det(\mathbb{E}) \cong \det(\mathbb{E}^t)$. □

If X carries a separable polarization then the corresponding map $X \to X^t$ induces an isomorphism $\mathbb{E} \cong \mathbb{E}^t$. (Is there always an isomorphism??)

The Grothendieck-Riemann-Roch theorem allows us to obtain relations in the Chow ring of the base space. We apply this to an ample line bundle on an abelian variety.

BasicRel **(13.10) Theorem.** *Let S be a smooth quasi-projective scheme over k and $\pi : X \to S$ be an abelian scheme over S with zero section s. Furthermore, let L be a symmetric line bundle on X/S such that s^*L is trivial and giving a polarization on each fibre. If Θ is the divisor class in $\mathrm{CH}^1_{\mathbb{Q}}(X)$ representing L then we have the identity*

$$\pi_*(\sum_{k=0}^{\infty} \frac{\Theta^{g+k}}{(g+k)!}) = d \cdot 1 \qquad \text{in } CH^*_{\mathbb{Q}}(S),$$

where $d = \deg(\Theta^g/g!)$.

Proof. The idea is to apply the Grothendieck-Riemann-Roch theorem to L. Actually, before doing that we first replace X by $Y = X^4$, g by $g' = 4g$ and L by $M = L^{\otimes 4}$ (in shorthand using the exterior tensor product, i.e., $M = p_1^*L \otimes p_2^*L \otimes p_3^*L \otimes p_4^*L$). Then by the Zarhin Trick there exists for any $n \in \mathbb{Z}_{\geqslant 1}$ an isogeny of α: $Y \to Y$ over S such that $\alpha^*(M) \cong M^{\otimes n}$. Moreover, if H is the kernel of α (a finite flat group scheme of rank n^{4g} over S) then we claim that $\det(O_H)$ is a trivial O_S-module. To see this, note that α is given by an integral 4×4 matrix corresponding to a quaternion $z = a + bi + cj + dk$. Since z lies in a quadratic subfield of the quaternions, the kernel of α is a direct sum of an even number of copies of group schemes $X[m]$ for divisors m of n. Now $X[m]$ is self-dual, hence the square of the determinant of $O_{X[m]}$ is trivial. This implies that $\det(O_H)$ is trivial, cf. [Faltings-Chai, p. 25?]

Now we take an integer n prime to the degree of L. Then we have a direct sum decomposition $K(M^{\otimes n}) \cong K(M) \oplus Y[n]$ and a similar decomposition $G(M^{\otimes n}) \cong G(M) \oplus Y[n]$. Theorem (8.14) tells us that we can lift H to a level subgroup (again denoted by H) of $G(M^{\otimes n})$ (the theory works over base schemes as well). Let H^c be the commutator of H in $G(M^{\otimes n})$ so that H^c/H is isomorphic to $G(M)$ by (8.16). By the representation theory of the theta group we find

$$\pi_*(M^{\otimes n}) \cong \mathrm{Ind}_{H^c}^{G(M^{\otimes n})} \pi_*(M).$$

Restrict the representation to the inverse image of $Y[n]$ in $G(M^{\otimes n})$. Then it decomposes as $\pi_*(M)$ tensor a representation of $G(M^{\otimes n})$ induced from a rank 1 representation of H^c with the property that its n-th power extends to a representation of $G(M^{\otimes n})$. If we ignore elements of finite order (and we do because we work in $\mathrm{CH}^*_{\mathbb{Q}}(S)$) then we may conclude that the determinant of this representation is equal to $\det(O_H)$, hence trivial. We thus get

$$\mathrm{ch}(\pi_*(M^{\otimes n})) = n^{g'} \,\mathrm{ch}(\pi_*(M)) \qquad \text{in} \quad \mathrm{CH}^*_{\mathbb{Q}}(S). \tag{1}$$

The Grothendieck-Riemann-Roch theorem applied to $\pi : Y \to S$ and M says

$$\begin{aligned} \mathrm{ch}(\pi_! M^{\otimes n}) &= \pi_*(\mathrm{ch}(M^{\otimes n}) \cdot \mathrm{Td}(\Omega^\vee_{Y/S}) \\ &= \pi_*(\mathrm{ch}(M^{\otimes n}) \cdot \mathrm{Td}(\pi^*(\mathbb{E}_Y^\vee))) \\ &= \pi_*(\mathrm{ch}(M^{\otimes n})) \cdot \mathrm{Td}(\mathbb{E}_Y^\vee) \end{aligned}$$

by the projection formula. Here $\mathbb{E}_Y$ is the Hodge bundle of Y/S. Since $R^i\pi_*(M) = 0$ for $i > 0$ it follows that $\pi_!(M) = \pi_*(M)$ is a vector bundle.

The relation (1) now gives writing $e^{n\Theta'}$ for $\mathrm{ch}(M^{\otimes n})$:

$$\pi_*\left(\sum_{k=0}^{\infty}\frac{n^{g'+k}{\Theta'}^{g'+k}}{(g'+k)!}\right)\mathrm{Td}(\mathbb{E}_Y^\vee)=n^{g'}\pi_*\left(\sum_{k=0}^{\infty}\frac{{\Theta'}^{g'+k}}{(g'+k)!}\right)\mathrm{Td}(\mathbb{E}_Y^\vee).$$

Comparing coefficients of n^m and using that $\mathrm{Td}(\mathbb{E}_Y)=1+\ldots$ gives the result immediately for Y, M and Θ'. It is easy to derive it then for X, L and Θ. □.

(13.10) Corollary. *With L as in the Theorem we have $ch(\pi_!(L))=d\,\mathrm{Td}(\mathbb{E}^\vee)$.*

By comparing codimension 1 classes in the Grothendieck-Riemann-Roch formula applied to π and L as in 13.10

$$\mathrm{ch}(\pi_!L)=\pi_*(e^{\Theta})\mathrm{Td}(\mathbb{E}^\vee=d\,\mathrm{Td}(\mathbb{E}^\vee) \tag{2}$$

and using $\mathrm{Td}_1(\mathbb{E}^\vee)=-\lambda_1/2$ we find the following Corollary.

KeyFormula **(13.11) Corollary.** (Key Formula) *For L as in the theorem we have the formula in $\mathrm{CH}^1_{\mathbb{Q}}(S)$*

$$c_1(\pi_!L)=-\mathrm{rank}(\pi_*(L))\,\lambda_1/2.$$

By Zarhin's trick we know that for any abelian variety X/S the abelian variety $Y=(X\times_S X^t)^4$ carries a principal polarization L. This implies that $\pi_!L$ lives in degree 0 and is given by a line bundle $\pi_*(L)$, so

$$\mathrm{ch}(\pi_*(L))=e^{-\lambda_1(\mathbb{E}_Y)/2}.$$

On the other hand, equation (2) implies $\mathrm{ch}(\pi_*(L))=\mathrm{Td}(\mathbb{E}_Y^\vee)$. By comparing these we get the following corollary.

ToddRel **(13.12) Corollary.** *Let X/S be an abelian scheme over a smooth quasi-projective basis S. Then if $\lambda_i=c_i(\mathbb{E})$ we have in $\mathrm{CH}^*_{\mathbb{Q}}(S)$ the relation*

$$\mathrm{Td}(\mathbb{E}^\vee)\mathrm{Td}((\mathbb{E}^t)^\vee)=e^{-\lambda_1}.$$

If X carries a separable polarization then we have $\mathrm{Td}(\mathbb{E}^\vee)=e^{-\lambda_1/2}$.

Proof. Note that $\mathrm{Td}(\mathbb{E}_Y^\vee)=\mathrm{Td}(\mathbb{E}^\vee)^4\mathrm{Td}((\mathbb{E}^t)^\vee)^4$ and $\lambda_1(\mathbb{E}_Y)=4\lambda_1+4\lambda_1^t=8\lambda_1$ by (10.9). If X/S carries a separable polarization then we get a separable isogeny $X\to X^t$ inducing an isomorphism between $\mathbb{E}$ and $\mathbb{E}^t$. □

As a consequence of the basic relation deduced in 13.10 we get the following fundamental relation for the Chern classes of the Hodge bundle.

LambdaRel **(13.13) Theorem.** *If X/S carries a separable polarization then we have in $\mathrm{CH}^*_{\mathbb{Q}}(S)$ the relation*

$$(1+\lambda_1+\lambda_2+\ldots+\lambda_g)(1-\lambda_1+\ldots+(-1)^g\lambda_g)=1. \tag{3}$$

Proof. The relation $\mathrm{Td}(\mathbb{E}^\vee)=e^{-\lambda_1/2}$ implies that $\mathrm{Td}(\mathbb{E}\oplus\mathbb{E}^\vee)=1$. This again implies that if $\alpha_1,\ldots,\alpha_g$ are the Chern roots of $\mathbb{E}$ then

$$\prod_{i=1}^{g}\frac{\alpha_i}{e^{\alpha_i}-1}=\prod_{i=1}^{g}e^{-\alpha_i/2},$$

equivalently, that

$$\prod_{i=1}^{g}(e^{\alpha_i/2}-e^{-\alpha_i/2})=\prod_{i=1}^{g}\alpha_i$$

and this implies that the even degree power sums of the α_i vanish. This is easily see to be equivalent to $\mathrm{ch}(\mathbb{E}\oplus\mathbb{E}^\vee)=2g$ or to the relation (3). □

Another important result on the Hodge bundle deals with the top Chern class λ_g of $\mathbb{E}$ in the rational Chow group $\mathrm{CH}^g_{\mathbb{Q}}(S)$.

LambdagisZero **(13.14) Theorem.** *Let $\pi\colon X\to S$ be an abelian scheme of relative dimension g over the smooth quasi-projective scheme S. Then the top Chern class $\lambda_g\in\mathrm{CH}^g_{\mathbb{Q}}(S)$ of the Hodge bundle $\mathbb{E}$ vanishes.*

Proof. We apply the Grothendieck-Riemann-Roch theorem to the structure sheaf O_X and the morphism $\pi: X\to S$. It says

$$\mathrm{ch}(\pi_!(O_X))=\pi_*(\mathrm{ch}(O_X)\mathrm{Td}((\Omega^1_{X/S})^\vee))=\pi_*(1)\,\mathrm{Td}(\mathbb{E}^\vee),$$

since $\Omega^1_{X/S}=\pi^*(\mathbb{E})$. We know the cohomology of O_X:

$$\pi_!(O_X)=1-\mathbb{E}^\vee+\wedge^2\mathbb{E}^\vee-\ldots+(-1)^g\wedge^g\mathbb{E}^\vee.$$

We thus get the identity

$$\mathrm{ch}(1-\mathbb{E}^\vee+\wedge^2\mathbb{E}^\vee-\ldots+(-1)^g\wedge^g\mathbb{E}^\vee)=\pi_*(1)\mathrm{Td}(\mathbb{E}^\vee)=0.$$

A general relation, due to Borel and Serre 1, p. 128 says that for a vector bundle B of rank r one has

$$\sum_{j=0}^{r}(-1)^j\mathrm{ch}(\wedge^jB^\vee)=c_r(B)\,\mathrm{Td}(B)^{-1}.$$

So we see $\lambda_g\,\mathrm{Td}(\mathbb{E}^\vee)=0$. Since Td is invertible the result follows. □

§3. *The Fourier transform of an abelian variety.*

PontrProd **(13.15) Definition.** Let S be a quasi-projective non-singular variety over a field k. Let X be an abelian scheme over S with multiplication map $m\colon X\times_S X\to X$. The *Pontryagin product*, or *convolution product*

$$*\colon \mathrm{CH}^*(X)\times\mathrm{CH}^*(X)\longrightarrow\mathrm{CH}^*(X)$$

(relative to S) is the map defined by

$$\alpha*\beta=m_*(p_1^*\alpha\cdot p_2^*\beta)\,.$$

Intuitively, the product $\alpha*\beta$ is obtained by adding the points on cycles representing α and β. Note that the Pontryagin product depends on the base variety S, though this is not indicated in the notation.

PontrRing **(13.16) Lemma.** *Let $g=\dim(X/S)$. The Pontryagin product makes $\mathrm{CH}^*(X)=\oplus_i\mathrm{CH}^i(X)$ into a commutative ring for which the cycle $\big[e(S)\big]\in\mathrm{CH}^g(X)$ given by the identity section $e(S)\subset X$ is the identity element.*

The proof of this fact is straightforward and is left to the reader.

PprodPushf **(13.17) Lemma.** *Let $f\colon X \to Y$ be a homomorphism of abelian schemes over S. Then we have $f_*(\alpha * \beta) = f_*(\alpha) * f_*(\beta)$ for all α, $\beta \in \mathrm{CH}^*(X)$.*

Proof. Denote the projections of $X \times_S X$ (resp. $Y \times_S Y$, resp. $Y \times_S X$) on the two factors by p_i (resp. q_i, resp. r_i), $i = 1, 2$. Since $f \circ m_X = m_Y \circ (f \times f) = m_Y \circ (\mathrm{id}_Y \times f) \circ (f \times \mathrm{id}_X)$, we have

$$\begin{aligned} f_*(\alpha * \beta) &= f_* m_{X,*}(p_1^*\alpha \cdot p_2^*\beta) \\ &= m_{Y,*}(\mathrm{id}_Y \times f)_*(f \times \mathrm{id}_X)_*(p_1^*\alpha \cdot p_2^*\beta) \\ &= m_{Y,*}(\mathrm{id}_Y \times f)_*\big(p_1^*\alpha \cdot (f \times \mathrm{id}_X)^* r_2^*\beta\big) \\ &= m_{Y,*}(\mathrm{id}_Y \times f)_*\big((f \times \mathrm{id}_X)_* p_1^*\alpha \cdot r_2^*\beta\big), \end{aligned}$$

where in the last step we use the projection formula. Applying (1) to the Cartesian diagram

$$\begin{array}{ccc} X \times_S X & \xrightarrow{f \times \mathrm{id}_X} & Y \times_S X \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle r_1} \\ X & \xrightarrow{f} & Y \end{array}$$

gives that

$$(f \times \mathrm{id}_X)_* p_1^*\alpha = r_1^* f_*\alpha = \big(q_1 \circ (\mathrm{id}_Y \times f)\big)^* f_*\alpha = (\mathrm{id}_Y \times f)^* q_1^* f_*\alpha\,.$$

Again using the projection formula, this gives $f_*(\alpha * \beta) = m_{Y,*}\big(q_1^* f_*\alpha \cdot (\mathrm{id}_X \times f)_* r_2^*\beta\big)$. Finally we apply (1) to the Cartesian diagram

$$\begin{array}{ccc} Y \times_S X & \xrightarrow{\mathrm{id}_Y \times f} & Y \times_S X \\ {\scriptstyle r_2}\downarrow & & \downarrow{\scriptstyle q_2} \\ X & \xrightarrow{f} & Y \end{array}\quad.$$

This gives the desired conclusion that $f_*(\alpha * \beta) = m_{Y,*}(q_1^* f_*\alpha \cdot q_2^* f_*\beta) = f_*\alpha * f_*\beta$. □

We now come to the main notion of this chapter.

FourTDef **(13.18) Definition.** Situation as in (13.15). Let $\ell = c_1(\mathscr{P}_X) \in \mathrm{CH}^1(X \times_S X^t)$ be the class of the Poincaré bundle of X. We define the *Fourier transform* T of X as the correspondence from X to X^t given by

$$T = \mathrm{ch}(\mathscr{P}) = \exp(\ell) = 1 + \ell + \frac{1}{2!}\ell^2 + \cdots \quad \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X^t)\,.$$

We write

$$\tau_K\colon K(X) \longrightarrow K(X^t) \qquad \text{and} \qquad \tau = \tau_{\mathrm{CH}}\colon \mathrm{CH}^*_{\mathbb{Q}}(X) \longrightarrow \mathrm{CH}^*_{\mathbb{Q}}(X^t)$$

for the homomorphisms associated to the element $[\mathscr{P}] \in K(X \times_S X^t)$, as explained in (13.4). Concretely,

$$\begin{aligned} &\tau_K(x) = p_{X^t,*}(\mathscr{P} \cdot p_X^* x) && \text{for } x \in K(X); \\ &\tau_{\mathrm{CH}}(x) = p_{X^t,*}(e^\ell \cdot p_X^* x) = p_{X^t,*}(T \cdot p_X^* x) && \text{for } x \in \mathrm{CH}^*_{\mathbb{Q}}(X). \end{aligned}$$

tau(1) **(13.19) Proposition.** *Let X/S be an abelian scheme of relative dimension g. Let $\xi^t\colon X^t \to S$ with zero section $e^t\colon S \to X^t$ be the dual abelian scheme. Then we have*

$$\tau_{\mathrm{CH}}(1_X) = (-1)^g \cdot e^t_*(1_S)$$

in $\mathrm{CH}^*_{\mathbb{Q}}(X^t)$.

Proof. Let $\mathbb{E}$ and $\mathbb{E}^t$ be the Hodge bundles of X/S and X^t/S, respectively. By (13.8) we have

Chow:chtau01
$$\mathrm{ch}\big(\tau_K[O_X]\big) = \tau_{\mathrm{CH}}(1_X) \cdot \xi^{t,*}\mathrm{Td}(\mathbb{E}^\vee)\,. \tag{3}$$

On the other hand we can calculate $\tau_K(1_X) = \tau_K[O_X]$ directly. Namely,

$$\begin{aligned}\tau_K[O_X] = p_{X^t,*}\big(\mathscr{P} \cdot p_X^*[O_X]\big) = p_{X^t,*}(\mathscr{P}) &= \sum_{i=0}^{g}(-1)^i \cdot [R^i p_{X^t,*}\mathscr{P}] \\ &= (-1)^g \cdot e^t_*\big(\det(\mathbb{E}^t)^{-1}\big) \\ &= (-1)^g \cdot e^t_*(O_S) \cdot \xi^{t,*}\det(\mathbb{E}^t)^{-1}\,,\end{aligned}$$

according to our calculation of the cohomology of the Poincaré bundle $\mathscr{P}$. Now we apply GRR to the morphism $e\colon S \to X^t$. This gives

$$\mathrm{ch}\big(e^t_*(O_S)\big) \cdot \mathrm{Td}(T_{X^t}) = e^t_*\big(\mathrm{Td}(T_S)\big)\,,$$

hence

$$\mathrm{ch}\big(\tau_K[O_X]\big) = (-1)^g \cdot e^t_*\big(\mathrm{Td}(T_S)\big) \cdot \mathrm{Td}(T_{X^t})^{-1} \cdot \xi^{t,*}\mathrm{ch}\big(\det(\mathbb{E}^t)\big)\,.$$

We have an exact sequence $0 \to \xi^{t,*}\mathbb{E}^{t,\vee} \to T_{X^t} \to \xi^{t,*}T_S \to 0$. This gives the relation $\mathrm{Td}(T_{X^t}) = \xi^{t,*}\mathrm{Td}(\mathbb{E}^{t,\vee}) \cdot \xi^{t,*}\mathrm{Td}(T_S)$. Since $e^{t,*} \circ \xi^{t,*} = \mathrm{id}$ we get, using the projection formula,

$$e^t_*\big(\mathrm{Td}(T_S)\big) \cdot \mathrm{Td}(T_{X^t})^{-1} = e^t_*\big(\mathrm{Td}(\mathbb{E}^{t,\vee})^{-1}\big) = e^t_*(1_S) \cdot \xi^{t,*}\mathrm{Td}(\mathbb{E}^{t,\vee})^{-1}\,.$$

In total this gives

Chow:chtau02
$$\mathrm{ch}\big(\tau_K[O_X]\big) = (-1)^g \cdot e^t_*(1_S) \cdot \xi^{t,*}\Big[\mathrm{Td}(\mathbb{E}^{t,\vee})^{-1} \cdot \mathrm{ch}\big(\det(\mathbb{E}^t)\big)^{-1}\Big]\,. \tag{4}$$

Let $\lambda_1 = c_1(\mathbb{E})$ and $\lambda_1^t = c_1(\mathbb{E}^t)$. As shown in 13.12 we have $\mathrm{Td}(\mathbb{E}^\vee)\mathrm{Td}((\mathbb{E}^t)^\vee) = \exp(-\lambda_1/2 - \lambda_1^t/2)$ and as we remarked in the beginning of section 2 we have $\lambda_1 = \lambda_1^t$. Comparison of the two expressions (3) and (4) gives the desired identity. □

Let T^t be the Fourier transform of X^t. It is associated to the Poincaré bundle on $X^t \times X^{tt}$. If we apply the isomorphism $\kappa_X\colon X \xrightarrow{\sim} X^{tt}$ then T^t can be identified with the transpose of the correspondence T.

FourAndHom **(13.20) Proposition.** *Let $f\colon X \to Y$ be a homomorphism of abelian schemes over S. Then $T_Y \circ [\Gamma_f] = [{}^{\mathrm{t}}\Gamma_{f^t}] \circ T_X$ in $\mathrm{CH}^*_{\mathbb{Q}}(X \times_S Y^t)$. If f is an isogeny then we further have the relation $T_X \circ [{}^{\mathrm{t}}\Gamma_f] = [\Gamma_{f^t}] \circ T_Y$ in $\mathrm{CH}^*_{\mathbb{Q}}(Y \times_S X^t)$.*

Proof. Lemma (13.6) gives $T_Y \circ [\Gamma_f] = (f \times \mathrm{id}_{Y^t})^*\mathrm{ch}(\mathscr{P}_Y)$ and $[{}^{\mathrm{t}}\Gamma_{f^t}] \circ T_X = (\mathrm{id}_X \times f^t)^*\mathrm{ch}(\mathscr{P}_X)$. So for the first assertion we have to show that

Chow:1xf*chP
$$(f \times \mathrm{id}_{Y^t})^*\mathrm{ch}(\mathscr{P}_Y) = (\mathrm{id}_X \times f^t)^*\mathrm{ch}(\mathscr{P}_X)\,. \tag{5}$$

But the dual f^t of f is defined by the identity $(\mathrm{id}_X \times f^t)^*(\mathscr{P}_X) = (f \times \mathrm{id}_{Y^t})^*(\mathscr{P}_Y)$. Applying the Chern character we get (5).

In a similar way, again using (13.6), the second assertion is equivalent to

Chow:fx1*chP
$$(f \times \mathrm{id}_{X^t})_* \mathrm{ch}(\mathscr{P}_X) = (\mathrm{id}_Y \times f^t)_* \mathrm{ch}(\mathscr{P}_Y)\,. \tag{6}$$

We use the Cartesian diagram

$$\begin{array}{ccc} X \times_S Y^t & \xrightarrow{\mathrm{id}_X \times f^t} & X \times_S X^t \\ {\scriptstyle f\times \mathrm{id}_{Y^t}}\big\downarrow & & \big\downarrow{\scriptstyle f\times \mathrm{id}_{X^t}} \\ Y \times_S Y^t & \xrightarrow{\mathrm{id}_Y \times f^t} & Y \times_S X^t \end{array}\quad .$$

This gives the identity

$$\begin{aligned} (\mathrm{id}_Y \times f^t)^*(f \times \mathrm{id}_{X^t})_* \mathrm{ch}(\mathscr{P}_X) &= (f \times \mathrm{id}_{Y^t})_* (\mathrm{id}_X \times f^t)^* \mathrm{ch}(\mathscr{P}_X) \\ &= (f \times \mathrm{id}_{Y^t})_* (f \times \mathrm{id}_{Y^t})^* \mathrm{ch}(\mathscr{P}_Y) \qquad \text{by (5)} \\ &= \deg(f) \mathrm{ch}(\mathscr{P}_Y)\,. \end{aligned}$$

Applying $(\mathrm{id}_Y \times f^t)_*$ to both sides gives $\deg(f^t)(f \times \mathrm{id}_{X^t})_* \mathrm{ch}(\mathscr{P}_X) = \deg(f)(\mathrm{id}_Y \times f^t)_* \mathrm{ch}(\mathscr{P}_Y)$, and if f is an isogeny then (6) follows because $\deg(f^t) = \deg(f) \neq 0$. □

CIdsThm **(13.21) Theorem.** *Let $m\colon X \times_S X \to X$ and $m^t\colon X^t \times_S X^t \to X^t$ be the group laws of X and X^t, respectively, let $\Delta\colon X \to X \times_S X$ and $\Delta^t\colon X^t \to X^t \times_S X^t$ be the diagonal morphisms, and let $T \otimes T$ denote the Fourier transform of $X \times_S X$. Then we have identities of correspondences*

$$\begin{aligned} T^t \circ T &= (-1)^g \cdot [{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_X}] && \text{in} \quad \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)\,; \\ T \circ [\Gamma_m] &= [{}^{\mathrm{t}}\Gamma_{\Delta^t}] \circ (T \otimes T) && \text{in} \quad \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X \times_S X^t)\,; \\ T \circ [{}^{\mathrm{t}}\Gamma_\Delta] &= (-1)^g \cdot [\Gamma_{m^t}] \circ (T \otimes T) && \text{in} \quad \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X \times_S X^t)\,. \end{aligned}$$

Proof. For the second identity one applies the previous proposition to the homomorphism m. (Use Exercise 7.1.)

Next remark that, by definition, the correspondence $T^t \circ T$ on $X \times_S X$ is

$$p_{13,*}(p_{12}^* e^{\ell} \cdot p_{23}^* e^{\ell^t}) = p_{13,*}\big(\exp(p_{12}^*\ell + p_{23}^*\ell^t)\big)\,.$$

Let $\mu\colon X \times_S X^t \times_S X \to X \times_S X^t$ be the homomorphism given on points by $(a,b,c) \mapsto (a+c,b)$ and let $s\colon X \times_S X^t \to X^t \times_S X$ be the map reversing the factors. Let $\mathscr{P}$ be the Poincaré bundle on $X \times_S X^t$. In $\mathrm{Pic}_{(X \times_S X^t \times_S X)/S}$ we have the identity

Chow:XXtXeq
$$p_{12}^*(\mathscr{P}) + p_{23}^* s^*(\mathscr{P}) = \mu^*(\mathscr{P})\,, \tag{7}$$

as follows from the Theorem of the Cube by checking that the two sides have the same restrictions to $X \times_S X^t \times e(S)$, to $X \times e(S) \times X$ and to $e(S) \times X^t \times X$. So we find that $T^t \circ T = p_{13,*}(e^{\mu^*(\ell)}) = p_{13,*}(\mu^* e^{\ell})$. From the Cartesian diagram

$$\begin{array}{ccc} X \times_S X^t \times_S X & \xrightarrow{\mu} & X \times_S X^t \\ {\scriptstyle p_{13}}\big\downarrow & & \big\downarrow{\scriptstyle p_1} \\ X \times_S X & \xrightarrow{m} & X \end{array}$$

we get $T^t \circ T = m^* p_{1,*}(e^\ell) = m^* \tau^t_{\mathrm{CH}}(1_{X^t})$. Application of Prop. (13.19) then gives $T^t \circ T = (-1)^g m^* e_*(1_S)$. But by the Cartesian square

$$\begin{array}{ccc} X & \xrightarrow{(\mathrm{id}_X, -\mathrm{id}_X)} & X \times X \\ \big\downarrow & & \big\downarrow m \\ \mathrm{Spec}(k) & \xrightarrow{\quad e \quad} & X \end{array}$$

we get $m^* e_*(1_S) = \Gamma_{-\mathrm{id}_X}$. This proves the first identity.

For the third identity, start from the relation

$$T^t \circ [\Gamma_{m^t}] = [{}^{\mathrm{t}}\Gamma_\Delta] \circ (T^t \otimes T^t)\,,$$

which is the second identity for X^t. Multiply by T from the left, by $(T \otimes T)$ from the right, and use the first identity (both for X^t and for $X \times_S X$). This gives

$$\begin{aligned} (-1)^g \cdot [{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_{X^t}}] \circ [\Gamma_{m^t}] \circ (T \otimes T) &= T \circ [{}^{\mathrm{t}}\Gamma_\Delta] \circ [{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_{X\times X}}] \\ &= T \circ [{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_X}] \circ [{}^{\mathrm{t}}\Gamma_\Delta]\,. \end{aligned}$$

Now observe that $T \circ [{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_X}] = [{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_{X^t}}] \circ T$, because both equal $\exp(-\ell)$. Since $[{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_{X^t}}] = [\Gamma_{-\mathrm{id}_{X^t}}]$ is a unit in the ring of correspondences from X^t to itself, this proves the third identity. □

CorrIdsCor **(13.22) Corollary.** *Situation as in* (13.15). *Let* $g = \dim(X/S)$.

(i) *We have* $\tau^t_{\mathrm{CH}} \circ \tau_{\mathrm{CH}} = (-1)^g (-\mathrm{id}_X)^*$. *For all* $x,\ y \in \mathrm{CH}^*_{\mathbb{Q}}(X)$ *we have the relations* $\tau_{\mathrm{CH}}(x * y) = \tau_{\mathrm{CH}}(x) \cdot \tau_{\mathrm{CH}}(y)$ *and* $\tau_{\mathrm{CH}}(x \cdot y) = (-1)^g \tau_{\mathrm{CH}}(x) * \tau_{\mathrm{CH}}(y)$.

(ii) *For a homomorphism* $f\colon X \to Y$ *we have* $\tau_Y \circ f_* = f^{t,*} \circ \tau_X$. *If* f *is an isogeny then also* $\tau_X \circ f^* = f^t_* \circ \tau_Y$.

Proof. These relations follow directly from Prop. (13.20) and Thm. (13.21). For example, for ii) note that $T \circ [\Gamma_m]$ induces a map $\mathrm{CH}^*_{\mathbb{Q}}(X \times_S X) \to \mathrm{CH}^*_{\mathbb{Q}}(X^t)$ with $p_1^*\alpha \cdot p_2^*\beta \mapsto \tau m_*(p_1^*\alpha \cdot p_2^*\beta) = \tau(\alpha * \beta)$. On the other hand, since $P_{X\times_S X} = p_1^* P_X \otimes p_2^* P_X$ we have

$$\begin{aligned} \tau_{X\times_S X}(p_1^*\alpha \cdot p_2^*\beta) &= p_{X^t \times_S X^t}(p_1^*(\alpha \cdot P_X) p_2^*(\beta \cdot P_X)) \\ &= p_1'^*(\tau(\alpha) \cdot p_2'^*(\tau(\beta)) \end{aligned}$$

with p_i' the projections of $X^t \times_S X^t$ onto its factors. Now $[{}^t\Gamma_{\Delta^t}]$ induces $(\Delta^t)^*$ so that $[{}^t\Gamma_{\Delta^t}] \circ T \otimes T$ induces a map sending $p_1^*(\alpha) \cdot p_2^*(\beta)$ to $\tau(\alpha) \cdot \tau(\beta)$. □

As another corollary we obtain the following elegant result.

CHXCHXt **(13.23) Theorem.** *The Fourier transform of* X *induces an isomorphism of rings*

$$\tau = \tau_{\mathrm{CH}}\colon \big(\mathrm{CH}^*_{\mathbb{Q}}(X), *\big) \xrightarrow{\sim} \big(\mathrm{CH}^*_{\mathbb{Q}}(X^t), \cdot\big)\,,$$

where $\cdot$ *and* $*$ *denote the intersection product and the convolution product, respectively.*

This theorem should justify the name Fourier transform. Just like the Fourier transform for functions on the real line which transform the convolution product into the usual product our Fourier transform interchanges the Pontryagin product, which one can see as a sort of convolution product, with the usual intersection product.

Gammax **(13.24)** For any reasonable cohomology theory with a Künneth formula, Poincaré duality and a cycle class map we have for an abelian variety X of dimension g

$$H^{2g}(X \times_k X) = \bigoplus_{i=0}^{2g} H^{2g-i}(X) \otimes_L H^i(X) = \bigoplus_{i=0}^{2g} H^i(X)^\vee \otimes_L H^i(X) = \bigoplus_{i=0}^{2g} \mathrm{End}_L\big(H^i(X)\big)\,.$$

The diagonal class $cl(\Delta_X) \in H^{2g}(X \times_k X)$ corresponds to the element $\oplus \mathrm{id}_{H^i(X)}$. Hence we can write

$$cl(\Delta_X) = \gamma_0 + \gamma_1 + \cdots + \gamma_{2g}\,,$$

with $\gamma_i \in \mathrm{End}_L\big(H^i(X)\big)$. The classes γ_i are called the Künneth components of the diagonal. Standard conjectures, as discussed for instance in Kleiman [1], predict that these classes are algebraic. That is, there should exist codimension g cycles D_i on $X \times_k X$ such that $[\Delta_X] = D_0 + D_1 + \cdots + D_{2g}$ and $cl(D_i) = \gamma_i$. The main result of this section establishes the existence of such algebraic classes.

Throughout this section, let S be a smooth connected quasi-projective scheme of dimension d over a field k. We consider an abelian scheme $f\colon X \to S$ of relative dimension g. Recall that if $\xi \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)$ then we define its transpose ${}^t\xi \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)$ by ${}^t\xi := s_*(\xi)$, where $s\colon X \times_S X \to X \times_S X$ is the automorphism switching the two factors.

If $x \in X(S)$ is a section of f, we define the graph class $[\Gamma_x]$ of x by

$$[\Gamma_x] := x_*[S] = \big[x(S)\big] \in \mathrm{CH}^g_{\mathbb{Q}}(X)\,.$$

In particular, $[\Gamma_e]$ is the identity element of $\mathrm{CH}^*_{\mathbb{Q}}(X)$ for the Pontryagin product.

Further, let $i_x := x \times 1_{X^t}\colon S \times_S X^t \to X \times_S X^t$, and consider the pull-back $i_x^*(\ell) \in \mathrm{CH}^1_{\mathbb{Q}}(X^t)$ of the class of the Poincaré bundle. The following two formulas, due to Beauville, give relations between $i_x^*(\ell)$ and the graph classes $[\Gamma_x]$.

BeauvForms **(13.25) Lemma.** *For all $x \in X(S)$ we have*

$$\tau\big([\Gamma_x]\big) = \exp(i_x^*\ell) \qquad \textit{and} \qquad \tau^t(i_x^*\ell) = (-1)^{g+1} \sum_{j=1}^{g+d} \frac{(-1)^j}{j} \cdot \big([\Gamma_x] - [\Gamma_e]\big)^{*j}\,.$$

Proof. We have $\tau\big([\Gamma_x]\big) = p_{X^t *}(p_X^* x_*[S] \cdot e^\ell) = p_{X^t *} i_{x*}\big([X^t] \cdot i_x^* e^\ell\big) = e^{i_x^*\ell}$. This proves the first relation. Further, in $\mathrm{CH}^*_{\mathbb{Q}}(X^t)$ we have the identity

$$i_x^*\ell = \log\big(1 - (1 - e^{i_x^*\ell})\big) = -\sum_{j=1}^{\infty} \frac{1}{j}(1 - e^{i_x^*\ell})^j\,.$$

Note that for dimension reasons a term of the form $\big(1 - \exp(i_x^*\ell)\big)^j$ vanishes for $j > \dim X^t = g + d$. By our first identity and Cor. (13.22) we have

$$\tau^t\big((1 - e^{i_x^*\ell})^j\big) = \tau^t \circ \tau\Big(\big([\Gamma_e] - [\Gamma_x]\big)^{*j}\Big) = (-1)^g(-1)^j\big([\Gamma_x] - [\Gamma_e]\big)^{*j}\,,$$

and combining this with the previous formula this gives the second relation. □

GamxGamy **(13.26) Lemma.** *For x, $y \in X(S)$ we have $[\Gamma_x] * [\Gamma_y] = [\Gamma_{x+y}]$.*

Proof. By the Theorem of the Square, $i^*_{x+y}\ell = i^*_x\ell + i^*_y\ell$. This implies that $\tau\big([\Gamma_x] * [\Gamma_y]\big) = \tau\big([\Gamma_x]\big)\tau\big([\Gamma_y]\big) = e^{i^*_x\ell}e^{i^*_y\ell} = e^{i^*_x\ell + i^*_y\ell} = \tau\big([\Gamma_{x+y}]\big)$. Now apply Thm. (13.23). □

These formulas can be used to deduce a vanishing property. Let $I(X/S)$ be the $\mathbb{Q}$-subspace of $\mathrm{CH}^g_{\mathbb{Q}}(X)$ generated by the elements $[\Gamma_x] - [\Gamma_e]$ for all $x \in X(S)$. By Lemma (13.26), $I(X/S)$ is a subring of $\mathrm{CH}^g_{\mathbb{Q}}(X)$ with respect to the ring structure defined by the Pontryagin product.

IXSbound **(13.27) Proposition.** *Let $d = \dim(S)$ and $g = \dim(X/S)$. Then $I(X/S)^{*(g+d+1)} = 0$.*

Proof. The Fourier transform of a product

$$\big([\Gamma_{x_1}] - [\Gamma_e]\big) * \big([\Gamma_{x_2}] - [\Gamma_e]\big) * \cdots * \big([\Gamma_{x_n}] - [\Gamma_e]\big)$$

equals $(\exp(i^*_{x_1}\ell)-1)\cdot(\exp(i^*_{x_2}\ell)-1)\cdots(\exp(i^*_{x_n}\ell)-1)$, and for dimension reasons this expression vanishes if $n > \dim(X^t) = g + d$. By Thm. (13.23) the result follows. □

In view of Lemma (13.25) we now put

$$\log\big([\Gamma_x]\big) := (-1)^{g+1} \cdot \tau^t(i^*_x\ell)\,.$$

This is a well-defined element of $I(X/S)$.

XSIXShom **(13.28) Corollary.** *The map $X(S) \to I(X/S)$ given by $x \mapsto \log\big([\Gamma_x]\big)$ is a group homomorphism.*

Proof. This follows from the identity of formal power series $\log\big((1+x)(1+y)\big) = \log(1+x) + \log(1+y)$. □

DenMurre **(13.29) Theorem.** (Deninger, Murre) *There is a unique decomposition of the class of the diagonal in $\mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)$,*

$$[\Delta_{X/S}] = \sum_{i=0}^{2g} \pi_i \tag{8}$$

FourChow:DDec

such that

$$\pi_i \circ \pi_j = \begin{cases} 0 & \text{if } i \neq j, \\ \pi_i & \text{if } i = j, \end{cases}$$

and such that

$$[{}^{\mathrm{t}}\Gamma_{n_X}] \circ \pi_i = n^i \pi_i \qquad \text{for all } n \in \mathbb{Z}\,. \tag{9}$$

FourChow:Gnpii

Moreover,

(i) $\pi_i \circ [{}^{\mathrm{t}}\Gamma_{n_X}] = n^i \pi_i$ *for all* $n \in \mathbb{Z}$;

(ii) ${}^{\mathrm{t}}\pi_i = \pi_{2g-i}$;

(iii) *if* $f\colon X \to Y$ *is a homomorphism then* $[{}^{\mathrm{t}}\Gamma_f] \circ \pi_{i,Y} = \pi_{i,X} \circ [{}^{\mathrm{t}}\Gamma_f]$.

Proof. First we prove unicity. Suppose $\{\pi'_i\}$ is another collection of elements satisfying (8) and (9). Then $\sum_{i=0}^{2g} n^i(\pi_i - \pi'_i) = 0$ for every integer n; hence $\pi_i = \pi'_i$ for every i.

Let us consider $X \times_S X$ as an abelian scheme over X via $p_1\colon X \times_S X \to X$. We also consider the convolution product on $\mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)$ relative to the base scheme X. If $n \in \mathbb{Z}$ then the morphism $X \to X \times_S X$ given by $x \mapsto (x, nx)$ is a section of $X \times_S X$ over X; its

graph class is none other than the class $[\Gamma_{n_X}] \in \mathrm{CH}^g_{\mathbb{Q}}(X \times_S X)$ of the graph of n_X. If there is no risk of confusion we simply write $[\Gamma_n]$ for this class. In particular, $[\Gamma_{\mathrm{id}}] = [\Gamma_1] = [\Delta]$ and $[\Gamma_e] = [\Gamma_0] = [X \times e(S)]$. (Here the "$e$" in Γ_e has to be interpreted as the identity section of $X \times_S X$ over X.)

For $i \leqslant 2g$, define $\pi_i \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)$ by

$$\pi_i := \frac{1}{(2g-i)!} \log\bigl([\Gamma_{\mathrm{id}}]\bigr)^{*(2g-i)} = \frac{1}{(2g-i)!} \Bigl(\sum_{j=1}^{\infty} \frac{(-1)^{j-1}}{j} \bigl([\Gamma_{\mathrm{id}}] - [\Gamma_e]\bigr)^{*j}\Bigr)^{*(2g-i)} .$$

Note that $\pi_i = 0$ for $i < -d$ and $\pi_{2g} = \bigl[X \times e(S)\bigr]$. By the identity $\exp\bigl(\log(1+x)\bigr) = 1 + x$ of formal power series we have

$$[\Delta] = [\Gamma_{\mathrm{id}}] = \sum_{i=-d}^{2g} \pi_i \,. \tag{10}$$

FourChow:DDec2

By Lemmas (13.6) and (13.17) we have $[\Gamma_n] \circ (\alpha * \beta) = \bigl([\Gamma_n] \circ \alpha\bigr) * \bigl([\Gamma_n] \circ \beta\bigr)$. Combining this with (13.26) and (13.28) we get

$$\begin{aligned} [\Gamma_n] \circ \pi_i &= \frac{1}{(2g-i)!} \log\bigl([\Gamma_n]\bigr)^{*(2g-i)} \\ &= \frac{1}{(2g-i)!} \log\bigl([\Gamma_{\mathrm{id}}]^{*n}\bigr)^{*(2g-i)} \\ &= \frac{1}{(2g-i)!} \bigl(n \, \log([\Gamma_{\mathrm{id}}])\bigr)^{*(2g-i)} = n^{2g-i} \pi_i \,. \end{aligned} \tag{11}$$

FourChow:Gnpii2

So we have $[\Gamma_n] = [\Gamma_n] \circ \Delta = [\Gamma_n] \circ \sum_{i=-d}^{2g} \pi_i = \sum_{i=-d}^{2g} n^{2g-i} \pi_i$; hence $n^{2g-j} \pi_j = [\Gamma_n] \circ \pi_j = \sum_{i=-d}^{2g} n^{2g-i} \pi_i \circ \pi_j$. As this holds for every integer n, it follows that

$$\pi_i \circ \pi_j = \begin{cases} 0 & \text{if } i \neq j, \\ \pi_j & \text{if } i = j. \end{cases}$$

From the relation $[\Gamma_n] = \sum n^{2g-j} \pi_j$ we get that $\pi_i \circ [\Gamma_n] = n^{2g-i} \pi_i$. Furthermore, we have $[\Gamma_n] \circ [{}^{\mathrm{t}}\Gamma_n] = n^{2g} \Delta$, and so $n^{2g-i} \pi_i \circ [{}^{\mathrm{t}}\Gamma_n] = \pi_i \circ [\Gamma_n] \circ [{}^{\mathrm{t}}\Gamma_n] = n^{2g} \pi_i$. We find that $[\Gamma_n] \circ {}^{\mathrm{t}}\pi_i = {}^{\mathrm{t}}\bigl(\pi_i \circ [{}^{\mathrm{t}}\Gamma_n]\bigr) = n^i \cdot {}^{\mathrm{t}}\pi_i$. Now remark that the relations (10) and (11) uniquely determine the collection $\{\pi_i\}$—the argument is the same as for the unicity with respect to the relations (8) and (9). But what we have shown means that the collection of elements $\{{}^{\mathrm{t}}\pi_{2g-i}\}$ satisfies (10) and (11) too, and (ii) follows. This also implies that $\pi_i = 0$ for $i < 0$, so (10) reduces to (8). Further, (9) and (i) follow by transposition from the relations that we have already proven.

To prove (iii) we let $c_{ij} = \pi_{j,X} \circ [{}^{\mathrm{t}}\Gamma_f] \circ \pi_{i,Y}$. Then

$$\begin{aligned} n^i c_{ij} &= \pi_{j,X} \circ [{}^{\mathrm{t}}\Gamma_f] \circ n^i \pi_{i,Y} \\ &= \pi_{j,X} \circ [{}^{\mathrm{t}}\Gamma_f] \circ [{}^{\mathrm{t}}\Gamma_n] \circ \pi_{i,Y} \\ &= \pi_{j,X} \circ [{}^{\mathrm{t}}\Gamma_n] \circ [{}^{\mathrm{t}}\Gamma_f] \circ \pi_{i,Y} = n^j c_{ij} \,, \end{aligned}$$

which implies that $c_{ij} = 0$ unless $i = j$. Hence

$$\begin{aligned} [{}^{\mathrm{t}}\Gamma_f] \circ \pi_{i,Y} &= [\Delta_X] \circ [{}^{\mathrm{t}}\Gamma_f] \circ \pi_{i,Y} \\ &= c_{ii} \\ &= \pi_{i,X} \circ [{}^{\mathrm{t}}\Gamma_f] \circ [\Delta_Y] = \pi_{i,X} \circ [{}^{\mathrm{t}}\Gamma_f] \,. \end{aligned}$$

This completes the proof of the theorem. □

DenMurExa **(13.30) Example.** As remarked in the proof, we have $\pi_{2g} = \big[X \times e(S)\big]$. Combining this with (ii) gives that $\pi_0 = \big[e(S) \times X\big]$.

Next consider an elliptic curve E over a field k. By formula (8) and the previous remark, we should have

$$\pi_1 = \big[\Delta_E\big] - \big[\{0\} \times E\big] - \big[E \times \{0\}\big] .$$

On the other hand, we have defined $\pi_1 \in \mathrm{CH}^*_{\mathbb{Q}}(E \times_k E)$ to be

$$\log\big([\Gamma_{\mathrm{id}}]\big) = \big([\Delta] - [E \times \{0\}]\big) - \frac{1}{2} \cdot \big([\Delta] - [E \times \{0\}]\big)^{*2} ,$$

where the Pontryagin is computed on $E \times_k E$, viewed as an abelian scheme over E via the first projection. Using Lemma (13.26) we find

$$\pi_1 = 2 \cdot \big[\Delta_E\big] - \frac{3}{2} \cdot \big[E \times \{0\}\big] - \frac{1}{2} \cdot \big[\Gamma_2\big] ,$$

where $\Gamma_2 \subset E \times_k E$ is the graph of multiplication by 2. To see that the two ansers for π_1 agree we should check that

FourChow:DivEq
$$\big[\Gamma_2\big] + \big[E \times \{0\}\big] - 2 \cdot \big[\Delta_E\big] - 2 \cdot \big[\{0\} \times E\big] = 0 \tag{12}$$

in $\mathrm{CH}^1_{\mathbb{Q}}(E \times_k E)$. This is indeed the case, for if E is given by a Weierstrass equation $f(X,Y) = 0$ for some cubic $f(X,Y) \in k[X,Y]$ then

FourChow:RatFn
$$(P,Q) \mapsto \frac{x_Q - x_{2P}}{\big(\partial f/\partial X\big)(P) \cdot (x_Q - x_P) + \big(\partial f/\partial Y\big)(P) \cdot (y_Q - y_P)} \tag{13}$$

is a rational function on $E \times E$ whose divisor is precisely the left hand side of (12). (Note that the restriction of the LHS of (12) to $\{P\} \times E$ equals $[2P] + [0] - 2[P]$. This is the divisor of the rational function l_1/l_2 where l_1 is the linear form that defines the line through $2P$ and 0, and where l_2 is the linear form that defines the tangent space at P. Working this out in coordinates, l_1 and l_2 give precisely the numerator and denominator in (13).)

DenMurRem **(13.31)** The interpretation of Thm. (13.29) is that the motive of X decomposes as a direct sum of $2g$ submotives—this point of view shall be further discussed in § 4 below. Let us now already make the connection with cohomology theory. For this, consider any Weil cohomology $X \mapsto H^\bullet(X)$, defined for varieties over a ground field k, with coefficients in a field L of characteristic 0. In particular, we have a Künneth formula, Poincaré duality, and a cycle class map cl: $\mathrm{CH}^*_{\mathbb{Q}}(X) \to H^\bullet(X)$ mapping $\mathrm{CH}^i_{\mathbb{Q}}(X)$ into $H^{2i}(X)$.

Let $g = \dim(X)$. By the Künneth decomposition and Poincaré duality we have

$$H^{2g}(X \times_k X) = \bigoplus_{i=0}^{2g} H^{2g-i}(X) \otimes_L H^i(X) = \bigoplus_{i=0}^{2g} H^i(X)^\vee \otimes_L H^i(X) = \bigoplus_{i=0}^{2g} \mathrm{End}_L\big(H^i(X)\big) .$$

The diagonal class $cl(\Delta_X) \in H^{2g}(X \times_k X)$ corresponds to the element $\oplus \mathrm{id}_{H^i(X)}$. Hence we can write

$$cl(\Delta_X) = \gamma_0 + \gamma_1 + \cdots + \gamma_{2g} ,$$

with $\gamma_i \in \mathrm{End}_L\big(H^i(X)\big)$. The classes γ_i are called the Künneth components of the diagonal. Standard conjectures, as discussed for instance in Kleiman [1], predict that these classes are algebraic. That is, there should exist codimension g cycles D_i on $X \times_k X$ such that $[\Delta_X] = D_0 + D_1 + \cdots + D_{2g}$ and $cl(D_i) = \gamma_i$. For abelian varieties, this is exactly what Theorem (13.29) achieves, as we shall now prove.

WeilCohAV **(13.32) Corollary.** *Let k be a field, and let $X \mapsto H^\bullet(X)$ be any Weil cohomology for k-varieties, with coefficients in a field of characteristic 0. Then for any abelian variety X the Künneth components of the diagonal are algebraic; more precisely, the classes π_i in (8) satisfy $cl(\pi_i) = \gamma_i$. Further we have $H^\bullet(X) \cong \wedge^\bullet H^1(X)$, and n_X induces multiplication by n^i on $H^i(X)$.*

Proof. Let $g := \dim(X)$. We make $H^\bullet := H^\bullet(X)$ into a graded bialgebra by taking m^* as co-multiplication and e^* as augmentation, cf. (6.14) where we used a similar construction for the cohomology of the structure sheaf. By the Borel-Hopf Theorem (6.12) we have $H^\bullet = H_1^\bullet \otimes \cdots \otimes H_r^\bullet$, with $H_i^\bullet$ generated by a single element x_i of degree $d_i > 0$. Note that the degrees d_i are odd. Indeed, if d_i were even then $x_i^q \neq 0$ for all $q > 0$, which is absurd; see the restrictions discussed in (iv) of (6.11), and see Exercise (6.4). It follows that the elements x_i, which are primitive in the sense of (6.16), satisfy $x_i^2 = 0$; see again Exercise (6.4). This means that $H^\bullet$ is a product of exterior algebras; more precisely: if $V_j \subset H^\bullet$ is the span of the elements x_i for which $d_i = j$ then we have

$$H^\bullet \cong \bigotimes_{j \text{ odd}} \big(\wedge^\bullet V_j\big)$$

as graded bialgebras. In particular, if $r_j := \dim(V_j)$ then

FourChow:H2g $$H^{2g} = \big(\wedge^{r_1} V_1\big) \otimes \big(\wedge^{r_3} V_3\big) \otimes \cdots \otimes \big(\wedge^{r_{2g-1}} V_{2g-1}\big)\,, \tag{14}$$

and by comparison of the degrees this gives the relation

FourChow:2geq $$2g = r_1 + 3r_3 + 5r_5 + \cdots + (2g-1)r_{2g-1}\,. \tag{15}$$

We are going to show that $r_j = 0$ for $j > 1$.

We have $cl(\Delta_X) = \sum_{i=0}^{2g} cl(\pi_i)$, and the elements $cl(\pi_i) \in \mathrm{End}_L(H^\bullet)$ are projectors. Let us provisionally write $H^\bullet\{i\}$ for the image of $cl(\pi_i)$. It follows from (9) that $H^\bullet\{i\} \subset H^\bullet$ is precisely the subspace on which n_X induces multiplication by n^i.

Suppose $h \in H^\bullet$ is a primitive element in the sense of (6.16). As 2_X equals the composition $m \circ \Delta\colon X \to X \times_k X \to X$, we find that $2_X^*(h) = \Delta^* m^*(h) = \Delta^*(h \otimes 1 + 1 \otimes h) = 2h$. Hence for every n which is a power of 2 we have $n_X^*(h) = nh$, and this suffices to conclude that $h \in H^\bullet\{1\}$. But the elements of $V := V_1 \oplus V_3 \oplus \cdots \oplus V_{2g-1}$ are all primitive; hence $V \subset H^\bullet\{1\}$. This implies that

$$\big(\wedge^{r_1} V_1\big) \otimes \big(\wedge^{r_3} V_3\big) \otimes \cdots \big(\wedge^{r_{2g-1}} V_{2g-1}\big) \subseteq H^\bullet\{s\} \quad \text{with} \quad s = r_1 + r_3 + \cdots + r_{2g-1}\,.$$

On the other hand, we know that n_X acts as multiplication by n^{2g} on H^{2g}, as H^{2g} is spanned by the cohomology class of a point. So it follows from (14) that $s = 2g$, and comparison with (15) gives that $r_1 = 2g$ and $r_j = 0$ for $j > 1$. Hence $H^\bullet = \wedge^\bullet H^1$ with $H^1 = V_1 \subset H^\bullet\{1\}$, so n_X induces multiplication by n^i on H^i. This last property also implies that $cl(\pi_i) = \gamma_i$. □

LiebTrick **(13.33)** Let X be an abelian variety over a field k. We now study the effect of n_X on $\mathrm{CH}^i_{\mathbb{Q}}(X)$. The elements π_l of (13.29) give rise to a collection of orthogonal idempotents in $\mathrm{End}_{\mathbb{Q}}\big(\mathrm{CH}^i_{\mathbb{Q}}(X)\big)$.

Accordingly, we can decompose $\mathrm{CH}^i_{\mathbb{Q}}(X)$ as a direct sum of subspaces. To make this more precise, let us define

$$\mathrm{CH}^{i,j}_{\mathbb{Q}}(X) := \big\{\alpha \in \mathrm{CH}^i_{\mathbb{Q}} \;\big|\; n_X^*(\alpha) = n^{2i-j}\alpha \quad \text{for all } n\big\}\,.$$

It follows from (9) that $\mathrm{CH}^{i,j}_{\mathbb{Q}}(X)$ is precisely the subspace of $\mathrm{CH}^i_{\mathbb{Q}}(X)$ that is cut out by the idempotent π_{2i-j}.

For example, for $i = 1$ we have $\mathrm{CH}^1(X) = \mathrm{Pic}(X)$. We know that

$$\mathrm{Pic}^0(X) = \big\{[L] \in \mathrm{Pic}(X) \;\big|\; n^*[L] = [L^{\otimes n}] \quad \text{for all } n\big\}\,,$$

and we may also consider the symmetric line bundles

$$\begin{aligned}\mathrm{Pic}^{\mathrm{sym}}(X) &:= \big\{[L] \in \mathrm{Pic}(X) \;\big|\; L \text{ is symmetric}\big\}\\ &= \big\{[L] \in \mathrm{Pic}(X) \;\big|\; n^*[L] = [L^{\otimes n^2}] \quad \text{for all } n\big\}\,,\end{aligned}$$

where the last equality follows from Cor. (2.12). After tensoring with $\mathbb{Q}$ we can invert 2 and we have a direct sum decomposition

$$\begin{aligned}\mathrm{CH}^1_{\mathbb{Q}}(X) &= \big(\mathrm{Pic}^0(X)\otimes\mathbb{Q}\big) \oplus \big(\mathrm{Pic}^{\mathrm{sym}}(X)\otimes\mathbb{Q}\big)\\ &= \mathrm{CH}^{1,1}_{\mathbb{Q}}(X) \oplus \mathrm{CH}^{1,0}_{\mathbb{Q}}(X)\,.\end{aligned}$$

(Cf. the comments after Cor. (2.12).) It is this decomposition that we shall now generalize.

tau(x)Dec **(13.34) Lemma.** *Let $x \in \mathrm{CH}^i_{\mathbb{Q}}(X)$, and write $\tau_{\mathrm{CH}}(x) = \sum_{j=0}^g \xi_j$ with $\xi_j \in \mathrm{CH}^j_{\mathbb{Q}}(X^t)$. Then $\xi_j \in \mathrm{CH}^{j,g-i+j}_{\mathbb{Q}}(X^t)$.*

Proof. Recall that we write $\ell \in \mathrm{CH}^1_{\mathbb{Q}}(X \times X^t)$ for the class of the Poincaré bundle. We have $(\mathrm{id}\times n)^*\ell = n\cdot\ell$, and, by definition, $\tau_{\mathrm{CH}}(x) = p_{X^t,*}\big(p_X^*(x)\cdot\exp(\ell)\big)$. Hence

$$\xi_j = p_{X^t *}\Big(p_X^*(x)\cdot\frac{\ell^{g-i+j}}{(g-i+j)!}\Big)\,,$$

so

$$n^*(\xi_j) = p_{X^t *}(\mathrm{id}\times n)^*\Big(p_X^*(x)\cdot\frac{\ell^{g-i+j}}{(g-i+j)!}\Big) = p_{X^t *}\Big(p_X^*(x)\cdot\frac{(n\cdot\ell)^{g-i+j}}{(g-i+j)!}\Big) = n^{g-i+j}\xi_j\,,$$

which is what we want. □

CHijchar **(13.35) Proposition.** *For $\alpha \in \mathrm{CH}^i_{\mathbb{Q}}(X)$ and $n \in \mathbb{Z}\setminus\{-1,0,1\}$, the following are equivalent:*

(i) $\alpha \in \mathrm{CH}^{i,j}_{\mathbb{Q}}(X)$;
(ii) $n^*(\alpha) = n^{2i-j}\alpha$;
(iii) $n_*(\alpha) = n^{2g-2i+j}\alpha$;
(iv) $\tau_{\mathrm{CH}}(\alpha) \in \mathrm{CH}^{g-i+j}_{\mathbb{Q}}(X^t)$;
(v) $\tau_{\mathrm{CH}}(\alpha) \in \mathrm{CH}^{g-i+j,j}(X^t)$.

Proof. That (i) implies (ii) is just the definition of $\mathrm{CH}^{i,j}_{\mathbb{Q}}$. For the implication (ii) ⇒ (iii) we use that n_*n^* is multiplication by n^{2g} on $\mathrm{CH}^*_{\mathbb{Q}}(X)$. To see that (iii) implies (iv) we use (ii) of Cor. (13.22), which gives

FourChow:n*tau
$$n^*\tau(\alpha) = \tau(n_*\alpha) = n^{2g-2i+j}\tau(\alpha)\,. \tag{16}$$

Since $|n| > 1$ this implies, by the preceding lemma, that $\tau(\alpha) \in \mathrm{CH}^{g-i+j}_{\mathbb{Q}}(X^t)$. The implication (iv) $\Rightarrow$ (v) is again the preceding lemma.

We now have shown that (i) implies (v). Next assume that (v) holds, and apply (i) $\Rightarrow$ (v) to the class $\tau_{\mathrm{CH}}(\alpha)$ on the dual abelian variety. We get that $\tau^t\tau(\alpha) \in \mathrm{CH}^{i,j}(X)$. By Cor. (13.22) this means that $(-1)^*\alpha \in \mathrm{CH}^{i,j}_{\mathbb{Q}}(X)$, which implies that $\alpha = (-1)^*(-1)^*\alpha \in \mathrm{CH}^{i,j}_{\mathbb{Q}}(X)$. □

tauCHij **(13.36) Corollary.** *The Fourier transform gives a bijection*

$$\tau_{\mathrm{CH}}\colon \mathrm{CH}^{i,j}_{\mathbb{Q}}(X) \xrightarrow{\sim} \mathrm{CH}^{g-i+j,j}_{\mathbb{Q}}(X^t)\,.$$

CHiDec **(13.37) Theorem.** *We have*

$$\mathrm{CH}^i_{\mathbb{Q}}(X) = \bigoplus_{j=i-g}^{i} \mathrm{CH}^{i,j}_{\mathbb{Q}}(X)\,.$$

If $\xi \in \mathrm{CH}^{i,j}_{\mathbb{Q}}(X)$ and $\eta \in \mathrm{CH}^{r,s}_{\mathbb{Q}}(X)$ then $\xi \cdot \eta \in \mathrm{CH}^{i+r,j+s}$ and $\xi * \eta \in \mathrm{CH}^{i+r-g,j+s}_{\mathbb{Q}}$.

Proof. It follows from (13.36) that $\mathrm{CH}^{i,j}_{\mathbb{Q}}(X)$ vanishes if $j > i$ or $j < i - g$, since then $g - i + j$ lies outside the range $[0, g]$. It is clear that $\xi \cdot \eta$ lies in $\mathrm{CH}^{i+r,j+s}$, and the last assertion follows from this using Thm. (13.23) and Cor. (13.36). □

§5. *Motivic decomposition.*

ChowMot **(13.38)** We now give a brief introduction to Chow motives. For more explanation we refer to Manin [1], Scholl [??], ...

Let S be a smooth quasi-projective scheme over a field k. For simplicity we shall assume S to be connected. The category $\mathscr{M}(S)$ of relative Chow motives has as its objects pairs $(f\colon X \to S, p)$ with f a smooth morphism, and with $p \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S X)$ an idempotent (meaning that $p \circ p = p$). If there is no risk of confusion we use the shorter notation (X, p). The morphisms are given by

$$\mathrm{Hom}_{\mathscr{M}(S)}\big((X,p),(Y,q)\big) = \big\{q \circ \alpha \circ p \;\big|\; \alpha \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S Y)\big\}\,,$$

and composition of morphisms is given by composition of correspondences.

The set of morphisms $\mathrm{Hom}_{\mathscr{M}(S)}\big((X,p),(Y,q)\big)$ carries a natural grading: if $X = \amalg_j X_j$ is the decomposition of X into connected components, with X_j of relative dimension $d(X_j/S)$ over S then we set

$$\mathrm{Hom}^i\big((X,p),(Y,q)\big) := \big\{q \circ \alpha \circ p \;\big|\; \alpha \in \oplus_j \mathrm{CH}^{d(X_j/S)+i}_{\mathbb{Q}}(X_j \times_S Y)\big\}\,.$$

Composition of morphisms respects this grading: if $\alpha \in \mathrm{Hom}^i$ and $\beta \in \mathrm{Hom}^j$ then $\alpha \circ \beta \in \mathrm{Hom}^{i+j}$.

EffChowMot The category $\mathscr{M}^0_+(S)$ of *effective Chow motives* is a variant of $\mathscr{M}(S)$. The objects are pairs (X, p) in $\mathscr{M}(S)$, but we require p to be of degree 0 and morphisms are also of degree 0; in other words, $\mathrm{Hom}_{\mathscr{M}^0_+(S)} = \mathrm{Hom}^0_{\mathscr{M}(S)}$. There is a natural contravariant functor $R\colon \mathscr{V}(S) \to \mathscr{M}^0_+(S)$ sending X/S to $(X, [\Delta_{X/S}])$, and sending a morphism $f\colon X \to Y$ over S to $[{}^t\Gamma_f]$.

In $\mathscr{M}^0_+(S)$ we have direct sums, given by taking disjoint unions; so,

$$(X,p)\oplus(Y,q)=(X\amalg Y, p\amalg q)\,.$$

For instance, if $p\in \mathrm{CH}^*_{\mathbb{Q}}(X)$ is a projector then so is $q:=[\Delta_{X/S}]-p$, and we have $R(X)\cong (X,p)\oplus(X,q)$.

Since we want to keep track of "Tate twists", we introduce a third category, denoted by $\mathscr{M}^0(S)$. Its objects are triples (X,p,m) with (X,p) in $\mathscr{M}^0_+(S)$ and $m\in\mathbb{Z}$ an integer. The morphisms are given by

$$\mathrm{Hom}_{\mathscr{M}^0(S)}\big((X,p,m),(Y,q,n)\big)=\mathrm{Hom}^{n-m}_{\mathscr{M}(S)}\big((X,p),(Y,q)\big)\,.$$

We view $\mathscr{M}^0_+(S)$ as a full subcategory of $\mathscr{M}^0(S)$ by sending (X,p) to $(X,p,0)$.

M0SProps **(13.40)** The category $\mathscr{M}^0(S)$ is an additive $\mathbb{Q}$-linear category in which every projector has a kernel and a cokernel. Such a category is called pseudo-abelian. We have a tensor product, given by

$$(X,p,m)\otimes(Y,q,n)=(X\times_S Y, p\times_S q, m+n)\,.$$

The object $1_S:=\big(S,[S],0\big)$ is an identity for the tensor product. As an immediate consequence of the definitions we have the Künneth formula

$$R(X\times_S Y)=R(X)\otimes R(Y)\,.$$

An object $M=(X,p,m)$ has a dual $M^\vee$ in $\mathscr{M}^0(S)$. Namely, if X is of pure relative dimension n over S then we set $M^\vee:=(X,{}^{\mathrm{t}}p,n-m)$; to extend this to the general case we first decompose X into connected components. We have a canonical isomorphism

$$\mathrm{Hom}(A\otimes B,C)=\mathrm{Hom}(A,B^\vee\otimes C)\,,$$

functorial in A, B and C in $\mathscr{M}^0(S)$. (In the terminology of tensor categories, as in Deligne and Milne [1], this makes $\mathscr{M}^0(S)$ into a rigid tensor category.)

We define Tate twisting in $\mathscr{M}^0(S)$ by

$$(X,p,m)\big(n\big):=(X,p,m+n)\,.$$

In particular, for X/S of relative dimension n we have the relation

$$R(X)^\vee=R(X)\big(n\big)\,,$$

which may be thought of as the motivic analogue of Poincaré duality. (Note, however, that in the present context this relation is a tautology.)

LefschMot **(13.41)** As an example of a Chow motive we have the *Lefschetz motive* $\mathbb{L}_S$. Take the projective line over S, take a section $e\colon S\to\mathbb{P}^1_S$, and consider the projector $[\Gamma_e]:=\big[\mathbb{P}^1_S\times_S e(S)\big]\in \mathrm{CH}^1_{\mathbb{Q}}(\mathbb{P}^1_S\times_S\mathbb{P}^1_S)$, which is independent of the choice of e. Then we define

$$\mathbb{L}_S:=(\mathbb{P}^1_S,[\Gamma_e],0)\,.$$

One can check that $R(\mathbb{P}^1_S)\cong 1_S\oplus\mathbb{L}_S$. This is reminiscent of the splitting $\mathbb{P}^1=\{\infty\}\amalg\mathbb{A}^1$, and indeed we can think of $\mathbb{L}_S$ as a "motivic form" of the affine line.

For $M \in \mathscr{M}^0(S)$ we have the relation $M(-1) \cong M \otimes \mathbb{L}$; see Exercise (13.3). It easily follows from this that for all $n \in \mathbb{Z}$ we have

FourChow:TatLef
$$M(n) \cong M \otimes \mathbb{L}^{\otimes n}\,, \tag{17}$$

where for $n = -\nu \leqslant 0$ we define $\mathbb{L}^{\otimes n}$ to be $\big(\mathbb{L}^\vee\big)^{\otimes \nu}$.

Using the Lefschetz motive we can say how to form direct sums in $\mathscr{M}^0(S)$. On the full subcategory $\mathscr{M}^0_+(S)$ the direct sum is as described in (13.39). We extend this to the whole of $\mathscr{M}^0(S)$ by using the relation (17). Thus, given $M = (X, p, m)$ and $N = (Y, q, n)$, choose $r \geqslant \max(m, n)$, and use that $M \cong M'(r)$ and $N \cong N'(r)$ with $M' = (X/S, p, 0) \otimes \mathbb{L}^{\otimes r-m}$ and $N'(Y/S, q, 0) \otimes \mathbb{L}^{r-n}$. Then M' and N' are in $\mathscr{M}^0_+(S)$ and $(M' \oplus N')\big(r\big)$ is a direct sum of M and N.

MultStr **(13.42)** A *multiplicative structure* on a relative motive M in $\mathscr{M}(S)$ is a morphism $M \otimes M \to M$ in $\mathscr{M}(S)$. A morphism $\varphi\colon M \to N$ in $\mathscr{M}(S)$ is compatible with multiplicative structures on M and N if it fits in a commutative diagram

$$\begin{array}{ccc} M \otimes M & \xrightarrow{\varphi\otimes\varphi} & N \otimes N \\ \big\downarrow & & \big\downarrow \\ M & \xrightarrow{\varphi} & N \end{array}\,.$$

For example, the relative motive $R(X/S)$ carries a canonical multiplicative structure coming from the diagonal embedding $\Delta\colon X \to X \times_S X$ via

$$R(X/S) \otimes R(X/S) = R(X \times_S X/S) \xrightarrow{[{}^{\mathrm{t}}\Gamma_\Delta]} R(X/S)\,.$$

Another example is given by an abelian scheme A/S. The multiplication $m\colon A \times_S A \to A$ induces the convolution multiplicative structure

$$R(A/S) \otimes_S R(A/S) \xrightarrow{[\Gamma_m]} R(A/S)\,.$$

The relations obtained in Thm. (13.21) may now be reformulated by saying that the Fourier transform τ yields an isomorphism $R(A/S) \xrightarrow{\sim} R(A^t/S)$, compatible with the canonical multiplicative structure on $R(A/S)$ and the convolution structure on $R(A^t/S)$. The inverse isomorphism is given by $(-1)^g[{}^{\mathrm{t}}\Gamma_{-\mathrm{id}_X}] \circ T^t$.

ExtProdMot **(13.43)** We shall need the exterior powers $\wedge^i M$ of a motive $M = (X, p, m)$ in $\mathscr{M}^0(S)$. Recall that for cycles we have an exterior product: if $\xi \in \mathrm{CH}^*_{\mathbb{Q}}(X)$ and $\eta \in \mathrm{CH}^*_{\mathbb{Q}}(Y)$ then we have a well-defined cycle class $\xi \times \eta \in \mathrm{CH}^*_{\mathbb{Q}}(X \times_S Y)$.

Let S_i be the symmetric group on i letters, acting on $X^i = X \times_S \cdots \times_S X$ by permuting the factors. Define $s_i \in \mathrm{CH}^*_{\mathbb{Q}}(X^i \times_S X^i)$ by

$$s_i := \frac{1}{i!} \sum_{\sigma \in S_i} [{}^{\mathrm{t}}\Gamma_\sigma]\,,$$

and let

$$s_{i,M} := s_i \circ (p \times \cdots \times p) = (p \times \cdots \times p) \circ s_i \circ (p \times \cdots \times p) = (p \times \cdots \times p) \circ s_i\,.$$

We now define

$$\wedge^i M := \big(X^i, s_{i,M}, mi\big)\,.$$

Note that $s_{i,M} \in \mathrm{CH}^*_{\mathbb{Q}}(X^i \times_S X^i)$ can be viewed both as a morphism $\wedge^i M \to M^{\otimes i}$ and as a morphism $M^{\otimes i} \to \wedge^i M$.

We say that M has finite dimension if there exists an integer d such that $\wedge^i M = 0$ for all $i > d$. For a finite-dimensional M we put

$$\wedge^* M = \oplus_{i=0}^{d} \wedge^i M\,.$$

The exterior algebra $\wedge^* M$ carries a canonical multiplicative structure induced by the composite maps

$$s_{i+j} \circ (s_i \times s_j)\colon \wedge^i M \otimes_S \wedge^j M \longrightarrow M^{\otimes i+j} \longrightarrow \wedge^{i+j} M\,.$$

MotReal **(13.44) Remark.** In order to get some feeling for these notions, it helps to think about realisations of motives. For instance, suppose $S = \mathrm{Spec}(k)$ and suppose we have a Weil cohomology $X \mapsto H^\bullet(X)$ for k-varieties, with coefficients in some field L. Then this gives a (covariant!) functor h from $\mathscr{M}^0(k)$ into the category of finite dimensional, augmented, graded-commutative L-algebras, referred to as a realisation functor. Via this functor we recognize several notions defined above as being "motivic analogues" of familiar notions in cohomology. For instance, the canonical multiplicative structure on $R(X)$ may be thought of as the motivic analogue of cup-product.

There is a subtle point in this last remark, though. If we have two motives $M_1 = (X_1, p_1, m_1)$ and $M_2 = (X_2, p_2, m_2)$ then there is an obvious isomorphism

$$\psi\colon M_1 \otimes M_2 \xrightarrow{\sim} M_2 \otimes M_1\,,$$

obtained from the isomorphism $X_1 \times X_2 \xrightarrow{\sim} X_2 \times X_1$ that reverses the two factors. However, with this identification the multiplicative structure on an exterior algebra $\wedge^* M$ is *commutative* rather than graded-commutative. Also, the canonical multiplicative structure on $R(X)$ is commutative, unlike cup-product, which is graded-commutative. Though this does not make any difference for the results discussed in this section, let us point out that, in a suitable sense, the above isomorphism ψ is not the right identification to use. A modified version of ψ would give a theory in which $\wedge^* M$ and $R(X)$ are graded-commutative, as it should be. However, to define the right identification $M_1 \otimes M_2 \cong M_2 \otimes M_1$ we need the algebraicity of the Künneth components of the diagonal, which, as already mentioned, is not known in general. See ?? for further discussion.

AVR(X)Dec **(13.45)** Let X/S be an abelian scheme of relative dimension g. Define

$$R^i(X) := (X, \pi_i, 0)\,,$$

with π_i as in (8). Then Theorem (13.29) yields a canonical decomposition

$$R(X) = \bigoplus_{i=0}^{2g} R^i(X)$$

such that $[{}^{\mathrm{t}}\Gamma_n]$ acts on $R^i(X)$ by n^i. Poincaré duality tells us that $R^{2g-i}(X)^\vee = R^i(X)\big(g\big)$.

Our goal is to prove a theorem of Künnemann, which asserts that $R^i(X)$ is isomorphic to $\wedge^i R^1(X)$. As a preparation we first give another description of the motive $\wedge^i R^1(X)$. Since we

shall need the projectors π_i for various abelian schemes, we shall from now on often write $\pi_{i,X}$ for the elements obtained in (8).

By definition we have $\wedge^i R^1(X) = \big(X^i, s_i \circ (\pi_{1,X} \times \cdots \times \pi_{1,X}), 0\big)$. By the motivic Künneth formula we have

$$\pi_{i,X^i} = \sum_{n_1+\cdots+n_i=i} \pi_{n_1,X} \times \cdots \times \pi_{n_i,X}\,,$$

where the indices n_i run from 0 to $2g$, satisfying the condition on their sum. To filter out the term $\pi_{1,X} \times \cdots \times \pi_{1,X}$ we use the action of $-\mathrm{id}_X$. Note that for $[X] \in \mathrm{CH}^0_{\mathbb{Q}}(X)$ we have

FourChow:1X* $$\mathrm{id}_X^*[X] - (-\mathrm{id}_X)^*[X] = 0\,. \tag{18}$$

Therefore, for $a = (a_1, \ldots, a_i) \in \{\pm 1\}^i$, let $\mathrm{sgn}(a) := a_1 a_2 \cdots a_i \in \{\pm 1\}$ and define

$$\lambda_i := (1/2^i) \sum_{a \in \{\pm 1\}^i} \mathrm{sgn}(a)[{}^{\mathrm{t}}\Gamma_a] \quad \in \mathrm{CH}^{gi}_{\mathbb{Q}}(X^i \times_S X^i)\,,$$

where of course Γ_a denotes the graph of the automorphism $(a_1, \ldots, a_i)$ of X^i. Now observe that

$$\begin{aligned} \lambda_i \circ \pi_{i,X^i} &= \lambda_i \circ \Big(\sum_{n_1+\cdots+n_i=i} \pi_{n_1,X} \times \cdots \times \pi_{n_i,X} \Big) \\ &= \lambda_i \circ (\pi_{1,X} \times \cdots \times \pi_{1,X}) \\ &= \pi_{1,X} \times \cdots \times \pi_{1,X}\,. \end{aligned} \tag{19}$$

FourChow:lambi

Indeed, if $n_j > 1$ for some index j then there is also an index $l \in \{1, \ldots, i\}$ with $n_l = 0$; but then it easily follows from (18) that the term $\lambda_i \circ (\pi_{n_1,X} \times \cdots \times \pi_{n_i,X})$ vanishes. We are left with the term corresponding to $(n_1, \ldots, n_i) = (1, \ldots, 1)$, which is preserved because each $[{}^{\mathrm{t}}\Gamma_a]$ acts on it as the identity.

wdgR1Lem **(13.46) Lemma.** *We have $\wedge^i R^1(X) = (X^i, \lambda_i \circ s_i \circ \pi_{i,X^i}, 0)$ in $\mathscr{M}^0(S)$.*

Proof. One easily checks that the elements s_i and λ_i are projectors and that they commute. Now (19) gives

$$\wedge^i R^1(X) = \big(X^i, s_i \circ (\pi_{1,X} \times \ldots \times \pi_{1,X}), 0\big) = (X^i, s_i \circ \lambda_i \circ \pi_{i,X^i}, 0) = (X^i, \lambda_i \circ s_i \circ \pi_{i,X^i}, 0)\,,$$

which is what we want. □

wedgeR1X **(13.47) Theorem.** (Künnemann) *There is an isomorphism of motives with multiplicative structures*

$$\wedge^* R^1(X) \xrightarrow{\sim} R(X)\,.$$

Proof. Let $\Sigma^i\colon X^i \to X$ and $\Delta^i\colon X \to X^i$ be the homomorphisms given by $\Sigma^i(x_1, \ldots, x_i) = x_1 + \cdots + x_i$ and $\Delta^i(x) = (x, \ldots, x)$. We have the relations

FourChow:GsG $$[{}^{\mathrm{t}}\Gamma_{\Delta^i}] \circ s_i = [{}^{\mathrm{t}}\Gamma_{\Delta^i}] \qquad \text{and} \qquad s_i \circ [{}^{\mathrm{t}}\Gamma_{\Sigma^i}] = [{}^{\mathrm{t}}\Gamma_{\Sigma^i}]\,. \tag{20}$$

Let us also note that we have the relations $\pi_{i,X^i} \circ s_i = s_i \circ \pi_{i,X^i}$ and $\pi_{i,X^i} \circ \lambda_i = \lambda_i \circ \pi_{i,X^i}$, as follows from (iii) of Thm. (13.29).

Define morphisms

$$\Phi_i := [{}^{\mathrm{t}}\Gamma_{\Delta^i}] \circ (\lambda_i \circ s_i \circ \pi_{i,X^i}) = [{}^{\mathrm{t}}\Gamma_{\Delta^i}] \circ \lambda_i \circ \pi_{i,X^i} \in \mathrm{Hom}_{\mathscr{M}^0(S)}\big(\wedge^i R^1(X), R(X)\big)\,,$$

and

$$\Psi_i := \frac{1}{i!}(\lambda_i \circ s_i \circ \pi_{i,X^i}) \circ [{}^{\mathrm{t}}\Gamma_{\Sigma^i}] = \frac{1}{i!}\lambda_i \circ \pi_{i,X^i} \circ [{}^{\mathrm{t}}\Gamma_{\Sigma^i}] \in \mathrm{Hom}_{\mathscr{M}^0(S)}\big(R(X), \wedge^i R^1(X)\big)\,.$$

The theorem will result from the following more precise claims:

(i) $\Phi_i \circ \Psi_i = \pi_{i,X}$,

(ii) $\Psi_i \circ \Phi_i = \lambda_i \circ s_i \circ \pi_{i,X^i} = \mathrm{id}_{\wedge^i R^1(X)}$.

To prove (i) we write

$$\begin{aligned}
\Phi_i \circ \Psi_i &= (1/i!) \cdot [{}^{\mathrm{t}}\Gamma_{\Delta^i}] \circ \lambda_i \circ \pi_{i,X^i} \circ \lambda_i \circ \pi_{i,X^i} \circ [{}^{\mathrm{t}}\Gamma_{\Sigma^i}] \\
&= (1/i!) \cdot [{}^{\mathrm{t}}\Gamma_{\Delta^i}] \circ \lambda_i \circ [{}^{\mathrm{t}}\Gamma_{\Sigma^i}] \circ \pi_{i,X} && \text{by (iii) of (13.29)} \\
&= (1/2^i i!) \cdot \sum_{a \in \{\pm 1\}^i} \mathrm{sgn}(a) [{}^{\mathrm{t}}\Gamma_{\Sigma^i \circ a \circ \Delta^i}] \circ \pi_{i,X} \\
&= (1/2^i i!) \cdot \sum_{a \in \{\pm 1\}^i} \mathrm{sgn}(a) [{}^{\mathrm{t}}\Gamma_{a_1 + \cdots + a_i}] \circ \pi_{i,X} \\
&= (1/2^i i!) \cdot \sum_{a \in \{\pm 1\}^i} \mathrm{sgn}(a)(a_1 + \cdots + a_i)^i \cdot \pi_{i,X} && \text{by (9).}
\end{aligned}$$

Now use that

$$\sum_{a \in \{\pm 1\}^i} \mathrm{sgn}(a)(a_1 + \cdots + a_i)^k = \begin{cases} 0 & \text{if } 0 \leqslant k < i, \\ 2^i i! & \text{if } k = i, \end{cases}$$

as is easily shown by induction on i.

To prove (ii) we must show that $(1/i!) \cdot \lambda_i \circ \pi_{i,X^i} \circ [{}^{\mathrm{t}}\Gamma_{\Sigma^i}] \circ [{}^{\mathrm{t}}\Gamma_{\Delta^i}] \circ \lambda_i \circ \pi_{i,X^i} = \lambda_i \circ s_i \circ \pi_{i,X^i}$. What we shall actually prove is that

FourChow:goal
$$(1/i!) \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ [\Gamma_{\Delta^i \circ \Sigma^i}] \circ {}^{\mathrm{t}}\pi_{i,X^i} \circ {}^{\mathrm{t}}\lambda_i = {}^{\mathrm{t}}\lambda_i \circ {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\pi_{i,X^i}\,. \tag{21}$$

After transposition, using (20) and using that s_i, λ_i and π_{i,X^i} are mutually commuting projectors, this gives the desired relation.

Write $\mathrm{pr}_l \colon X^i \to X$ for the projection on the lth factor and $j_l \colon X \to X^i$ for the inclusion of the lth factor.

As before, we view $X^i \times_S X^i$ as an abelian scheme over X^i via the first projection. We know that ${}^{\mathrm{t}}\pi_{i,X^i} = \pi_{2gi-i,X^i}$, and by construction the latter equals $(1/i!) \cdot \log\big([\Gamma_{\mathrm{id}}]\big)^{*i}$. (This takes place on X^i.) Recall that when we write "Γ_{id}" we may interpret this as the graph class associated to the section $\xi \mapsto (\xi, \xi)$ of $X^i \times_S X^i$ over X^i. Likewise, we have meaningfully defined graph classes $[\Gamma_{j_k \circ \mathrm{pr}_l}]$.

With these remarks, the LHS of (21) equals

$$\begin{aligned}
&(1/i!)^2 \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ [\Gamma_{\Delta^i \circ \Sigma^i}] \circ \log\big([\Gamma_{\mathrm{id}}]\big)^{*i} \circ {}^{\mathrm{t}}\lambda_i \\
&= (1/i!)^2 \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \log\big([\Gamma_{\Delta^i \circ \Sigma^i}]\big)^{*i} \circ {}^{\mathrm{t}}\lambda_i && \text{using Exercise (13.4)} \\
&= (1/i!)^2 \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \Big(\sum_{k,l=1}^{i} \log\big([\Gamma_{j_k \circ \mathrm{pr}_l}]\big)\Big)^{*i} \circ {}^{\mathrm{t}}\lambda_i \\
&= (1/i!)^2 \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \Big(\sum_{k_1,\ldots,k_i=1}^{i} \sum_{l_1,\ldots,l_i=1}^{i} \log\big([\Gamma_{j_{k_1} \circ \mathrm{pr}_{l_1}}]\big) * \cdots * \log\big([\Gamma_{j_{k_i} \circ \mathrm{pr}_{l_i}}]\big)\Big) \circ {}^{\mathrm{t}}\lambda_i\,.
\end{aligned}$$

We claim that this equals

$$(1/i!)^2 \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \Big(\sum_{\sigma\in S_i} \sum_{\tau\in S_i} \log\big([\Gamma_{j_{\sigma(1)}\circ \mathrm{pr}_{\tau(1)}}]\big) * \cdots * \log\big([\Gamma_{j_{\sigma(i)}\circ \mathrm{pr}_{\tau(i)}}]\big)\Big)\,. \tag{22}$$

FourChow:sigtau

Indeed, expanding λ_i we have

$$\begin{aligned} &{}^{\mathrm{t}}\lambda_i \circ \Big(\log\big([\Gamma_{j_{k_1}\circ \mathrm{pr}_{l_1}}]\big) * \cdots * \log\big([\Gamma_{j_{k_i}\circ \mathrm{pr}_{l_i}}]\big)\Big) \circ {}^{\mathrm{t}}\lambda_i \\ &= 2^{-2i} \cdot \sum_{a,b\in\{\pm1\}^i} \mathrm{sgn}(a)\mathrm{sgn}(b) \cdot \log\big([\Gamma_{a\circ j_{k_1}\circ \mathrm{pr}_{l_1}\circ b}]\big) * \cdots * \log\big([\Gamma_{a\circ j_{k_i}\circ \mathrm{pr}_{l_i}\circ b}]\big)\,. \end{aligned} \tag{23}$$

If $(a_1,\ldots,a_i)$ is not a permutation of $(1,\ldots,i)$, choose $j \in \{1,\ldots,i\} \setminus \{n_1,\ldots,n_i\}$; then the corresponding terms with $a_j = -1$ and $a_j = 1$ cancel out. Likewise, if there is an index j in $\{1,\ldots,i\} \setminus \{b_1,\ldots,b_i\}$ then the terms with $b_j = -1$ and $b_j = 1$ cancel out. Hence we may assume that $(k_1,\ldots,k_i) = \big(\sigma(1),\ldots,\sigma(i)\big)$ and $(l_1,\ldots,l_i) = \big(\tau(1),\ldots,\tau(i)\big)$. If for $\alpha \in \{\pm1\}^i$ we group the 2^i terms of (23) with $a_{\sigma(i)} \cdot b_{\tau(i)} = \alpha_i$ for all i then we find that (23) equals

$$\begin{aligned} &2^{-i} \cdot \sum_{\alpha\in\{\pm1\}^i} \mathrm{sgn}(\alpha) \cdot \Big(\log\big([\Gamma_{\alpha\circ j_{\sigma(1)}\circ \mathrm{pr}_{\tau(1)}}]\big) * \cdots * \log\big([\Gamma_{\alpha\circ j_{\sigma(i)}\circ \mathrm{pr}_{\tau(i)}}]\big)\Big) \\ &= {}^{\mathrm{t}}\lambda_i \circ \Big(\log\big([\Gamma_{j_{\sigma(1)}\circ \mathrm{pr}_{\tau(1)}}]\big) * \cdots * \log\big([\Gamma_{j_{\sigma(i)}\circ \mathrm{pr}_{\tau(i)}}]\big)\Big)\,, \end{aligned}$$

proving our claim.

Next we remark that we may reorder the log-factors in (22), and since ${}^{\mathrm{t}}s_i \circ \log\big([\Gamma_{j_{\sigma(l)}\circ \mathrm{pr}_l}]\big) = \log\big([\Gamma_{j_l\circ \mathrm{pr}_l}]\big)$ for all σ and l, we finally get that the LHS of (21) equals

$$\begin{aligned} &(1/i!) \cdot {}^{\mathrm{t}}\lambda_i \circ {}^{\mathrm{t}}s_i \circ \Big(\sum_{\sigma\in S_i} \log\big([\Gamma_{j_{\sigma(1)}\circ \mathrm{pr}_1}]\big) * \cdots * \log\big([\Gamma_{j_{\sigma(i)}\circ \mathrm{pr}_i}]\big)\Big) \\ &= {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \Big(\log\big([\Gamma_{j_1\circ \mathrm{pr}_1}]\big) * \cdots * \log\big([\Gamma_{j_i\circ \mathrm{pr}_i}]\big)\Big)\,. \end{aligned} \tag{24}$$

The RHS of (21) equals

$$\begin{aligned} &(1/i!) \cdot {}^{\mathrm{t}}\lambda_i \circ {}^{\mathrm{t}}s_i \circ \log\big([\Gamma_{\mathrm{id}}]\big)^{*i} \\ &= (1/i!) \cdot {}^{\mathrm{t}}\lambda_i \circ {}^{\mathrm{t}}s_i \circ \Big(\log\big([\Gamma_{j_1\circ \mathrm{pr}_1}]\big) + \cdots + \log\big([\Gamma_{j_i\circ \mathrm{pr}_i}]\big)\Big)^{*i} \\ &= (1/i!) \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \Big(\sum_{n_1,\ldots,n_i=1}^{i} \log\big([\Gamma_{j_{n_1}\circ \mathrm{pr}_{n_1}}]\big) * \cdots * \log\big([\Gamma_{j_{n_i}\circ \mathrm{pr}_{n_i}}]\big)\Big)\,. \end{aligned}$$

With the same argument as above we see that the only non-trivial contributions come from the terms with $(n_1,\ldots,n_i)$ a permutation of $(1,\ldots,i)$. Hence we get

$$(1/i!) \cdot {}^{\mathrm{t}}s_i \circ {}^{\mathrm{t}}\lambda_i \circ \Big(\sum_{\sigma\in S_i} \log\big([\Gamma_{j_{\sigma(1)}\circ \mathrm{pr}_{\sigma(1)}}]\big) * \cdots * \log\big([\Gamma_{j_{\sigma(i)}\circ \mathrm{pr}_{\sigma(i)}}]\big)\Big)\,,$$

and after reordering the log-factors we see that this equals (24), proving relation (ii).

To finish the proof of the theorem we have to check that the maps $\sum_i \Phi_i\colon \wedge^* R^1(X) \to R(X)$ and $\sum_i \Psi_i\colon R(X) \to \wedge^* R^1(X)$ respect the multiplicative structures. This is a straightforward verification that we leave as an exercise. □

(13.48) Remark. Passing to cohomology this gives another proof of Thm. (13.32).

Exercises.

Ex:SyminCH **(13.1)** Let X be an abelian variety. Write $\tau = \tau_{\mathrm{CH}}$. If $\alpha \in \mathrm{CH}^*_{\mathbb{Q}}(X)$ is a symmetric element, meaning that $(-1_X)^*\alpha = \alpha$, prove that $\tau(\alpha)$ is symmetric too, and that $\tau(\alpha) \in \oplus_j \mathrm{CH}^{g-i+2j}_{\mathbb{Q}}(X)$. Similarly, if α is anti-symmetric, meaning that $(-1_X)^*\alpha = -\alpha$, prove that $\tau(\alpha)$ is also anti-symmetric, and that $\tau(\alpha) \in \oplus_j \mathrm{CH}^{g-i+2j+1}_{\mathbb{Q}}(X)$.

Ex:ThetaCH **(13.2)** Let Θ be a divisor on an abelian variety X giving a principal polarization. Let $\theta \in \mathrm{CH}^1_{\mathbb{Q}}(X)$ be its class. Prove that $\tau(e^{\theta}) = e^{-\theta}$.

Ex:MOS **(13.3)** Consider the category $\mathscr{M}^0(S)$ as in (13.39). Let $\mathbb{L} = (\mathbb{P}^1_S, [\Gamma_e], 0)$ be the Lefschetz motive as defined in (13.41).

(i) Let $q := [\Delta] - [\Gamma_e]$, with $\Delta \subset \mathbb{P}^1_S \times_S \mathbb{P}^1_S$ the diagonal. Show that $(\mathbb{P}^1_S/S, q, 0) \cong 1_S$. Conlude that $R(\mathbb{P}^1_S/S) \cong 1_S \oplus \mathbb{L}$.

(ii) For M in $\mathscr{M}^0(S)$ and $\mathbb{L}$, prove that $M(-1) \cong M \otimes \mathbb{L}$.

Ex:GflogGx **(13.4)** Let $f\colon X \to Y$ be a homomorphism of abelian schemes over a basis S as in (13.38). For $x \in X(S)$, view $\log\big([\Gamma_x]\big)$ as a correspondence from S to X. Show that $[\Gamma_f] \circ \log\big([\Gamma_x]\big) = \log\big([\Gamma_{f(x)}]\big)$. Using Lemmas (13.6) and (13.17), generalize this to the identity $[\Gamma_f] \circ \log\big([\Gamma_x]\big)^{*n} = \log\big([\Gamma_{f(x)}]\big)^{*n}$ for all $n \geqslant 0$.

Notes. Pontryagin introduced the Pontryagin product in his investigations of the homology of Lie groups in 1935; see Pontryagin [1], [2]. The Fourier transform can be defined in various contexts. It first occurred in a paper of Lieberman (see Kleiman [1], Appendix) at the level of cohomology. Mukai introduced it in the derived category of O_X-modules and established many properties of it. Beauville studied the Fourier transform on the Chow rings of an abelian variety and especially the action of multiplication by n. Deninger and Murre [1] used work of Beauville to give a canonical decomposition of the Chow motive of an abelian variety which is the analogue of the well-known cohomological decomposition $H(X) \cong \oplus_{i=0}^{2g} H^i(X)$. It is based on the decomposition of $\mathrm{CH}^*_{\mathbb{Q}}(X \times X)$ into eigenspaces of the endomorphism $(1_X \times n_X)^*$ for any integer n. If $|n| > 1$ then the components of the diagonal for this decomposition yield pairwise orthogonal idempotents in the ring of correspondences and this gives a decomposition of the Chow motive of an abelian variety. Shermenev had given such a decomposition earlier, but his decomposition was not canonical. Künneman used these idempotents to prove that the Chow motive $R(X)$ is the exterior algebra $\wedge^1 R^1$ generalizing the result for cohomology. Proposition (13.27) is due to Bloch; the proof using the Fourier transform stems from Beauville.

Inventarisatie van wat we nodig hebben in dit hoofdstuk:

— $\xi^t\colon X^t \to S$ dan $R^g\xi^t_*\mathscr{P} \cong e^t_* \det(\mathbb{E}^t)^{-1}$;

— resultaten over Chern klassen van de Hodge bundel; i.h.b. dat $\mathrm{Td}(\mathbb{E}) = \exp(\lambda_1/2)$ en dat $\lambda_1 = \lambda_1^t$;

— Thm of the Cube voor abelse schema's;

— Thm of the Square voor abelse schema's.

In this chapter we study a class of abelian varieties that are : Jacobian varieties of curves. In fact, every abelian variety is isogenous to a quotient of a Jacobian variety. The definition of the Jacobian $J = \mathrm{Jac}^0(C)$ of a curve C was already given in Chapter 6: it is the identity component of $\mathrm{Pic}_{C/k}$. If the curve has genus g then J is birationally equivalent to the g-fold symmetric product of C; this allows for a detailed study of the Jacobian.

The Jacobian comes equipped with a principal polarization given by the theta divisor $\Theta \subset \mathrm{Jac}^{g-1}(C)$ of effective divisor classes of degree $g-1$. The geometry of this divisor reflects the properties of the curve in a spectacular way. The Torelli theorem says that the Jacobian with its polarization determines the curve. But not every abelian variety is a Jacobian. The Matsusaka Criterion often helps us to decide whether it is or not.

Unless indicated otherwise, by a curve over a field k we shall mean a 1-dimensional variety over k. In particular, a curve is supposed to be geometrically irreducible and reduced. In § 9 we shall consider more general curves, that are not assumed to be irreducible.

§1. *The Jacobian variety of a curve.*

JacCDef **(14.1)** We recall from Chapter 6 the definition of the Jacobian variety of a curve. Let k be a field and let C/k be a proper smooth curve of genus g. We started with the functor $P_{C/k}\colon \mathsf{Sch}^0_{/k} \to \mathsf{Ab}$ given by $T \mapsto \mathrm{Pic}(C_T) = H^1(C_T, O^*_{C_T})$. We cannot expect that this functor is representable; to repair this we have to sheafify it. The relative Picard functor $\mathrm{Pic}_{C/k}\colon \mathsf{Sch}^0_{/k} \to \mathsf{Ab}$ is defined as the fppf sheaf associated to the presheaf $P_{C/k}$. By standard results, see (6.3) and (6.8), this functor is representable by a smooth group scheme over k whose connected components are complete. We shall be most interested in the identity component

$$J = J_{C/k} := \mathrm{Pic}^0_{C/k}\,,$$

which is a g-dimensional abelian variety over k with $H^1(C, O_C)$ as its tangent space at the origin.

If C has a k-rational point $\varepsilon\colon \mathrm{Spec}(k) \to C$ then $\mathrm{Pic}_{C/k}$ can be identified with the functor of line bundles with rigidification along ε. In this case we find that $\mathrm{Pic}_{C/k}$ is isomorphic with the functor $\mathsf{Sch}^0_{/k} \to \mathsf{Ab}$ given by $T \mapsto \mathrm{Pic}(C_T)/p_T^*\mathrm{Pic}(T)$, where $p_T\colon C_T \to T$ is the projection. In general, not assuming that C has a k-rational point, there is an exact sequence

Jacs:PicBrSeq
$$0 \to \mathrm{Pic}(T) \to \mathrm{Pic}(C_T) \to \mathrm{Pic}_{C/k}(T) \to \mathrm{Br}(T) \to \mathrm{Br}(C_T)\,, \tag{1}$$

where $\mathrm{Br}(X)$ denotes the Brauer group of a scheme X; see ??. The boundary map $\mathrm{Pic}_{C/k}(T) \to \mathrm{Br}(T)$ can be non-zero, which means that not every class in $\mathrm{Pic}_{C/k}(T)$ can be represented by a line bundle on C_T. See Example (14.3) for a simple concrete example.

For a line bundle L on C_T the function $d_L\colon |T| \to \mathbb{Z}$ given by $t \mapsto \deg(L_t)$ is locally constant. This is a consequence of the fact that the Euler-Poincaré characteristic $\chi(L_t)$ is locally constant (see HAG, Chap. 3, (9.9)), as we have the Riemann-Roch relation $\chi(L_t) = \deg(L_t) + 1 - g$. Hence d_L can be viewed as a T-valued point of the constant group scheme $\mathbb{Z}$. As we have

Jac, 8 februari, 2012 (635)

$d_{L\otimes M} = d_L + d_M$, the map $L \mapsto d_L$ defines a homomorphism of presheaves $d\colon P_{C/k} \to \mathbb{Z}$. Now define

deg

Jac

$$\deg\colon \mathrm{Pic}_{C/k} \to \mathbb{Z}$$

to be the associated homomorphism of group schemes, bearing in mind that $\mathrm{Pic}_{C/k}$ is the fppf sheaf associated to $P_{C/k}$. Of course, if a T-valued point of $\mathrm{Pic}_{C/k}$ is represented by a line bundle L on C_T then $\deg\big([L]\big)$ is just the function d_L.

We now define, for $n \in \mathbb{Z}$,

$$\mathrm{Jac}^n(C) := \deg^{-1}(n)\,.$$

(One could also call this $\mathrm{Pic}^n_{C/k}$ but in the context of Jacobians of curves we shall rather use $\mathrm{Jac}^n(C)$.) Note that $\mathrm{Jac}^n(C)$ is a non-empty scheme, as it is clear that it has $\overline{k}$-valued points.

Since deg is locally constant, $J \subseteq \mathrm{Jac}^0(C)$. We assert that, in fact, $\mathrm{Jac}^0(C)$ is connected, and hence $J = \mathrm{Jac}^0(C)$. To see this, we may extend scalars to an algebraic closure of k. Then every class in $\mathrm{Jac}^0(C)$ is represented by a line bundle $O_C(D)$ with D a divisor of degree 0, i.e., D is of the form $\sum_{i=1}^r (P_i - Q_i)$ with P_i, $Q_i \in C(\overline{k})$. Now remark that for fixed $Q \in C(\overline{k})$ the map $C \to \mathrm{Jac}^0(C)$ given on points by $P \mapsto [P - Q]$ has a connected image.

The following result summarizes our conclusions thus far.

Jacobian **(14.2) Theorem.** *Let C be a proper smooth curve of genus g over a field k. Then $J = J_{C/k} := \mathrm{Pic}^0_{C/k}$ is an abelian variety of dimension g whose tangent space at the origin is isomorphic with $H^1(C, O_C)$, and which coincides with $\mathrm{Jac}^0(C)$, the kernel of the degree homomorphism* $\deg\colon \mathrm{Pic}_{C/k} \to \mathbb{Z}$.

The resulting variety $J = \mathrm{Pic}^0_{C/k} = \mathrm{Jac}^0(C)$ is called *the Jacobian variety* or simply *the Jacobian* of C. The functor $\mathrm{Jac}^n(C)$ is represented by an algebraic variety of dimension g over k which is a torsor under J. In particular, each $\mathrm{Jac}^n(C)$ is again connected and complete. By construction we have $\mathrm{Pic}_{C/k} = \coprod_{n\in\mathbb{Z}} \mathrm{Jac}^n(C)$.

As we shall later, the Jacobian J comes equipped with a natural principal polarization $\lambda\colon J \xrightarrow{\sim} J^t$. Let us note here that in some literature the term "Jacobian" refers to the pair (J, λ), or to J together with a theta divisor $\Theta \subset J$. In this book, the term "Jacobian" refers to the abelian variety J itself.

genus0Exa **(14.3) Example.** If C has genus 0 then the degree map gives an isomorphism $\mathrm{Pic}_{C/k} \xrightarrow{\sim} \mathbb{Z}$ and all components $\mathrm{Jac}^n(C)$ are isomorphic to $\mathrm{Spec}(k)$. This does not mean that for any n there exists a line bundle of degree n on C ! For example, take $k = \mathbb{R}$ and consider the curve $C \subset \mathbb{P}^2$ given by $X^2 + Y^2 + Z^2 = 0$. This curve only has line bundles of even degree. However, $C_{\mathbb{C}} \cong \mathbb{P}^1_{\mathbb{C}}$, so given $n \in \mathbb{Z}$ there is, up to isomorphism, a unique line bundle L_n of degree n on $C_{\mathbb{C}}$. Hence the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ fixes the class $[L_n] \in \mathrm{Pic}(C_{\mathbb{C}})$, and therefore L_n defines an $\mathbb{R}$-valued (and not just $\mathbb{C}$-valued) point of $\mathrm{Jac}^n(C)$. Taking $T = \mathrm{Spec}(\mathbb{C})$, the sequence (1) in this example reads

$$0 \longrightarrow 0 \longrightarrow 2\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \to 0\,.$$

Of course, in genus 0 the Jacobian is not a very interesting object. Some more interesting examples shall be discussed in § 5 of this chapter. In what follows we shall usually only consider curves of genus $g \geqslant 1$.

By (3.15) we have

$$\Omega^1_{\mathrm{Jac}^n(C)/k} \cong H^0(C, \Omega^1_{C/k}) \otimes_k O_{\mathrm{Jac}^n(C)}\,,$$

where we use the identification $T_{J,0}^\vee = H^1(C, O_C)^\vee$ of Cor. (6.6), part (i), and the Serre duality isomorphism $H^1(C, O_C)^\vee \cong H^0(C, \Omega^1_{C/k})$. In particular this gives an isomorphism

Jacs:H0JacnOm1
$$H^0\big(\mathrm{Jac}^n(C), \Omega^1_{\mathrm{Jac}^n(C)/k}\big) \cong H^0(C, \Omega^1_{C/k})\,. \tag{2}$$

CtoJac1 **(14.4) Theorem.** *Let*

$$j\colon C \to \mathrm{Jac}^1(C)$$

be the morphism that associates to a T-valued point P of C the class of the line bundle $O_{C_T}(P)$ on C_T.

(i) *If $g \geqslant 1$ then j is a closed immersion.*

(ii) *The induced map $j^*\colon H^0\big(\mathrm{Jac}^1(C), \Omega^1_{\mathrm{Jac}^1(C)/k}\big) \to H^0(C, \Omega^1_{C/k})$ coincides with the isomorphism* (2).

Proof. Without loss of generality we may assume that $k = \overline{k}$. Since j is a morphism of smooth k-varieties, it is a closed embedding if it separates points and tangent vectors. To see that j separates points, suppose that Q_1, $Q_2 \in C(k)$ have the same image under j. Then $O_C(Q_1) \otimes O_C(Q_2)^{-1} \cong O_C(Q_1 - Q_2)$ is trivial, i.e., $Q_1 - Q_2$ is the divisor of a function f. But then f defines an isomorphism of C with $\mathbb{P}^1$, contradicting the assumption that $g(C) \geqslant 1$.

Next we want to compute the tangent map of j. Let $Q \in C(k)$. Choose a local coordinate t at Q, i.e., an element of $k(C)$ that vanishes to order 1 at Q. Let U_1 be an affine open neighbourhood of Q in C such that t has no zeroes or poles on $U_1 \setminus \{Q\}$. Set $U_2 = C \setminus \{Q\}$ and let $U_{12} := U_1 \cap U_2$. Then the class of the line bundle $O_C(Q)$ in $\mathrm{Pic}(C) = H^1(C, O_C)$ is represented by the Čech 1-cocycle $t^{-1} \in O_C^*(U_{12})$ with respect to the covering $C = U_1 \cup U_2$.

Let $\partial_t \in T_{C,Q}$ be the tangent vector at Q given by the local coordinate t. We claim that the tangent map

$$Tj\colon T_{C,Q} \to T_{\mathrm{Jac}^1(C), j(Q)} \cong H^1(C, O_C) \cong H^0(C, \Omega^1_{C/k})^\vee$$

is given as follows: If $\omega \in H^0(C, \Omega^1_{C/k})$, write ω locally near Q as $\omega = f(t)dt$; then $Tj(\partial_t)\big(\omega\big) = f(Q)$.

For the proof of this claim, write $C[\varepsilon] := C \otimes_k k[\varepsilon]$ and $U_i[\varepsilon] := U_i \otimes_k k[\varepsilon]$, where $k[\varepsilon]$ is the ring of dual numbers. We can describe the tangent vector ∂_t as a $k[\varepsilon]$-valued point $\tilde{Q}\colon \mathrm{Spec}\big(k[\varepsilon]\big) \to U_1[\varepsilon] \subset C[\varepsilon]$ that reduces to Q modulo ε. If we let $A := O_C(U_1)$ then $\tilde{Q}$ is given on rings by a homomorphism $\tilde{Q}\colon A[\varepsilon] \to k[\varepsilon]$ of the form $\tilde{Q}(a+b\varepsilon) = Q(a)+\varepsilon\cdot\big(\delta(a)+Q(b)\big)$, where $\delta\colon A \to k$ is a k-derivation. We find that the tangent vector "$\tilde{Q} = \partial_t$" is the one corresponding to the unique k-derivation $\delta\colon A \to k$ with $\delta(t) = 1$, and that $\tilde{t} := t - \varepsilon$ is a local coordinate for $\tilde{Q}$. The class of the line bundle $O_{C[\varepsilon]}(\tilde{Q})$ is then represented by the Čech 1-cocycle $\tilde{t}^{-1} \in O^*_{C[\varepsilon]}(U_{12})$. Hence the class of the line bundle $O_{C[\varepsilon]}(\tilde{Q} - Q)$ in $H^1\big(C[\varepsilon], 1 + \varepsilon O_C\big)$ is given by the cocycle $\tilde{t}^{-1} \cdot t = 1 + t^{-1}\varepsilon \in O^*_{C[\varepsilon]}(U_{12})$, and therefore corresponds to the class in $H^1(C, O_C)$ represented by the cocycle $t^{-1} \in O_C(U_{12})$.

The isomorphism $H^1(C, O_C) \xrightarrow{\sim} H^0(C, \Omega^1_{C/k})^\vee$ can be described in terms of residues of differentials; cf. HAG, Chap. III, Sect. 7. In the particular case considered here we find that $Tj(\partial_t)\big(\omega\big)$ equals the residue at Q of the differential $t^{-1} \cdot \omega \in \Omega^1_{C/k}(U_{12})$. If we write ω locally near Q as $\omega = f(t)dt$ then $\mathrm{res}_Q(t^{-1} \cdot \omega) = f(Q)$, and this proves our claim.

To complete the proof of (i), observe that the canonical system $|K_C|$ of C is base-point free, as $g \geqslant 1$. This just means that there is an $\omega \in H^0(C, \Omega^1_{C/k})$ that does not vanish at Q. Hence $Tj(\partial_t) \neq 0$, and since $T_{C,Q}$ is 1-dimensional, the tangent map at every point is injective.

The assertion in (ii) is essentially a reformulation of the claim that we have proved. To see this, take $\omega \in H^0(C, \Omega^1_{C/k})$, and let α be the global 1-form on $\mathrm{Jac}^1(C)$ corresponding to ω under the isomorphism (2). Suppose we have a line bundle L of degree 1 on C, and a line bundle $\tilde{L}$ on $C[\varepsilon]$ that reduces to L modulo ε. Write $L[\varepsilon]$ for the pull-back of L under the natural morphism $C[\varepsilon] \to C$. Then $\tilde{L} \otimes L[\varepsilon]^{-1}$ is a line bundle on $C[\varepsilon]$ that is trivial modulo ε, and therefore represents a class in $H^1(C, O_C)$. On the other hand, we can view L as a k-valued point of $\mathrm{Jac}^1(C)$ and $\tilde{L}$ as a tangent vector at $[L]$. Now the relation between α and ω is that the evaluation of α at the tangent vector $\tilde{L}$ equals the evaluation of $\omega \in H^0(C, \Omega^1_{C/k}) \cong H^1(C, O_C)^\vee$ at the class given by $\tilde{L} \otimes L[\varepsilon]^{-1}$.

Now we compose with j. Let $Q \in C(k)$, choose a local coordinate t, and let "$\tilde{Q} = \partial_t$" be the corresponding tangent vector. Then we find that the value of $j^*\alpha$ at $\tilde{Q}$ equals the evaluation of ω at the class in $H^1(C, O_C)$ given by the bundle $O_{C[\varepsilon]}(\tilde{Q} - Q)$. But by the computation done above, if we write $\omega = f(t)dt$ then the value we find is just $f(Q)$, which is also the evaluation of ω at the tangent vector $\tilde{Q}$. As this holds for all points Q, this means precisely that $j^*\alpha = \omega$, as claimed in (ii). □

GaussMapdef **(14.5)** As $\mathrm{Pic}_{C/k}$ is a group scheme, its tangent bundle is globally trivial. To be precise, using the translations we get a natural identification of the tangent bundle of $\mathrm{Pic}_{C/k}$ with $O_{\mathrm{Pic}_{C/k}} \otimes_k T_{J,0}$. For $Q \in C(k)$ the tangent map $Tj_Q \colon T_{C,Q} \to T_{\mathrm{Jac}^1(C), j(Q)}$ can therefore be viewed as a map $\gamma_Q \colon T_{C,Q} \to T_{J,0}$. Alternatively, γ_Q is the map on tangent spaces induced by $t_{-j(Q)} \circ j \colon C \to J$. By (i) of the theorem γ_Q is injective. Hence $\gamma_Q(T_{C,Q})$ is a line in $T_{J,0}$, or equivalently, a point $\gamma(Q) \in \mathbb{P}(T_{J,0})\big(k\big)$. In this way we obtain a well-defined morphism

$$\gamma \colon C \to \mathbb{P}(T_{J,0})\,,$$

called the *Gauss map*. As an immediate corollary of the theorem and its proof we find that this Gauss map is in fact nothing but the canonical map of C.

Gaussmap **(14.6) Corollary.** *The Gauss map $C \to \mathbb{P}(T_{J,0}) \cong \mathbb{P}^{g-1}$ that assigns to a point P the tangent space to $j(C)$ at $j(P)$ translated to the origin, coincides with the canonical map $\varphi \colon C \to \mathbb{P}(H^0(C, \Omega^1_C)^\vee)$.*

§2. *Comparison with the g-th symmetric power of C.*

Let C be a proper smooth curve of genus g over a field k. Let $n \in \mathbb{Z}_{\geqslant 1}$. The n-th symmetric power of C over k, notation $C^{(n)}$, is defined as

$$C^{(n)} := C^n/\mathfrak{S}_n\,,$$

the quotient of C^n under the action of the symmetric group $\mathfrak{S}_n$ via permutation of the coordinates. (Of course, C^n stands for the n-fold product $C \times_k \cdots \times_k C$ over k.) Note that in (5.16) we have used a different notation for symmetric powers; this was necessary to avoid confusion with the pull-back of a scheme in characteristic p via the absolute Frobenius. In this chapter we shall use the more common notation $C^{(n)}$.

For $m, n \geqslant 0$ the natural isomorphism $C^m \times C^n \xrightarrow{\sim} C^{m+n}$ induces a morphism $s_{m,n} \colon C^{(m)} \times C^{(n)} \to C^{(m+n)}$ that we shall refer to as the sum map. The terminology comes from the fact,

explained in more detail below, that $C^{(m)}$ is the variety of effective divisors of degree m on C; with this interpretation the morphism $s_{m,n}$ is the map that sends a pair of effective divisors (D, E) to their sum $D + E$. More generally, given non-negative integers $m_1, \ldots, m_r$ we have a natural morphism $s = s_{m_1,\ldots,m_r}\colon C^{(m_1)} \times \cdots \times C^{(m_r)} \to C^{(M)}$, where $M = m_1 + \cdots + m_r$.

C(n)smooth **(14.7) Lemma.** *Let C be a proper smooth curve over k. Let $n \in \mathbb{Z}_{\geqslant 1}$.*

(i) *Suppose given a partition $n = m_1 + \cdots + m_r$ and points $P_1, \ldots, P_r \in C(k)$ with $P_i \neq P_j$ if $i \neq j$. Write $m_iP_i \in C^{(m_i)}(k)$ for the image of the point $(P_i, \ldots, P_i) \in C^{m_i}$ under the quotient map $C^{m_i} \to C^{(m_i)}$. Then the sum morphism $s\colon C^{(m_1)} \times \cdots \times C^{(m_r)} \to C^{(n)}$ is étale at the point $(m_1P_1, \ldots, m_rP_r)$.*

(ii) *The n-th symmetric power $C^{(n)}$ is a smooth k-variety.*

The "divisor-like" notation for points of the symmetric powers of C will be further justified below.

Note that the action of $\mathfrak{S}_n$ on C^n is not free but that, nevertheless, the quotient $C^{(n)}$ is smooth over k. It is essential for this that C is a curve; a similar conclusion does not hold in general for the symmetric powers of higher-dimensional varieties.

Proof. Part (i) is an easy application of the result in Exercise (4.5)(ii). For the proof of (ii) we may assume that k is algebraically closed, and by (i) and induction on n we only need to show that $C^{(n)}$ is non-singular at points of the form nP for $P \in C(k)$. (Here again nP is the image of $(P, \ldots, P) \in C^n(k)$.) By part (i) of Exercise (4.5) the completed local ring of $C^{(n)}$ at nP is isomorphic to the ring of $\mathfrak{S}_n$-invariants in $\hat{O}_{C^n,(P,\ldots,P)}$. But $\hat{O}_{C^n,(P,\ldots,P)}$ is isomorphic to the formal power series ring $k[\![t_1, \ldots, t_n]\!]$, with $\mathfrak{S}_n$ acting via permutation of the variables. The subring of invariants is the formal power series ring $k[\![\sigma_1, \ldots, \sigma_n]\!]$ in the elementary symmetric polynomials σ_i, and this is a regular ring. □

C(n)andDiv **(14.8)** As before, let C/k be a smooth proper curve. If $k \subset \overline{k}$ is an algebraic closure then to give a $\overline{k}$-valued point of $C^{(n)}$ is the same as giving an unordered n-tuple of $\overline{k}$-valued points $\{P_1, \ldots, P_n\}$, or, what is the same, an effective divisor $P_1 + \cdots + P_n$ of degree n. This interpretation of $C^{(n)}$ as the variety parameterising effective divisors of degree n in fact works over an arbitrary basis. To explain this in detail we need the notion of an effective relative Cartier divisor. See the first few pages of Katz and Mazur [1] for an excellent introduction. Let us summarize what we need.

If T is any k-scheme then an effective (relative) Cartier divisor in $C_T := C \times_k T$ over T is a closed subscheme $D \subset C_T$ which is flat over T and such that the ideal sheaf $I_D \subset O_{C_T}$ is an invertible O_{C_T}-module. As C is proper over k, such a Cartier divisor is proper over T too, and O_D is finite locally free as an O_T-module. The rank of O_D as an O_T-module (which is a locally constant function on T) is called the degree of D.

An effective relative Cartier divisor in C_T/T can also be described as the isomorphism class of a pair (L, s), where L is an invertible sheaf on C_T and $s \in H^0(C_T, L)$ is a global section, such that the quotient sheaf

$$L/s(O_{C_T}) := \mathrm{Coker}(O_{C_T} \xrightarrow{s} L)$$

is flat over T. Two such pairs (L, s) and (L', s') are considered to be isomorphic if there is an isomorphism of O_{C_T}-modules $h\colon L \xrightarrow{\sim} L'$ with $h(s) = s'$. The correspondence is that to a pair (L, s) we associate the zero scheme $D = Z(s) \subset C_T$ of the section s; conversely, to $D \subset C_T$ we associate the pair (I_D^{-1}, s), where s is the global section of $I_D^{-1} = \mathit{Hom}(I_D, O_{C_T})$ given by the inclusion $I_D \hookrightarrow O_{C_T}$.

Effective Cartier divisors in C_T/T can be added. If D corresponds to the pair (L,s) and D' to the pair (L',s') then $D+D'$ is the effective Cartier divisor corresponding to $(L\otimes L', s\otimes s')$. rel

If $D\subset C_T$ is an effective Cartier divisor of degree n over T and $h\colon T'\to T$ is a morphism of k-schemes then we can pull D back to an effective Cartier divisor $D_{T'}=h^*D\subset C_{T'}$ of degree n over T'. In this way we obtain a contravariant functor

$$\mathrm{Div}^{\mathrm{eff},n}_{C/k}\colon \mathsf{Sch}_{/k}\to \mathsf{Sets} \qquad \text{with} \quad \mathrm{Div}^{\mathrm{eff},n}_{C/k}(T)=\left\{\begin{array}{c}\text{effective Cartier divisors}\\ D\subset C_T \text{ of degree } n \text{ over } T\end{array}\right\}.$$

In the case considered here, this functor is the same as the Hilbert functor $\mathrm{Hilb}^n_{C/k}$ of closed subschemes of C that are locally free of rank n over the basis. See for instance BLR, Section 8.2 or SGA4, Exp. ?? for further details.

If $P\in C(T)$ is a T-valued point of C then this gives a section $T\to C_T$ of the structural morphism, whose image is an effective Cartier divisor $P\subset C_T$ of degree 1 over T. More generally, for $P_1,\dots,P_n\in C(T)$ we get an effective Cartier divisor $P_1+\cdots+P_n$ of degree n. In this way we obtain a morphism of functors $C^n\to \mathrm{Div}^{\mathrm{eff},n}_{C/k}$. But it is obvious that this morphism is $\mathfrak{S}_n$-invariant; hence it factors through a morphism

$$h\colon C^{(n)}\to \mathrm{Div}^{\mathrm{eff},n}_{C/k}.$$

C(n)=Div **(14.9) Proposition.** *The morphism h is an isomorphism, so $C^{(n)}\xrightarrow{\sim}\mathrm{Div}^{\mathrm{eff},n}_{C/k}$.*

Proof (sketch). We need a construction to go back from an effective Cartier divisor $D\subset C_T$ of degree n over T to a T-valued point of $C^{(n)}$. If $f\colon C_T\to T$ is the structural morphism then f_*O_D is an O_T-algebra that is locally free of rank n as an O_T-module. If $z\in O_D\big(f^{-1}(U)\big)$ for some open $U\subset T$ then multiplication by z is an $O_T(U)$-linear endomorphism of $O_D\big(f^{-1}(U)\big)$ which has a determinant $\det_{D/T}(z)\in O_T(U)$. This gives a map of sheaves $\det_{D/T}\colon f_*O_D\to O_T$ which is multiplicative and has the property that $\det_{D/T}(c\cdot z)=c^n\cdot\det_{D/T}(z)$ for local sections c of O_T and z of f_*O_D. Writing $S^n(f_*O_D)\subset\otimes^n_{O_T}(f_*O_D)$ for the sub-O_T-algebra of symmetric tensors, one shows that there is a unique homomorphism of O_T-algebras $\mathfrak{d}\colon S^n(f_*O_D)\to O_T$ with the property that $\mathfrak{d}(z\otimes\cdots\otimes z)=\det_{D/T}(z)$ for all local sections z. (To prove this we may work locally on T and assume that f_*O_D is free as an O_T-module.) In terms of schemes this means we have a morphism

$$\mathfrak{d}\colon T\to D^{(n)}:=D^n/\mathfrak{S}_n=\mathrm{Spec}\big(S^n(f_*O_D)\big)$$

which is a section of the structural morphism $D^{(n)}\to T$. Composing this with the canonical morphism $D^{(n)}\to C^{(n)}$ induced by the inclusion $D\hookrightarrow C$ we obtain a T-valued point of $C^{(n)}$. Now one verifies that this gives an inverse of the morphism h. □

alphanDef **(14.10)** We shall henceforth identify $C^{(n)}$ with $\mathrm{Div}^{\mathrm{eff},n}_{C/k}$ via the above isomorphism h.

Earlier we have studied the morphism $j\colon C\to \mathrm{Jac}^1(C)$, given on points by $P\mapsto O_C(P)$. We can generalize this to a morphism $j^{(n)}\colon C^{(n)}\to\mathrm{Jac}^n(C)$, as follows. If $P_1,\dots,P_n\in C(T)$ for some k-scheme T then $j(P_1)+\cdots+j(P_n)$ is a T-valued point of $\mathrm{Jac}^n(C)$, and this defines a morphism $C^n\to\mathrm{Jac}^n$. As this morphism is clearly invariant under $\mathfrak{S}_n$, we get an induced morphism $j^{(n)}\colon C^{(n)}\to\mathrm{Jac}^n(C)$; this is the morphism in which we are interested. In terms

of Cartier divisors, $j^{(n)}$ sends an effective Cartier divisor $D \subset C_T$ of degree n over T to the class in $\mathrm{Jac}^n(C)\big(T\big)$ represented by $O_{C_T}(D)$. Better still, if we describe a Cartier divisor as the isomorphism class of a pair (L,s), then $j^{(n)}$ is simply the forgetful map $\big[(L,s)\big] \mapsto [L]$. In particular, this last description makes it clear that the k-valued points of the fibre of $j^{(n)}$ over $[L]$ form the projective space $\mathbb{P}\big(H^0(C,L)\big)$. This is Abel's theorem that the fibres of $j^{(n)}$ are precisely the linear systems of degree n. In particular, all (non-empty) fibres are projective spaces. We shall now give the precise details and prove this scheme-theoretically.

j(n)fibres **(14.11) Abel's Theorem.** *Let L be a line bundle of degree n on C. Then the (scheme-theoretic) fibre of the morphism $j^{(n)}\colon C^{(n)} \to \mathrm{Jac}^n(C)$ over the point $[L]$ is $\mathbb{P}\big(H^0(C,L)\big)$, the complete linear system of effective divisors D with $O_C(D) \cong L$.*

Proof. Write $\Phi \subset C^{(n)}$ for the scheme-theoretic fibre of $j^{(n)}$ over $[L]$, and let $\mathbb{P} := \mathbb{P}\big(H^0(C,L)\big)$. Let $f\colon T \to \mathrm{Spec}(k)$ be a k-scheme and consider the cartesian diagram

$$\begin{array}{ccc} C_T & \xrightarrow{g} & C \\ {\scriptstyle p_T}\big\downarrow & & \big\downarrow{\scriptstyle p} \\ T & \xrightarrow{f} & \mathrm{Spec}(k) \end{array} .$$

By definition, $\mathbb{P} = \mathrm{Proj}\big(\mathrm{Sym}^\bullet\big((p_*L)^\vee\big)\big)$. A T-valued point of $\mathbb{P}$ is given by a line bundle M on T together with a surjective homomorphism $t\colon f^*\big((p_*L)^\vee\big) \to M$, where two such pairs (M,t) and (M',t') are considered equivalent if there exists an isomorphism $\alpha\colon M \xrightarrow{\sim} M'$ with $\alpha\circ t = t'$; see EGA II, Prop. 4.2.3. By the projection formula, $t = p_{T,*}(s)$ for a unique global section $s \in H^0(C_T, g^*L \otimes p_T^*M)$, and the pair $(g^*L \otimes p_T^*M, s)$ defines a T-valued point of Φ. As this construction is functorial in T, it defines a morphism of schemes $\iota\colon \mathbb{P} \to \Phi$ over k. Conversely, if (L',s) is a T-valued point of Φ then $L' \cong g^*L \otimes p_T^*M$ for some line bundle M on T, and the pair $\big(M, p_{T,*}(s)\big)$ defines a T-valued point of $\mathbb{P}$. This gives an inverse of ι, which therefore is an isomorphism. □

j(n)birat **(14.12) Corollary.** *Let C/k be a smooth proper curve of genus $g \geqslant 1$. For $0 \leqslant n \leqslant g$ the morpism $j^{(n)}$ is a birational morphism from $C^{(n)}$ to its image in $\mathrm{Jac}^n(C)$. For $n \geqslant g$ the morphism $j^{(n)}$ is surjective.*

Proof. We may assume that k is algebraically closed. If $n \geqslant g$ and $[L] \in \mathrm{Jac}^n(C)\big(k\big)$ then it is immediate from Riemann-Roch that L is effective, so $[L]$ is in the image of $j^{(n)}$.

Now suppose $1 \leqslant n \leqslant g$. As the dimensions of the fibres of $j^{(n)}$ vary in an upper-semicontinuous manner, it suffices to show that there exists an effective divisor D of degree n such that $h^0(D) = 1$. Indeed, if we know this then it follows that there is a non-empty open $U \subset C^{(n)}$ such that $j^{(n)}_{|U}$ is an immersion, which is what we assert. We proceed by induction on $n \leqslant g$. For $n = 1$ the assertion is clear, as the assumption that $g \geqslant 1$ implies that $h^0(P) = 1$ for any point $P \in C(k)$. Suppose then that $2 \leqslant n \leqslant g$ and that we have an effective divisor E of degree $n-1$ with $h^0(E) = 1$. Let K be a canonical divisor of C. Riemann-Roch gives $h^0(K-E) = g+1-n \geqslant 1$, so $K-E$ is effective. Now choose any point $Q \in C$ which is not a base point of the linear system $|K-E|$. Then $h^0(K-E-Q) = h^0(K-E) - 1$, and again by Riemann-Roch $E+Q$ has $h^0(E+Q) = 1$. □

ThetaDef **(14.13) Definition.** Let C be a complete, non-singular curve of genus $g \geqslant 1$. For an

integer n with $0 \leqslant n \leqslant g$ we define $W_n \subset \mathrm{Jac}^n(C)$ to be the image of the morphism $j^{(n)}\colon C^{(n)} \to \mathrm{Jac}^n(C)$. For $n = g-1$ we usually write

$$\Theta \subset \mathrm{Jac}^{g-1}(C)$$

for W_{g-1}; it is called the theta divisor.

Note that W_n is a reduced and irreducible closed subscheme of $\mathrm{Jac}^n(C)$, as it is the image of the reduced and irreducible scheme $C^{(n)}$ under the proper morphism $j^{(n)}$. By construction, W_n parametrizes the effective line bundles of degree n on C. Also note that, by the Corollary, Θ is indeed a divisor in $\mathrm{Jac}^{g-1}(C)$. We further remark that W_0 is the origin of J, that $W_1 = j(C)$, and that $W_g = \mathrm{Jac}^g(C)$.

In the rest of this chapter, whenever we discuss the theta divisor, we assume that our curve has genus $g \geqslant 1$. Most of the theory works fine in the case $g = 0$, too, if we define Θ to be the empty divisor in $\mathrm{Jac}^{g-1}(C) \cong \mathrm{Spec}(k)$. But as we have seen in Example (14.3), there is not much interest in developing the theory of Jacobians for $g = 0$.

In view of its importance we highlight the case $n = g$ of Corollary (14.12). The dimensions of $C^{(g)}$ and $\mathrm{Jac}^g(C)$ are equal and $j^{(g)}$ is surjective.

Jacobiinversion **(14.14) Jacobi's Inversion Theorem.** *The morphism $j^{(g)}\colon C^{(g)} \to \mathrm{Jac}^g(C)$ is a birational equivalence.*

So roughly speaking, $\mathrm{Jac}^g(C)$ is "$C^{(g)}$ with the linear systems contracted". (Recall that the only morphisms from a projective space to an abelian variety are the constant maps, cf. Prop. (1.7).) We shall discuss some examples of low genus in ?? below.

Corollary (14.12) also implies that the cycle classes of the subschemes $W_n \subset \mathrm{Jac}^n(C)$ are, up to a factor, just the Pontryagin powers of the class of the curve. Here we define Pontryagin products

$$*\colon \mathrm{CH}\big(\mathrm{Jac}^d(C)\big) \times \mathrm{CH}\big(\mathrm{Jac}^e(C)\big) \to \mathrm{CH}\big(\mathrm{Jac}^{d+e}(C)\big)$$

by the usual rule $\alpha * \beta = m_*(\alpha \times \beta)$, where $m\colon \mathrm{Jac}^d(C) \times \mathrm{Jac}^e(C) \to \mathrm{Jac}^{d+e}(C)$ is the addition map. The precise result is then as follows.

CycClassesWn **(14.15) Corollary.** *Assume C has genus $g > 0$. Let $w_n \in \mathrm{CH}^{g-n}\big(\mathrm{Jac}^n(C)\big)$ be the cycle class of $W_n \subset \mathrm{Jac}^n(C)$. Write $\gamma = w_1$, which is the class of the 1-cycle $j(C) \subset \mathrm{Jac}^1(C)$. Then for $0 \leqslant n \leqslant g$ we have $\gamma^{*n} = n!w_n$. As particular instances of this we have*

$$\gamma^{*(g-1)} = (g-1)!\,\theta\,, \qquad \text{and} \qquad \gamma^{*g} = g!\,\big[\mathrm{Jac}^g(C)\big]\,,$$

where $\theta = w_{g-1} \in \mathrm{CH}^1(\mathrm{Jac}^{g-1}(C))$ is the class of the theta divisor Θ and where $\big[\mathrm{Jac}^g(C)\big] = w_g \in \mathrm{CH}^0(\mathrm{Jac}^g(C))$ is the fundamental class of $\mathrm{Jac}^g(C)$.

Proof. We identify C with its image $j(C)$ in $\mathrm{Jac}^1(C)$. Consider the addition map $\big(\mathrm{Jac}^1(C)\big)^n \to \mathrm{Jac}^n(C)$. The restriction of this map to C^n is generically finite of degree $n!$ to its image W_n. Taking cycle classes and using the definition of the Pontryagin product gives the relation $\gamma^{*n} = n!w_n$. □

In the study of the morphisms $j^{(n)}\colon C^{(n)} \to \mathrm{Jac}^n(C)$ we see a clear transition from the case $n \leqslant g$, when $j^{(n)}$ is generically finite to its image, to the case $n > 2g-2$, when all fibres have

dimension $n+1-g$, and $C^{(n)}$ is in fact a projective bundle over $\mathrm{Jac}^n(C)$. This is a geometric incarnation of the Riemann-Roch Theorem for curves. For the theory of Jacobians the cases $n = g-1$ and $n = g$ are most important. We shall further discuss the case $n > 2g-2$ in ??.

§3. *Universal line bundles and the Theta divisor.*

PBonCxJac **(14.16)** Suppose the curve C has a k-valued point $\varepsilon \in C(k)$. Then on $C \times \mathrm{Pic}_{C/k}$ we have a universal line bundle $\mathscr{P} = \mathscr{P}_C$ with rigidification along $\{\varepsilon\} \times \mathrm{Pic}_{C/k}$, which we call the *Poincaré bundle*. Its universal property is that given any k-scheme T and a line bundle M on $C_T := C \times_k T$ together with a trivialisation along $\{\varepsilon\} \times T$, there is a unique morphism of k-schemes $h\colon T \to \mathrm{Pic}_{C/k}$ such that $M \cong h^*\mathscr{P}$ as rigidified line bundles.

This Poincaré bundle depends on the chosen point ε in the following way. Let ε_1 and ε_2 be k-rational points of C, and let $\mathscr{P}_1$ and $\mathscr{P}_2$ be the associated Poincaré bundles. Consider the morphism

$$(\varepsilon_2, \mathrm{id})\colon \mathrm{Pic}_{C/k} = \mathrm{Spec}(k) \times_k \mathrm{Pic}_{C/k} \to C \times_k \mathrm{Pic}_{C/k}\,,$$

which is a section of the second projection $\mathrm{pr}_2\colon C \times \mathrm{Pic}_{C/k} \to \mathrm{Pic}_{C/k}$. Then we have $\mathscr{P}_2 \cong \mathscr{P}_1 \otimes \mathrm{pr}_2^*(\varepsilon_2, \mathrm{id})^*\mathscr{P}_1^{-1}$.

UnivDivOnCC(n) **(14.17)** Without the assumption that C has a k-rational point, it is not clear how to define or construct a universal line bundle on $C \times \mathrm{Pic}_{C/k}$, or on the various connected components $C \times \mathrm{Jac}^n(C)$. In fact, it is known that in general there does not exist a universal line bundle over $C \times \mathrm{Jac}^n(C)$; see Mestrano and Ramanan [1]. (However, as we shall see in Thm. (14.20), for some values of n there does always exist a universal line bundle on $C \times \mathrm{Jac}^n(C)$.)

By contrast, over $C \times C^{(n)}$ with $n \geqslant 1$ we can easily write down a universal relative divisor. Namely, consider the morphism $s_n\colon C \times C^{(n-1)} \to C \times C^{(n)}$ given on points by $(x, D) \mapsto (x, D+x)$. Here we interprete points of $C^{(n-1)}$ and $C^{(n)}$ as divisors on C. The morphism s_n is a closed immersion that realizes $C \times C^{(n-1)}$ as an irreducible divisor in $C \times C^{(n)}$. Let us write $\mathscr{D}_n \subset C \times C^{(n)}$ for this divisor. We view $\mathscr{D}_n$ as a relative effective Cartier divisor over $C^{(n)}$; as such it has degree n. As we shall show next, $\mathscr{D}_n$ is a universal divisor in $C \times C^{(n)}$, by which we mean that for any effective divisor E on C of degree n, the restriction of $\mathscr{D}_n$ to $C \times \{E\}$ is precisely E.

It is useful for us to reformulate the assertion that $\mathscr{D}_n$ is a universal divisor. Namely, if T is a k-scheme and if D is a relative effective Cartier divisor of degree n on C_T over T then by Prop. (14.9) we have a corresponding classifying morphism $\psi(D)\colon T \to C^{(n)} = \mathrm{Div}^{\mathrm{eff},n}_{C/k}$. Applying this with $T = C^{(n)}$ and $D = \mathscr{D}_n$ we obtain a morphism $\psi(\mathscr{D}_n)\colon C^{(n)} \to C^{(n)}$. The assertion that $\mathscr{D}_n$ is a universal relative divisor then just means that $\psi(\mathscr{D}_n) = \mathrm{id}_{C^{(n)}}$.

DnIsUnivDiv **(14.18) Proposition.** *Let $n \geqslant 1$ and consider the relative effective Cartier divisor $\mathscr{D}_n \subset C \times C^{(n)}$ as just defined. Then $\mathscr{D}_n$ is a universal divisor in $C \times C^{(n)}$ over $C^{(n)}$, in the sense that the classifying morphism $\psi(\mathscr{D}_n)\colon C^{(n)} \to C^{(n)}$ is the identity.*

Proof. As $C^{(n)}$ is irreducible, it suffices to show that $\psi(\mathscr{D}_n)$ is the identity on the open part $U \subset C^{(n)}$ consisting of divisors of the form $E = P_1 + \cdots + P_n$ with $P_1, \ldots, P_n$ mutually distinct. But for such E it is immediate from the definition of the map s_n that $(\mathscr{D}_n)_{|C \times \{E\}} = E$. □

Even if this construction does not directly give us a universal line bundle on $C \times \mathrm{Jac}^n(C)$, it will be useful in our study of the Jacobian.

nvolutJacg-1Rem **(14.19) Remark.** We have natural morphisms $\nu_n\colon \mathrm{Jac}^n(C) \to \mathrm{Jac}^{2g-2-n}(C)$ given by $[L] \mapsto \big[\omega_C \otimes L^{-1}\big]$. Note that $\nu_{2g-2-n} \circ \nu_n$ is the identity on $\mathrm{Jac}^n(C)$. In particular, on $\mathrm{Jac}^{g-1}(C)$ we obtain an involution $\nu = \nu_{g-1}$. By Riemann-Roch, if L is a line bundle on C of degree $g-1$ then $h^0(L) = h^0\big(\omega_C \otimes L^{-1}\big)$; hence $\Theta \subset \mathrm{Jac}^{g-1}(C)$ is mapped into itself under ν.

UnivBunCJacg **(14.20) Proposition.** *Consider the morphism $f\colon C \times \mathrm{Jac}^g(C) \to \mathrm{Jac}^{g-1}(C)$ given on points by $(x, M) \mapsto M(-x)$. Then $f^*O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ is a universal line bundle on $C \times \mathrm{Jac}^g(C)$.*

Proof. Let $V \subset \mathrm{Jac}^g(C)$ be the open subset of points $[M]$ with $h^0(M) = 1$. The line bundle $f^*O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ on $C \times \mathrm{Jac}^g(C)$ gives rise to a morphism $\psi\colon \mathrm{Jac}^g(C) \to \mathrm{Pic}_{C/k}$, and the assertion that $f^*O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ is a universal line bundle just means that ψ is the identity map on $\mathrm{Jac}^g(C)$. It suffices to show that ψ is the identity when restricted to V. (Cf. the proof of Prop. (14.18).)

Let $U \subset C^{(g)}$ be the preimage of V under $j^{(g)}\colon C^{(g)} \to \mathrm{Jac}^g(C)$. By Abel's Theorem $j^{(g)}$ restricts to an isomorphism $U \xrightarrow{\sim} V$. It then follows from Prop. (14.18) that the restriction of $O_{C \times C^{(g)}}(\mathscr{D}_g)$ to $C \times U \cong C \times V$ defines a universal line bundle on $C \times V$ over V. Recall that $\mathscr{D}_g$ was obtained as the image of the map $s_g\colon C \times C^{(g-1)} \hookrightarrow C \times C^{(g)}$. Further, we have a commutative diagram

$$\begin{array}{ccc} C \times C^{(g-1)} & \xrightarrow{s_g} & C \times C^{(g)} \\ {\scriptstyle \mathrm{id}_C \times j^{(g-1)}}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{id}_C \times j^{(g)}} \\ C \times \mathrm{Jac}^{g-1}(C) & \underset{t}{\xrightarrow{\sim}} & C \times \mathrm{Jac}^g(C) \end{array}$$

where $t\colon C \times \mathrm{Jac}^{g-1}(C) \xrightarrow{\sim} C \times \mathrm{Jac}^g(C)$ is the isomorphism given by $(x, N) \mapsto \big(x, N(x)\big)$. Note that $h^0\big(N(x)\big) = 1$ implies that $h^0(N) \leqslant 1$; so, again by Abel's Theorem, the morphism $\mathrm{id}_C \times j^{(g-1)}$ is an embedding on the preimage of $C \times V \subset C \times \mathrm{Jac}^g(C)$. The divisor in $t^{-1}(C \times V)$ that we obtain in this way is just the restriction of $C \times \Theta = \mathrm{pr}_2^*(\Theta)$. So the conclusion is that $(t^{-1})^*\mathrm{pr}_2^* O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ is a universal line bundle when restricted to $C \times V$. This gives what we want because $\mathrm{pr}_2 \circ t^{-1}\colon C \times \mathrm{Jac}^g(C) \to \mathrm{Jac}^{g-1}(C)$ is precisely the morphism f given by $(x, M) \mapsto M(-x)$. □

hetaPullbackCor **(14.21) Corollary.** *Let $j\colon C \to \mathrm{Jac}^1(C)$ be the natural map. Let L be a line bundle of degree $g-2$ on C, and let $t_L\colon \mathrm{Jac}^1(C) \to \mathrm{Jac}^{g-1}(C)$ be the translation over $[L]$. Then the pull-back of $O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ via $t_L \circ j\colon C \to \mathrm{Jac}^{g-1}(C)$ is isomorphic to $\omega_C \otimes L^{-1}$.*

Proof. With ν as in Remark (14.19), consider the morphism $\nu \circ t_L \circ j\colon C \to \mathrm{Jac}^{g-1}(C)$; it is given by $x \mapsto \omega_C \otimes L(x)^{-1} = \big(\omega_C \otimes L^{-1}\big)(-x)$. By the proposition, the pull-back of $O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ under this morphism is isomorphic to $\omega_C \otimes L^{-1}$. On the other hand, ν is an involution of $\mathrm{Jac}^{g-1}(C)$ that preserves Θ, so $\nu^* O_{\mathrm{Jac}^{g-1}(C)}(\Theta) = O_{\mathrm{Jac}^{g-1}(C)}(\Theta)$ and we obtain the corollary. □

In terms of divisors, the corollary says the following. Let K be a canonical divisor on C, and let D be a divisor of degree $g-2$. Consider the translated theta divisor $\Theta_D \subset \mathrm{Jac}^1(C)$. It is given by the reduced irreducible subscheme whose points are the $[M] \in \mathrm{Jac}^1(C)$ such that $M(D)$ is effective. Then the pull-back of Θ_D under the canonical morphism $j\colon C \to \mathrm{Jac}^1(C)$ is linearly equivalent to $K - D$.

PPolJacDiscuss **(14.22)** As another application of Prop. (14.20) we shall next prove that the theta divisor gives rise to a principal polarization $\varphi_\Theta\colon J \xrightarrow{\sim} J^t$ of the Jacobian. Note that by the construction

explained in Chapter 11, § 4, the line bundle $O_{\mathrm{Jac}^{g-1}}(\Theta)$ indeed gives rise to a homomorphism $\varphi_\Theta\colon J \to J^t$. Concretely, we apply Definition (11.43) with the line bundle $O_{\mathrm{Jac}^{g-1}}(\Theta)$ on the J-torsor $\mathrm{Jac}^{g-1}(C)$.

Classically one usually defines the principal polarization of J by first translating the theta divisor to the Jacobian J, avoiding the theory of Chapter 11, § 4. This is done as follows. Let us first assume that there exists a line bundle M of degree $g-1$ on C; in particular this is the case if C has a k-rational point. We have the translation $t_M\colon J = \mathrm{Jac}^0(C) \xrightarrow{\sim} \mathrm{Jac}^{g-1}(C)$, and we can consider the divisor $\Theta_M := t_M^*(\Theta)$ on J. This divisor depends on the choice of M, but up to translations in J it is independent of this choice. In particular, the class of $O_J(\Theta_M)$ in $\mathrm{NS}_{J/k}(k)$, which is the class of Θ_M modulo algebraic equivalence, does not depend on M. (Here we use that $\mathrm{Jac}^{g-1}(C)$ is connected.) It follows from Lemma (7.15), see also (7.26), that the associated homomorphism $\varphi_{\Theta_M}\colon J \to J^t$ is independent of the choice of M, so we may call this homomorphism φ_Θ.

In general, C does not have a line bundle of degree $g-1$ over the given field k. In this case we may choose a finite Galois extension $k \subset K$ such that on C_K we do have a line bundle M of degree $g-1$. The previous construction gives us a homomorphism $\varphi_{\Theta,K}\colon J_K \to J_K^t$. We need to show that this homomorphism is defined over k. To prove this it suffices to show that $\varphi_{\Theta,K}$ is invariant under the natural action of the Galois group $\mathrm{Gal}(K/k)$ on $\mathrm{Hom}(J_K, J_K^t)$. The point here is that, because Θ is defined over k, we have ${}^\sigma(\Theta_M) = \Theta_{{}^\sigma M}$ as divisors on J_K, and as just explained, $\Theta_{{}^\sigma M}$ and Θ_M give the same homomorphism $J_K \to J_K^t$.

This classical construction of course gives the same homomorphism $\varphi_\Theta\colon J \to J^t$ as the homomorphism that is obtained using Def. (11.43). To see this, remark that, with $k \subset K$ as before, we have $\mathrm{Hom}(J, J^t) \hookrightarrow \mathrm{Hom}(J_K, J_K^t)$, so it suffices to verify that the two constructions agree in case C has a line bundle of degree $g-1$. In this case the verification is only a matter of unraveling the definitions; see also ??. Though the two constructions differ in presentation, they are in essence the same.

PPolJacThm **(14.23) Theorem.** *The homomorphism $\varphi_\Theta\colon J \to J^t$ associated to the theta divisor is a principal polarization.*

Proof. We may assume that $k = \overline{k}$ and that $g \geqslant 1$. Choose a point $x_0 \in C(k)$, consider the translated theta divisor $\Theta_0 := t^*_{(g-1)x_0}(\Theta)$ in J, and let $L := O_J(\Theta_0)$ be the corresponding line bundle. Because L is effective, to prove that the associated symmetric homomorphism $\varphi_L = \varphi_\Theta\colon J \to J^t$ is a principal polarization it suffices to show that it is an isomorphism. (Indeed, if this holds then L is non-degenerate, and by Prop. (2.22) it follows that L is ample.)

Let $\Lambda(L) = m^*(L) \otimes \mathrm{pr}_1^*(L)^{-1} \otimes \mathrm{pr}_2^*(L)^{-1}$ be the Mumford bundle on $J \times J$ associated to L. Recall from Def. (2.16) that $K(L)$ is the largest subscheme $K \subset J$ with the property that $\Lambda_{J \times K(L)}$ is trivial. By Thm. (6.18) we have $K(L) = \mathrm{Ker}(\varphi_\Theta)$, so it suffices to prove that $K(L) = \{0\}$.

Let $i\colon C \hookrightarrow J$ be the closed embedding given by $x \mapsto \big[O_C(x_0 - x)\big]$. We have a commutative diagram

$$\begin{array}{ccc} C \times J & \xrightarrow{m \circ (i \times \mathrm{id})} & J \\ {\scriptstyle \mathrm{id}_C \times t_{gx_0}}\big\downarrow\wr & & \wr\big\downarrow{\scriptstyle t_{(g-1)x_0}} \\ C \times \mathrm{Jac}^g(C) & \xrightarrow{\quad f \quad} & \mathrm{Jac}^{g-1}(C) \end{array}$$

where $m\colon J \times J \to J$ is the group law and f is the map $(x, M) \mapsto M(-x)$ of Prop. (14.20). By Prop. (14.20) it follows that the restriction of $\Lambda(L)$ to $C \times J$ (via the closed embedding

$i \times \mathrm{id}\colon C \times J \hookrightarrow J \times J$) is the Poincaré bundle $\mathscr{P}_C$ on $C \times J$ with rigidification along $\{x_0\} \times J$ and $C \times \{0\}$. But the largest subscheme $K' \subset J$ such that $\mathscr{P}_{|C \times K'}$ is trivial, is $K' = \{0\}$. Hence also $K(L) = \{0\}$, as we wanted to prove. □

PPolJacCor **(14.24) Corollary.** *We have* $\deg(\Theta^g) = g!$ *and* $h^0(\mathrm{Jac}^{g-1}(C), \Theta) = 1$.

Proof. This follows from the theorem by the Riemann-Roch Theorem (9.11). □

Our next topic is the connection between theta characteristics and symmetric theta divisors in J.

ThetaChar **(14.25) Definition.** Let C be a curve of genus g over a field k. A theta characteristic on C is a line bundle L such that $L^{\otimes 2} \cong \omega_C$. A theta characteristic L is said to be even (resp. odd) if $h^0(L)$ is even (resp. odd).

ThetaCharFacts **(14.26) Proposition.** *Let k be an algebraically closed field with* $\mathrm{char}(k) \neq 2$. *If C is a curve of genus g over k then C has 2^{2g} theta characteristics, $2^{g-1}(2^g + 1)$ of them even, $2^{g-1}(2^g - 1)$ of them odd.*

An alternative, maybe more satisfactory, definition of the theta divisor is as follows.

We assume that C has a point $P \in C(k)$. Let L be a Poincaré line bundle on $C \times \mathrm{Jac}^{g-1}(C)$, that is, a line bundle L on $C \times \mathrm{Jac}^{g-1}(C)$ which is of degree $g-1$ on all fibres $C \times \{[D]\}$, and such that $L_{|C\times\{[D]\}} \cong O(D)$ for all $[D] \in \mathrm{Jac}^{g-1}(C)$.

We choose an effective divisor E of degree g on C and consider the line bundle $L(E) = L \otimes p_1^* O(E)$ on $C \times \mathrm{Jac}^{g-1}(C)$. Since E is effective we thus have an exact sequence $0 \to L \longrightarrow L(E) \longrightarrow L(E)/L \to 0$. Let $\pi = p_2$ be the projection of $C \times \mathrm{Jac}^{g-1}(C)$ on the second factor. Since we have $H^1(C, O(D)) = (0)$ for any divisor D of degree $2g-1$ on C it follows that $R^1\pi_*(L(E)) = (0)$ and we find the following long exact sequence of sheaves on Jac^{g-1} in cohomology

$$0 \to R^0\pi_* L \longrightarrow R^0\pi_* L(E) \xrightarrow{\alpha} R^0\pi_*(L(E)/L) \longrightarrow R^1\pi_* L \to 0. \tag{6}$$

To be explicit, over $[D]$ we have the exact sequence of fibres

$$0 \to H^0(C, O(D)) \longrightarrow H^0(C, O(D+E)) \longrightarrow O(D+E)_{|E} \longrightarrow H^1(C, O(D)) \to 0.$$

Since $\dim H^0(C, O(D+E)) = g$ for every divisor of degree g it follows that $R^0\pi_*(L(E))$ is a vector bundle of rank g on $\mathrm{Pic}^{(g-1)}(C)$. Also $R^0\pi_*(L(E)/L))$ is a vector bundle of rank g; it can be identified with $L(E)_{|E}$, the direct sum of the fibres of $L(E)$ over the g points of the support of E. So $\alpha : R^0\pi_*(L(E)) \longrightarrow L(E)|E$ is a morphism of vectorbundles on $\mathrm{Pic}^{g-1}(C)$ of the same rank g.

Thetadef **(14.27) Definition.** *The* theta divisor $\Theta \subset \mathrm{Pic}^{(g-1)}(C)$ *is the locus where the determinant of the bundle map α vanishes. It equals the image of* α_{g-1}: $C^{(g-1)} \to \mathrm{Jac}^{g-1}(C)$.

Note that by the local triviality of the two vectorbundles Θ is locally described by the vanishing of a matrix and carries in a natural way a scheme structure. Furthermore, the theta divisor does not depend on the choice of E and L. For example, if we replace E by E' then $\det(\alpha)$ is changed by multiplying with an invertible function. Note that

$$\det(\alpha) \text{ vanishes at } [D] \iff H^0(C, O(D)) \neq (0) \iff H^1(C, O(D)) \neq (0). \tag{7}$$

Therefore the support of Θ coincides with the support of the image that we find the same divisor Θ as above. Since Θ in either definition is reduced we find the same divisor. In particular, it does not depend on the existence of a point P on C.

DetCohomRem **(14.28) Remarks.** (i) Let K be a canonical divisor on C. If D is a divisor on C of degree $g-1$ then $h^0(D) = h^0(K-D)$. So the map $[D] \mapsto [K-D]$ defines an involution of $\mathrm{Jac}^{g-1}(C)$ that sends Θ to itself.

(ii) The sequence (6) shows that the bundle $O(-\Theta)$ represents the "determinant bundle" of the cohomology of L. Its fibre over a point $[D]$ equals

$$\det H^0\big(C, O(D)\big) \otimes_k \det H^1\big(C, O(D)\big)^{-1}$$

cf. Knudson ??

(iii) We have found a canonically defined divisor $\Theta \subset \mathrm{Jac}^{g-1}(C)$. If y is a k-rational point of $\mathrm{Jac}^{g-1}(C)$ then $\Theta_y := t_{-y}(\Theta)$, the translate of Θ over $-y$, is a divisor on $\mathrm{Jac}(C)$. But of course Θ_y is independent of the choice of y only up to translation. So if we speak of the theta divisor on $\mathrm{Jac}(C)$ we mean a divisor (or a divisor class) that is defined up to translation.

Note that we can choose y, at least over $\overline{k}$, in such a way that Θ_y is symmetric, meaning that $(-1)^*\Theta_y = \Theta_y$. Since, as just remarked, Θ is stable under the involution $[D] \mapsto [K - D]$ the classes $y \in \mathrm{Jac}^{g-1}(C)$ for which Θ_y is symmetric are precisely the theta-characteristics, i.e., the divisor classes y for which $2y$ is the canonical class.

We shall now prove that the theta divisor defines a principal polarization, that is, the map φ_Θ: $\mathrm{Jac}(C) \longrightarrow \mathrm{Jac}(C)^t$ is an isomorphism. The reason for this is the fact that the pull-back of the divisor $\Theta - t^*_{[D]}(\Theta)$ to C via α_1 is non-trivial for non-zero $[D]$ of degree $g - 2$.

Jacisppav **(14.29) Theorem.** *Let j: $C \to \mathrm{Jac}^1(C)$ be the natural map. Let D be a divisor of degree $g - 2$ on C. Then the pull-back of $O(\Theta)$ via $t_{[D]} \circ j$: $C \to \mathrm{Jac}^1(C) \to \mathrm{Jac}^{g-1}(C)$ is isomorphic to $O_C(K - D)$. Equivalently, in terms of divisor classes, $j^*(\Theta - [D])$ is linearly equivalent to $K - D$ on C.*

Proof. This calculation was done by Riemann in 1857. It is no restriction of generality to extend the base field so that C has a rational point or even to assume that k is algebraically closed. We shall first prove the result for general D in the following sense. Consider the open subset U' of $\mathrm{Jac}^g(C)$ of divisors D' of degree g with $h^0(D') = 1$ and such that D' is a sum of g distinct points. Since α_g is birational U' is non-empty. We let $U \subset \mathrm{Jac}^{g-2}$ be the corresponding set $\{D = K - D' \colon D' \in U'\}$.

Now for a point P of C the image point $\alpha_1(P)$ lies on the divisor $t^*_D(\Theta)$ if and only if there exists an effective divisor of degree $g - 1$ on C such that $P + E$ is linearly equivalent to $K - D$. We now assume that D lies in U. Then $P + E$ is an effective divisor in $|K - D|$, hence coincides by the assumptions on D' with D'. So $\alpha_1(P)$ lies on $t^*_D(\Theta)$ if and only if P is one of the g points of support of D'. Since the map $C \times \Theta \to \mathrm{Jac}^g(C)$ given by $(P, E) \mapsto P + E$ is generically finite of degree g we see that the pull back under α_1 of the 0-cycle $\alpha_1(C) \cdot t^*_D\Theta$ equals the divisor D'. This proves the result for D in U.

To extend our conclusion to all D of degree $g - 2$ we consider the pull back of $O(\Theta)$ under the addition map m: $\mathrm{Jac}^1(C) \times \mathrm{Jac}^{g-2}(C) \to \mathrm{Jac}^{g-1}(C)$ and the line bundle $M = (\alpha_1 \times \mathrm{id}_{\mathrm{Jac}^{g-2}(C)})^* m^* O(\Theta)$ on $C \times \mathrm{Jac}^{g-2}(C)$. The restriction of M to a fibre $C \times [D]$ is isomorphic to $O(K - D)$ for $[D] \in U$. The restriction to $P \times \mathrm{Jac}^{g-2}(C)$ is $t^*_P O(\Theta)$ with t_P: $\mathrm{Jac}^{g-2}(C) \to \mathrm{Jac}^{g-1}(C)$ translation over $\alpha_1(P)$. So M agrees by the SeeSaw Principle with the Poincaré bundle (the variant for $C \times \mathrm{Jac}^{g-2}(C)$). But this shows that $\alpha_1^* t^*_D O(\Theta)$ is isomorphic to $O_C(K - D)$ for all D of degree $g - 2$. □

Thetapp **(14.30) Conclusion.** *The divisor $\Theta \subset \mathrm{Jac}^{g-1}(C)$ defines a principal polarization on $\mathrm{Jac}(C)$. In particular, $\deg(\Theta^g) = g!$ and $h^0(\mathrm{Jac}(C), O(\Theta)) = 1$.*

Proof. We must show that the map $\varphi_\Theta : \mathrm{Jac}(C) \to \mathrm{Jac}(C)^t$ given by $x \mapsto [t^*_x\Theta - \Theta]$ is an isomorphism. To see this we may extend the base field. Let then D be a fixed divisor of degree $g - 1$ on C. Now Θ defines a principal polarization if and only if $(-1)^*\Theta$ defines a principal polarization. Therefore, we may as well look at $\varphi_{(-1)^*\Theta}$. But by 14.29 we find that $\alpha_1^*(O(t^*_x t^*_{[D]} D\Theta - t^*_{[D]}\Theta)) \cong O_C(D - D')$ with $x + [D] = [D']$. This shows that the pull back of of the Mumford bundle $\Lambda(O(-\Theta))$ is the Poincaré bundle L_P and since the maximal subscheme over which L_P is trivial is (0) it follows that the kernel $K((-1)^*\Theta)$ of $\varphi_{(-1)^*\Theta}$ is trivial. The conclusions $\Theta^g = g!$ and $h^0(X, O(\Theta)) = 1$ follow from (?.?).

We can deduce conclusions on some cycle classes from the geometric results. Recall that the morphism $C^n \to \mathrm{Jac}^n(C)$ is generically finite of degree $n!$ to its image.

Jacclasses **(14.31) Proposition.** *Let $\gamma \in \mathrm{CH}^{g-1}(\mathrm{Jac}^1(C))$ be the class of the 1-cycle $\alpha_1(C)$ and $\theta \in \mathrm{CH}^1(\mathrm{Jac}^{g-1}(C))$ be the class of the theta divisor Θ. Then we have the relations*

$$\gamma^{*(g-1)} = (g-1)!\theta, \quad \gamma^{*g} = g!\, 1_{\mathrm{Jac}^g(C)}, \quad \text{and} \quad \deg(\theta^g) = g!,$$

with $*$ the Pontryagin product.

Proof. The addition map of $\mathrm{Jac}^1(C)^{g-1} \to \mathrm{Jac}^{g-1}(C)$ restricted to $\alpha_1(C)$ is a map $\alpha_1(C)^n \to \Theta$ generically finite of degree $(g-1)!$. This shows that $\gamma^{*(g-1)} = (g-1)!\theta$. Similarly, $\gamma^{*g} = g!\theta$ follows from the fact that $C^g \to \mathrm{Jac}^g(C)$ has degree $g!$. From 14.30 it foolows that $\deg(\theta^g) = g!$. □

§4. *Riemann's Theorem on the Theta Divisor.*

A geometric translation of '`omegaatD`' interprets the tangent space to Θ at a smooth point in the following way. Let $[D = \sum P_i]$ be a smooth point of Θ. Then the projectivized tangent space of Θ translated to the origin is the hyperplane that cuts out on the canonical image $\psi(C)$ the divisor $\sum \psi(P_i)$. But one can also interpret singular points of Θ as Riemann showed in 1857.

RiemannThm **(14.32) Theorem.** *Let D be a divisor of degree $g-1$ on C. Then the multiplicity of the theta divisor $\Theta \subset \mathrm{Jac}^{g-1}(C)$ at $[D]$ is given by*

$$\mathrm{mult}_{[D]}\Theta = h^0(D).$$

Proof. To verify the statement we may extend the base field to an algebraic extension. We know that Θ is a Cartier divisor in $\mathrm{Jac}^{g-1}(C)$, so Θ is locally given by one equation $\vartheta = 0$. We know also that Θ parametrizes effective divisor classes $[D]$ of degree $g-1$ on C and we thus may assume that D is an effective divisor with $h^0(D) = r+1$ and $r \geqslant 0$.

Let m be the maximal ideal of the local ring $O_{J,[D]}$ of J at $[D]$. We must show

$$\vartheta \in m^{r+1}, \quad \vartheta \notin m^{r+2}.$$

We first show that $\vartheta \in m^{r+1}$. For this we choose local parameters $x_1, \ldots, x_g$ at $[D]$ on J and we expand ϑ as

$$\vartheta = \vartheta_1 + \vartheta_2 + \ldots \quad \in k[[x_1, \ldots, x_g]],$$

where ϑ_j is a homogeneous polynomial of degree j in the $x_1, \ldots, x_g$. Note that we may and shall identify the coordinates $x_1, \ldots, x_g$ with a basis $\omega_1, \ldots, \omega_g$ of $H^0(C, \Omega^1_C) = H^1(C, O_C)^\vee \cong T^\vee_{\mathrm{Jac}(C),0}$. We shall show that $\vartheta_1, \ldots, \vartheta_r$ vanish by interpreting them geometrically in the canonical space $\mathbb{P}^{g-1}$. An term ϑ_ℓ is an element of $\mathrm{Sym}^\ell(H^0(C, \Omega^1_C)$ and using the isomorphism $H^0(C^{(g-1)}, \Omega^1_{C^{(g-1)}}) \cong H^0(C, \Omega^1_C)$ we can consider the pull back under α_{g-1} as an element of $\mathrm{Sym}^\ell(H^0(C^{(g-1)}, \Omega^1_{C^{(g-1)}}))$. If $E = \sum P_i$ is a divisor of degree $g-1$ in $|D|$ with support on $g-1$ distinct points P_i with local coordinates t_i at P_i then the pull back $\alpha^*_{g-1}\theta_\ell$ is given by an expression $\sum a_{i_1,\ldots,i_\ell} dt_{i_1} \cdots dt_{i_\ell}$.

Recall that $\psi : C \longrightarrow \mathbb{P}^{g-1}$ is the canonical map given by the sections of Ω^1_C. If $D = \sum P_i$ is an effective divisor of degree $g-1$ and ω an element of $H^0(C, \Omega^1_C)$ then we have by '`omegaatD`'

that $\alpha_{g-1}^*\omega$ vanishes at $D \in C^{(g-1)}$ if and only if $\omega \in H^0(C, K-D)$, or in other words, the hyperplane of $\mathbb{P}^{g-1}$ defined by ω cuts out on C the divisor $\sum_{i=1}^{g-1}\psi(P_i)$.

Consider now $\vartheta_1 = \sum a_i\omega_i$ with $a_i = \partial\vartheta/\partial x_i([D])$. If it is non-zero it defines the tangent space to Θ at $[D]$. Suppose that $r \geqslant 1$. Then $|D|$ is at least 1-dimensional. This means that for any point Q of C there is a divisor $E \in |D|$ which contains Q. The form $\vartheta_1 = \sum a_i\omega_i$ is contained in $H^0(C, K-E)$, i.e., vanishes in Q. So the hyperplane in $\mathbb{P}^{g-1}$ defined by ϑ_1 contains the whole canonical curve. Since this curve spans $\mathbb{P}^{g-1}$ the form $\sum a_i\omega_i$ must vanish identically, i.e. $\vartheta_1 = 0$ and $\vartheta \in m^2$.

Now we consider the next term $\vartheta_2 = \sum a_{ij}\omega_i\omega_j \in \mathrm{Sym}^2(H^0(C, \Omega_C^1)$. It is not difficult to generalize '`omegaatD`' partially and see that the vanishing of $\alpha_{g-1}^*(\sum a_{ij}\omega_i\omega_j)$ at $E \in |D| \subset C^{(g-1)}$ implies that the bilinear form $\sum a_{ij}\omega_i\omega_j$ vanishes at all pairs $(\psi(P_a), \psi(P_b))$ with P_a, P_b in the support of E. Suppose now that $r \geqslant 2$. Since $|D|$ is at least 2-dimensional we can find for each pair P_a, P_b of points on C an effective divisor E in $|D|$ containing P_a and P_b. We see that the bilinear form $\sum a_{ij}\omega_i\omega_j$ vanishes in all pairs $(\psi(Q_a), \psi(Q_b)$. Since the canonical curve $\psi(C)$ spans $\mathbb{P}^{g-1}$ this implies that the bilinear form $\sum a_{ij}\omega_i\omega_j$ vanishes identically. This implies $\vartheta_2 = 0$, i.e. $\vartheta \in m^3$. We leave it to the reader to generalize this argument and show by induction that $\vartheta \in m^{r+1}$.

We now show that $\vartheta \notin m^{r+2}$. We do this by showing that the pull back of the theta divisor under a suitable map $\alpha : C^{(r+1)} \longrightarrow J$ locally at a point $E \in C^{(r+1)}$ lying over $[D]$ consists of $r+1$ (smooth) divisors of the form $C^{(r)}$.

So let D be a divisor of degree $g-1$ with $h^0(D) = r+1$. We choose an effective divisor $E = \sum_{i=1}^{r+1} Q_i$ of degree $r+1$ on C such that

$$h^0(D-E) = 0, \quad h^0(D+E) = h^0(D). \tag{$*$}$$

It is easy to see that such a divisor exists. (Indeed, take successively $Q_{\ell+1}$ outside the base points of $|D - \sum_{j=1}^{\ell} Q_j|$ and $|K - D - \sum_{j=1}^{\ell} Q_j|$ for $\ell = 0, \ldots r$.)

The map we consider is

$$\alpha : C^{(r+1)} \longrightarrow \mathrm{Jac}^{g-1}(C), \quad F \mapsto [D+E-F].$$

Then the pull back of the divisor Θ under α is of the form $\alpha^*(\Theta) = a_1Z_1 + \cdots + a_{r+1}Z_{r+1} + R$, where

$$Z_i = \{F \in C^{(r+1)} : F - Q_i \geqslant 0\} \quad \text{is a divisor isomorphic to } C^{(r)}$$

and where $R = \{F : h^0(D-F) > 0\}$ is a divisor that does not contain E because of (*). So if we prove that the multiplicities a_i of the smooth divisors Z_i are 1 it follows that the divisor $\sum_{i=1}^{r+1} Z_i + R$ has multiplicity $r+1$ at $D \in C^{(r+1)}$. But then Θ cannot have multiplicity greater than $r+1$ at $[D]$ because multiplicities can only increase under pullback and we are done.

For this we consider the tangent map $T\alpha$ of α at a general point $Q_i + A$ with $A \in C^{(r)}$ of Z_i and show that $T\alpha(T_{Z_1, Q_1+A})$ is not contained in the tangent space $T_{\Theta, \alpha(Q_i+A)}$ for $i = 1, \ldots, r+1$, or equivalently, that there exists an $\eta \in H^0(C, \Omega_C^1)$ that vanishes on $T_{\Theta, \alpha(Q_i+A)}$ but with $\alpha^*(\eta) \neq 0$ on T_{Z_i, Q_i+A}.

But recall that η vanishes at the tangent space to Θ at $\alpha(Q_i + A)$ if the divisor of η contains the effective divisors in $|\alpha(Q_i + A)|$. Furthermore, $\alpha^*\eta$ vanishes on the tangent space to Z_i at $Q_i + A$ if the divisor of η contains the divisor A.

But we are free to choose A and E as long as the conditions (*) are satisfied. So first we choose A in $C^{(r)}(k)$ such that $h^0(D-A) = 1$. Let D' be the unique divisor in $|D-A|$. Then we have

$$\alpha(Q_i + A) = [D + E - Q_i - A] = [D' + (E - Q_i)].$$

and we let η_i be a form that vanishes in the effective divisor $D' + (E - Q_i)$. If we now choose our Q_i such that the conditions (*) hold and the Q_i are not contained in the divisors of the η_i for $i = 1, \dots r+1$ then we are done. But the requirements are satisfied on a dense open set. This proves the theorem. □

We refer to the Chapter on Singularities of the Theta divisor for more details on theta and its singularities.

§5. *Examples.*

Like a multifaceted diamond, the Jacobian of a curve reflects the geometry of the curve in a splendid way. A few examples for the low genera should make this clear.

We have already seen in Example (14.3) that $\mathrm{Pic}_{C/k} \xrightarrow{\sim} \mathbb{Z}$ if $g(C) = 0$, so let us start with curves of genus 1.

genus1Exa **(14.33) Example:** $g = 1$**.** For a curve C of genus 1 the Jacobian $J = \mathrm{Jac}^0(C)$ is an elliptic curve. By Thm. (14.4) the natural morphism of curves

$$j\colon C \to \mathrm{Jac}^1(C)$$

is an isomorphism. In particular, C is a J-torsor. Note, however, that C may have no k-rational points. For a concrete example of a curve of genus 1 without rational points, consider the plane cubic C over $\mathbb{Q}$ defined by

$$3x^3 + 4y^3 + 5z^3 = 0\,.$$

This curve has no $\mathbb{Q}$-rational points. The elliptic curve $\mathrm{Jac}(C)$ is the curve defined by

$$x^3 + y^3 + 60z^3 = 0$$

with origin $(1 : -1 : 0)$. See Selmer [1].

The theta divisor $\Theta \subset J = \mathrm{Jac}^{g-1}(C)$ is the origin $O \in J$.

genus2Exa **(14.34) Example:** $g = 2$**.** A curve C of genus 2 is hyperelliptic: the canonical linear system $|K_C|$ defines a morphism $\pi\colon C \longrightarrow \mathbb{P}^1$ of degree 2. This morphism is ramified, but the ramification points need not be rational over the given field.

By Abel's theorem the natural map

$$j^{(2)}\colon C^{(2)} \to \mathrm{Jac}^2(C)$$

is a birational morphism and its fibres are the linear systems of degree 2. For a line bundle L of degree 2 Riemann-Roch gives $h^0(L) = 1 + h^0(\omega_C \otimes L^{-1})$. But $\omega_C \otimes L^{-1}$ has degree 0, so $h^0(\omega_C \otimes L^{-1}) > 0$ only if $L \cong \omega_C$. Hence, for L of degree 2 we have

$$h^0(L) = \begin{cases} 2 & \text{if } L \cong \omega_C; \\ 1 & \text{else.} \end{cases}$$

It follows that the map $C^{(2)} \longrightarrow \mathrm{Jac}^2(C)$ is the blow-up of $\mathrm{Jac}^2(C)$ in the canonical point K_C. The exceptional divisor is the canonical linear system $|K_C| \subset C^{(2)}$, which is just the linear

system of fibres of the morphism π. If $i\colon C \to C$ is the hyperelliptic involution then over $\overline{k}$ the fibres of π are the divisors of the form $P + i(P)$ with $P \in C(\overline{k})$, so we see that $|K_C| \subset C^{(2)}$ is the image of C under the morphism $C \to C^{(2)}$ given by $P \mapsto P + i(P)$. Note that this morphism factors as

$$C \xrightarrow{\pi} \mathbb{P}^1 = |K_C| \hookrightarrow C^{(2)}\,,$$

and in fact π is the quotient morphism of C modulo the action of the group $\langle i \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Now we are back at the description of the Jacobian given in (1.10).

The theta divisor is the image of the morphism $j\colon C \to \mathrm{Jac}^1(C)$ and is isomorphic to C. We see that we find the curve back from the Jacobian together with its polarization. This is in fact true in general; see Torelli's theorem in ('??') below.

genus3Exa **(14.35) Example: $g = 3$.** Let C be a curve of genus 3. We first determine the fibres of the birational morphism $j^{(3)}\colon C^{(3)} \to \mathrm{Jac}^3(C)$. If L is a line bundle of degree 3 then $h^0(L) = 1 + h^0(\omega_C \otimes L^{-1})$ by Riemann-Roch. As $\omega_C \otimes L^{-1}$ has degree 1, it is effective if and only if it is isomorphic to $O_C(P)$ for some $P \in C(k)$. So we find, for L of degree 3, that

$$h^0(L) = \begin{cases} 2 & \text{if } L \cong \omega_C(-P) \text{ for some } P \in C(k); \\ 1 & \text{else.} \end{cases}$$

As the morphism $h\colon C \to \mathrm{Jac}^3(C)$ given by $P \mapsto \omega_C(-P)$ is the composition

$$C \xrightarrow{j} \mathrm{Jac}^1(C) \xrightarrow{[-1]_{\mathrm{Jac}(C)}} \mathrm{Jac}^{-1}(C) \xrightarrow{t_{[\omega_C]}} \mathrm{Jac}^3(C)$$

it follows from Thm. (14.4) that h is a closed immersion. We claim that $j^{(3)}\colon C^{(3)} \to \mathrm{Jac}^3(C)$ is the blowing-up of $\mathrm{Jac}^3(C)$ along $h(C)$. [**to do:** give precise proof]

For the remainder of this example, we treat the hyperelliptic and the non-hyperelliptic case separately. First assume C is not hyperelliptic. In this case the canonical map $C \to \mathbb{P}^2$ gives an embedding of C as a non-singular quartic curve. The fibre of $j^{(3)}$ over the point $\big[\omega_C(-P)\big]$ corresponds to the pencil of lines in $\mathbb{P}^2$ through the point P. More precisely, for each such line ℓ we get a divisor D_ℓ of degree 3 such that $\ell \cap C = P + D_\ell$, and $|K_C - P|$ is the linear system of divisors D_ℓ obtained in this way.

The theta divisor $\Theta \subset \mathrm{Jac}^2(C)$ is the image of the morphism $j^{(2)}\colon C^{(2)} \to \mathrm{Jac}^2(C)$. We claim that in the non-hyperelliptic case $j^{(2)}$ is a closed immersion. This follows from the fact that there are no line bundles L on C of degree 2 with $h^0(L) > 1$, as this would give the existence of a g^1_2 on C, contradicting the assumption that C is not hyperelliptic. (As Thm. (14.11) is a result about the scheme-theoretic fibres of the map $j^{(2)}$, this fact is enough to conclude that $j^{(2)}$ is an immersion.)

The involution ν of the theta divisor $\Theta \subset \mathrm{Jac}^2(C)$ has a nice geometric interpretation in terms of the canonical embedding $C \hookrightarrow \mathbb{P}^2$. Namely, if $D = P + Q$ is an effective divisor of degree 2, let $\ell = \ell_{PQ}$ be the line in $\mathbb{P}^2$ through P and Q. In case $Q = P$ we take ℓ to be the tangent line of C at the point P. Then $\ell \cap C$ is a divisor of degree 4 (counting intersections with their multiplicity) and we can write $\ell \cap C = D + D'$. The involution ν on Θ is then given by $D \mapsto D'$. The fixed points of this involution correspond (working over $k = \overline{k}$) to the $2^{3-1}(2^3 - 1) = 28$ even theta characteristics of C; in the geometric interpretation of ν we see that these correspond to the 28 bitangents of $C \subset \mathbb{P}^2$.

and the linear systems $|D|$ giving rise to non-trivial fibres of $C^{(3)} \longrightarrow \mathrm{Jac}^3(C)$ are exactly the systems $|K - P|$ where P varies through C. That is, they come from the pencils of lines

passing through a point P on C. So the map φ^3 contracts a $\mathbb{P}^1$ for each point of C, i.e. it collapses a $\mathbb{P}^1$-bundle over C. The image in $\mathrm{Jac}^3(C)$ is a copy of C given by $P \mapsto [K-P]$. If C is hyperelliptic with linear system g^1_2 of degree 2 and dimension 1, the positive dimensional fibres of φ^3 are the linear systems $g^1_2 + P$ with P a point of C. Again $\mathbb{P}^1$-bundle over C is collapsed under φ^3.

Consider now the theta divisor $\Theta \subset \mathrm{Jac}^{g-1}(C)$. The fibres of $C^{(2)} \longrightarrow \mathrm{Jac}^2(C)$ are the linear systems of degree 2 that move, i.e. with $h^0(D) > 1$. But a curve of genus g that has a linear system g^1_2 of degree 2 and $\dim |D| = 1$ is necessarily hyperelliptic by Clifford's theorem. So Θ is isomorphic to $C^{(2)}$ in case C is not hyperelliptic.

Now if C is hyperelliptic the system g^1_2 gives rise to a point $[g^1_2] \in \mathrm{Jac}^2(C)$ with a fibre under φ^{-1} that is not just a point. This implies that Θ is obtained from $C^{(2)}$ by contracting a curve $E = \mathbb{P}^1$. Now one checks easily that $E^2 = -2$ on $C^{(2)}$, so the image of E must be a singular point (an ordinary double point).

$$g = 4$$

We distinguish two cases: C is hyperelliptic or not. If C is not hyperelliptic then the image of C under the canonical map $C \to \mathbb{P}^3$ has as image the intersection of a quadric and a cubic. If the quadric Q is smooth and split, i.e. $\mathbb{P}^1 \times \mathbb{P}^1$ then the two projections of Q to the factors $\mathbb{P}^1$ define two linear systems g_1 and g_2 of degree 3 and dimension 1. If the quadric is non-split, then again we have two such linear systems, but they are defined over a quadratic extension of k. If the quadric is singular (but irreducible) then it is a cone over conic and the projection gives one linear system g' of degree 3. What are the linear systems of degree 4 that move? If D is a divisor of degree 4 with $h^0(D) > 1$ then $h^0(K-D) > 0$, so $K - D$ is represented by an effective divisor of degree 2 on C. One can now check here that φ^4 contracts a $\mathbb{P}^1$ bundle over $C^{(2)}$, where $C^{(2)}$ is mapped to $\mathrm{Jac}^4(C)$ by $P_1 + P_2 \mapsto [K - P_1 - P_2]$.

To describe the theta divisor, consider the map $C^{(3)} \longrightarrow \mathrm{Jac}^3(C)$. The fibres are the linear systems of degree 3. But a linear system of degree 3 is contained in the canonical linear system, and one easily sees that we find only the g^1_3 mentioned before. So the morphism $C^{(3)} \longrightarrow \mathrm{Jac}^3(C)$ contracts two copies of $\mathbb{P}^1$ to a singular point on Θ if the quadric Q is smooth, but just one in case Q is singular.

In case C is hyperelliptic the linear systems of degree 4 that move are of the form $[K - P_1 - P_2]$, and these have $h^0(D) = 2$ except for the linear system $2g^1_2$, with $h^0(2g^1_2) = 3$. The linear systems of degree 3 that move are the linear systems composed with the g^1_2: $|g^1_2 + P|$ with P an arbitrary point of C. As one can check this leads to a whole curve of singularities on Θ. We refer to Ch. ?? for a more precise description of the singularities of the theta divisor.

Already some salient features emerge from this exploratory tour: in every case we can recover the curve C from the pair $(\mathrm{Jac}(C), \Theta)$. That this is generally true is Torelli's theorem which we prove in section '`The Theorem of Torelli`'. We also see that as the genus rises the divisor Θ acquires more singularities. In fact, for a curve of genus $g \geqslant 3$ we have $\dim \mathrm{Sing}(\Theta) \geqslant g - 4$ and $= g - 3$ for hyperelliptic curves; for this we refer to Ch. ?? and books on algebraic curves.

§6. *A universal property—the Jacobian as Albanese.*

In this section we deal with a universal property of the Jacobian that is of a covariant nature; this in contrast with the contravariant nature of the Picard functor.

Albanese **(14.36) Proposition.** *Let $P \in C(k)$ and let $\varphi_P\colon C \to J$ be the morphism given on points by $Q \mapsto \big[O_C(Q-P)\big]$. Then every morphism of C to an abelian variety factors uniquely through φ_P.*

Proof. Suppose $\beta\colon C \to X$ is a morphism of C to an abelian variety. Possibly after a translation on X (which does not affect the validity of our assertion) we can assume that $\beta(P) = 0$. For $n \geqslant 1$ let $\beta^{(n)}\colon C^{(n)} \to X$ be the morphism given on points by $[Q_1 + \cdots + Q_n] \mapsto \beta(Q_1) + \cdots + \beta(Q_n)$. By Jacobi's Inversion Theorem we obtain a rational map $b = \beta^{(g)} \circ \big(j^{(g)}\big)^{-1}\colon \mathrm{Jac}^g(C) \dashrightarrow X$, which by Theorem (1.18) extends to a morphism, again denoted by b. Let $t_{gP}\colon J \xrightarrow{\sim} \mathrm{Jac}^g(C)$ be the morphism "translation by gP". Then we have a morphism $b \circ t_{gP}\colon J \to X$ (in fact, even a homomorphism, as the assumption that $\beta(P) = 0$ implies that $b \circ t_{gP}$ sends 0 to 0), and the composition $(b \circ t_{gP}) \circ \varphi_P$ is easily seen to equal β. □

CminusC Though we have a canonical morphism $\alpha_1\colon C \to \mathrm{Jac}^1(C)$ there is no canonical map $C \to J$. As a remedy, there is a canonical map

$$\delta\colon C \times C \to J$$

given on points by $(P, Q) \mapsto [O(P - Q)]$. This morphism contracts the diagonal $\Delta \subset C^2$.

If C is not hyperelliptic then δ gives an isomorphism of $(C \times C) \setminus \Delta$ with its image in J. In case C is hyperelliptic, the map is of degree 2 on $(C \times C) \setminus \Delta$. For more information on the surface $\delta(C \times C) \subset J$ we refer to Chapter ?? in which we study the geometry of the theta divisor.

A variant of this is obtained by considering the surface $C \times C$ and the morphism δ.

Albanese2 **(14.38) Proposition.** *Let $\alpha\colon C \times C \longrightarrow X$ be a morphism to an abelian variety that contracts the diagonal. Then α factors through δ.*

We leave the proof to the reader.

The functor $\mathrm{Pic}^0_{C/k}$ is contravariant, but the universal property of the proposition above points to a covariant aspect. Let C_1 and C_2 be (proper, smooth, absolutely irreducible) curves and $\chi\colon C_1 \to C_2$ a finite morphism. If $P_2 \in C_2(k)$ is a rational point defining $\varphi_P\colon C_2 \longrightarrow \mathrm{Jac}(C_2)$ the composition $\varphi_P\, \chi : C_1 \longrightarrow \mathrm{Jac}(C_1)$ factors through $\mathrm{Jac}(C_1)$ thus giving rise to $\mathrm{Jac}(C_1) \longrightarrow \mathrm{Jac}(C_2)$. This is the 'covariant aspect' we alluded to before. An abelian variety with the universal property expressed in the preceding two propositions is called the Albanese variety.

§7. *Any Abelian Variety is a Factor of a Jacobian.*

Here we show that any abelian variety over an infinite field is a factor of a Jacobian variety. We start with a definition.

(14.38) Definition. *Let C be an algebraic curve on an abelian variety X. We say that C generates the abelian variety X if there is no abelian subvariety of X containing C.*

Note that the inclusion $C \hookrightarrow X$ induces for every positive integer n a morphism $C^{(n)} \longrightarrow X$. Then C generates X if and only if the induced homomorphism $\mathrm{Jac}(C) \longrightarrow X$ is surjective.

AVquoJac **(14.39) Theorem.** *Let X be an abelian variety over an infinite field k of dimension $\geqslant 1$. Then X carries a smooth irreducible curve that generates X.*

Proof. If $\dim(X) = 1$ the result is clear: $C = X$. So we shall suppose now that $g = \dim(X) > 1$. We can embed X into projective space $\mathbb{P}$ using an ample line bundle. By Bertini's theorem (reference?) there exists an open dense subset $U \subset \mathbb{P}^\vee$ parametrizing the hyperplanes H of $\mathbb{P}$ such that $H \cap X$ is a smooth variety. Since k is infinite U possesses a k-rational point and we thus obtain a smooth variety $X_1 = H \cap X$ to which we can apply Bertini's theorem again. Thus, by applying Bertini's theorem $g-1$ times we find a smooth irreducible curve C on X. We must show that C generates X.

Note that the cycle class $[C]$ of C in cohomology or in the Chow group $CH^{g-1}(X)$ is h^{g-1} with h the class of the hyperplane. Suppose now that C does not generate X. By Poincaré's complete irreducibility theorem there exist positive dimensional abelian subvarieties Y and Z of X such that $C \subset Y$ and $Y \times Z \to X$ is an isogeny. Let Γ on Z be an effective divisor which does not contain the finitely many intersection points of Y and Z in X. Look at the divisor $Y \times \Gamma$ which maps finite to one to a divisor D on X. Then the intersection number $C \cdot D$ is zero. On the other hand, since $[C] = h^{g-1}$ and because h is the class of an ample divisor the intersection number $C \cdot D$ must be non-zero. (Use that for an ample divisor the intersection number with any curve is positive, so $H \cdot (H^{g-2} \cap D) > 0$.) This contradiction shows that C generates X and finishes the proof.

QuoJac **(14.40) Corollary.** *If X is an abelian variety over an infinite field k then X is a quotient of a Jacobian variety.*

Proof. After the preceding theorem First remark that the theorem is obviously true for dimension $g = 0$. If $g > 0$ apply the theorem. Then the map $C \to X$ induces a morphism $\mathrm{Jac}(C) \to X$ which is surjective. □

Example. An example of a 2-dimensional abelian variety that is not a Jacobian is given by a product of two elliptic curves with the product polarization. Then the theta divisor consists of $E_1 \times \{0\} \cup \{0\} \times E_2$ and this divisor is reducible, hence cannot be the image of an irreducible curve.

§8. *The Theorem of Torelli.*

A crucial result about Jacobians is Torelli's Theorem that says that we can retrieve the curve from the Jacobian together with its principal polarization.

Torelli **(14.41) Theorem.** (Torelli's Theorem)*Let C_1 and C_2 be two proper smooth irreducible curves over an algebraically closed field k. Then C_1 and C_2 are isomorphic if and only if the principally polarized abelian varieties $(\mathrm{Jac}(C_1), \Theta_1)$ and $(\mathrm{Jac}(C_2), \Theta_2)$ are isomorphic.*

There is a slightly stronger statement which says that if (X, Θ) is an abelian variety and C_1 and C_2 are two curves on X such that (X, Θ) is the Jacobian of both C_1 and C_2 then C_2 is a translate of C_1 or of $(-1_X)(C_1)$. The theorem that Torelli proved was stronger. He proved that if $f : C_2 \to \mathrm{Jac}(C_1)$ is a morphism of a curve of genus $g = g(C_1)$ such that $f(C_2)$ generates X and $\deg(f^*(O(\Theta)) = g$ then f is an injection and $f(C_2)$ is a translate of C_1 or of $(-1_X)(C_1)$. In relation to this we refer to the next Section and the Notes.

There are many proofs for this theorem in the literature, see the Notes; here we sketch Andreotti's beautiful proof, cf. [An]. In the Chapter on the geometry of the theta divisor we shall give another proof.

Proof. It is immediate that if C_1 and C_2 are isomorphic their polarized Jacobians are isomorphic. So it suffices to prove that for a proper smooth irreducible curve C we can recover C from the pair $(\mathrm{Jac}(C), \Theta)$. To do this we shall consider the Gauss map of the theta divisor $\Theta \subset \mathrm{Jac}^{g-1}(C)$ that associates to a smooth point of Θ its tangent space translated to the origin:

$$\gamma : \Theta_{\mathrm{sm}} \longrightarrow \mathbb{P}^\vee, \quad [D] \mapsto T_{\Theta,[D]} \subset T_{\mathrm{Jac}^{g-1}(C),[D]} = T_{\mathrm{Jac}(C),0}$$

where $\mathbb{P}^\vee$ is the projective space of hyperplanes in $T_{\mathrm{Jac}(C),0}$. Note that it is also the dual of the projective space $\mathbb{P}^{g-1}$ to which the canonical map $\psi = Tj : C \to \mathbb{P}^{g-1}$ of C goes.

Now recall the description of the tangent space to Θ at a smooth point $[D]$ of Θ, cf.'`omegaatD`'. If $[D]$ is represented by a unique effective divisor $\sum_{i=1}^{g-1} P_i$ then the tangent space to Θ translated to the origin is the hyperplane spanned by the points $\psi(P_i)$: $\gamma([D]) = \mathrm{Span}(\psi(P_i), i = 1, \ldots, g-1)$. We define

$$\Gamma = \text{closure of the graph of } \gamma \text{ in } \Theta \times \mathbb{P}^\vee$$

and let $\tilde{\Gamma}$ be the normalization of Γ. We have a natural morphism $p_2 : \tilde{\Gamma} \longrightarrow \mathbb{P}^\vee$ induced by projection onto the second factor. We let B be the branch locus in $\mathbb{P}^\vee$ of p_2. The beautiful idea behind the proof is now that (at least for non-hyperelliptic curves C) the branch locus of p_2 is the so-called envelop of $\psi(C)$, i.e. the set of hyperplanes tangent to $\psi(C)$, and this determines C. We now distinguish two cases.

Case 1. C is not hyperelliptic. In this case we shall identify C with its canonical image $\psi(C) \subset \mathbb{P}$. We need the following lemma from the theory of curves. (Reference ?)

curvelemma **(14.42) Lemma.** *Let C be a non-hyperelliptic curve of genus $g \geqslant 2$. Then the canonical image has only finitely many bitangent lines (i.e. lines that are tangent to at least two different points). Moreover, a general canonical divisor K consists of $2g-2$ distinct points and any $g-1$ of them are linearly independent, i.e. for any effective divisor D of degree $g-1$ contained in K we have $h^0(D) = 1$.*

The lemma implies that for a general hyperplane $H \subset \mathbb{P}$ the canonical divisor $H \cdot C$ contains $\binom{2g-2}{g-1}$ divisors D all of which give classes $[D]$ in Θ_{sm}. In particular, for a general H the fibre of γ is contained in the smooth locus Θ_{sm} and γ is unramified in the fibre over H.

In order to describe $\tilde{\Gamma}$ more precisely we consider the variety

$$\Gamma_0 = \{(D, H) \in C^{(g-1)} \times \mathbb{P}^\vee : H \cdot C \text{ contains the divisor } D\}.$$

This is a closed subset of $C^{(g-1)} \times \mathbb{P}^\vee$ and we have an embedding $\Theta_{\mathrm{sm}} \to \Gamma_0$ given by $[D] \mapsto (D, H)$, with D the unique effective divisor representing $[D]$ and H the hyperplane spanned by it. The second projection projection $\gamma_0 = p_2$ extends $\gamma : \Theta_{\mathrm{sm}} \to \mathbb{P}^\vee$. Obviously, γ_0 is a quasi-finite separable map of degree $\binom{2g-2}{g-1}$, hence a finite map. There is a natural morphism $\Gamma_0 \to \Gamma$ with $(D, H) \mapsto ([D], H)$ which is quasi-finite and generically of degree 1. Therefore the map of the normalization $\tilde{\Gamma}$ to $\mathbb{P}^\vee$ factors through Γ_0 and it is a finite map. We study now its branch locus B.

branchnh **(14.43) Lemma.** *The branch locus B is irreducible and coincides with the envelope $C^\vee = \{H \in \mathbb{P}^\vee : H$ is tangent to C at some point$\}$.*

Proof. It follows immediately from the definitions that the branch locus is the envelope. It is well known that the envelope of a smooth irreducible curve is irreducible (see Exercise).

So to prove Torelli's theorem for non-hyperelliptic curves we have to show that we can recover C from $C^\vee$. For this we refer to [?].

Case 2. C is hyperelliptic. We denote the hyperelliptic involution of C by σ. In this case the canonical image of C is a rational normal curve R in $\mathbb{P}$ and we have maps

$$\varepsilon : C^{(g-1)} \longrightarrow R^{(g-1)} \xrightarrow{\rho} \mathbb{P},$$

where the first map is of degree 2^{g-1} and ρ is the regular map that associates to D the hyperplane spanned by D. Note that ρ is indeed regular: if R is obtained by embedding $\mathbb{P}^1$ into $\mathbb{P}$ via $t \mapsto (1 : t : t^2 : \ldots : t^{g-1})$ then ρ is given by $(t_1, \ldots, t_{g-1}) \mapsto (\sigma_{g-1} : \sigma_{g-2} : \ldots : \sigma_0)$ with σ_j the j-th elementary symmetric function in the t_i. The map ε is the canonical map of $C^{(g-1)}$. The analogue of 14.43 is now

branchhe **(14.44) Lemma.** *The branch locus of ε is reducible and consists of the envelope of R and the hyperplanes dual to the branch points of $\varphi : C \to R$.*

If the characteristic is not 2 it is easy to retrieve the curve C from the Gauss map $\Theta \to \mathbb{P}^\vee$: the $2g+2$ hyperplanes determine the branch locus of φ, hence the hyperelliptic curve C. But this argument does not work in characteristic 2.

We now give an argument that works for every characteristic. We consider the map $\varepsilon : C^{(g-1)} \to \mathbb{P}^\vee$ and the image of the small diagonal δ of $C^{(g-1)}$ under ε. It is given by associating to $P \in C$ the osculator hyperplane to R at $\psi(P)$ (which intersects the curve at $\psi(P)$ with multiplicity $g-1$). The inverse image $\varepsilon^{-1}(\delta)$ consists of the images on $C^{(g-1)}$ of the maps

$$d_i : C \longrightarrow C^{(g-1)}, \quad Q \mapsto iQ + (g-1-i)Q^\sigma \qquad (0 \leqslant i \leqslant [(g-1)/2]).$$

Note that the degree of inseparability of d_0 is p^α with $\alpha = \mathrm{ord}_p(g-1)$. Thus we can retrieve C from the image of d_0. But we have to see that the isomorphism class of $C^{(g-1)}$ determines the image of d_0. To distinguish the image δ of d_0 from the images of the other d_i we have the following lemma whose proof is left to the reader.

fixedpart **(14.45) Lemma.** *The fixed part of the canonical system of $C^{(g-1)}$ consists of $g^1_2 + C^{(g-3)} \subset C^{(g-1)}$.*

It now suffices to observe that the base locus $g^1_2 + C^{(g-3)}$ of the canonical system of $C^{(g-1)}$ contains the images of the maps d_i for $i = 1, \ldots, [(g-1)/2]$, but not the image of d_0. So the isomorphism class of $C^{(g-1)}$ determines the image of d_0 and that determines the isomorphism class of C. This completes the proof of the Torelli theorem. □

§9. *The Criterion of Matsusaka-Ran.*

In this section we give a criterion for deciding that an abelian variety is a jacobian. For later convenience we formulate it not only for smooth curves, but for stable curves of compact type as defined in the following definition. The proof is due to Collino [Co].

Definition A connected complete reduced curve is called *of compact type* if the curve is a stable curve whose dual graph is a tree.

MatsusakaRan **(14.46) Theorem.** The Criterion of Matsusaka-Ran. *Let (X, L) be a polarized abelian variety of dimension g and let C be an effective 1-cycle on X which generates X such that the intersection number $C \cdot L \leqslant g$. Then C is a reduced stable curve $\sum_{i=1}^n C_i$ of compact type whose components C_i are smooth irreducible curves and (X, L) is isomorphic to the Jacobian $\mathrm{Jac}(C)$, i.e. to the product of the canonically polarized Jacobians $\prod_{i=1}^n \mathrm{Jac}(C_i)$ of the components.*

Proof. We write $C = \sum_{i=1}^n m_i C_i$ with distinct irreducible reduced curves C_i and we denote the normalization of C_i by $\tilde{C}_i$ and its genus by g_i. We denote the embedding $C_{\mathrm{red}} \to X$ by ι. The natural map $\tilde{C}_i \to C_i \to X$ factors through the Jacobian $\mathrm{Jac}(\tilde{C}_i)$, say via $\psi_i : \mathrm{Jac}(\tilde{C}_i) \to X$, by the (covariant) universal property of $\mathrm{Jac}(\tilde{C}_i)$ as explained in Section 3. By Exercise (II,??) we know that we can represent L by an effective reduced divisor D. The Moriwaki-Matsusaka construction (see Chapter on End) gives us now an endomorphism $\alpha(C, L) : X \to X$. If we translate C the map $\alpha(C, L)$ does not change, so if we assume that D does not contain any component of C the map $\alpha(C, L)$ is given on an open set of X by $x \mapsto \mathrm{sum}(C \cdot (D + x) - C \cdot D)$. It is then clear that $\alpha(C, L)$ fits into a commutative diagram

$$\begin{array}{rccccc} \alpha(C,L): & X & \xrightarrow{q} & \prod \mathrm{Jac}(\tilde{C}_i) & \xrightarrow{\psi} & X \\ & & \searrow^{\lambda} \quad \nearrow_{\iota^*} & & & \\ & & X^t & & & \end{array}$$

where $\psi = (\psi_1, \ldots, \psi_n)$ and where $\lambda(x) = [(D + x) - D]$. The dual of ι^* is $-\psi$ by 14.29 and Exercise ??. Now ψ is surjective since C generates X, hence ι^* and $\iota^*\lambda$ have finite kernel. It follows that $\dim \prod_{i=1}^m \mathrm{Jac}(\tilde{C}_i) = g$. Now we know that $\sum_{i=1}^m m_i C_i \cdot L \leqslant g$, but on the other hand by construction the map q factors through $X \to \tilde{C}_1^{(d_1)} \times \ldots \times \tilde{C}_n^{(d_n 0}$ with $d_i = C_i \cdot L$, hence

$$g = \dim \alpha(C, L)(X) \leqslant \sum (C_i, L) \leqslant g$$

and by comparing we get $m_i = 1$ for $i = 1, \ldots, n$ and $C_i \cdot L = \dim \mathrm{Jac}(\tilde{C}_i)$ and $\sum g_i = g$.

We must show that ψ is an isomorphism of polarized abelian varieties. We do this by showing that $\psi^*(L)$ is a principal polarization and then by showing that it coincides with the canonical polarization on this product of Jacobians.

Suppose that $\psi^*(L)$ is not a principal polarization. Let D be a reduced effective divisor representing L. Then the linear system $|D|$ has dimension $\geqslant 1$ and also all translates $t_y^*(D)$ have this property. Consider a general translate $F = t_y^*(D)$ and an effective divisor $G \neq F$ linearly equivalent to F. Since y is general the pullbacks of F and G under ψ_i are distinct and it follows that the pullback of $t_y^*(D)$ is a special divisor of degree g_i on $\tilde{C}_i$. But this divisor is the pull back of $t_y^*(D) \cdot C_i$ and this is the image of y under the i-th component of q. This implies that the general element of $\mathrm{Jac}^{g_i}(\tilde{C}_i)$ is a special divisor, a contradiction. We thus see that $\psi_i^*(L)$ is a principal polarization. Moreover, the map $\psi_i : \mathrm{Jac}(\tilde{C}_i) \to X$ is an embedding because $\varphi_{\psi^*(L)} = \hat{\psi}_i \varphi_L \psi_i$ is an isomorphism. Now if $i \neq j$ the map $\hat{\psi}_j \varphi_L \psi_i$ is zero (see Exercise ..) and thus

$$\varphi_{\psi^* L} = \hat{\psi} \varphi_L \psi = \sum_j \prod_i \hat{\psi}_i \varphi_L \psi_j = \prod_i \hat{\psi}_i \varphi_L \psi_i$$

implying that $\psi^* L$ and $\otimes_i p_i^* \varphi_i^* L$ are algebraically equivalent. Thus $\psi^* L$ is a principal polarization. We also see that ψ is an isomorphism and $C_i \cong \tilde{C}_i$.

Since ψ is an isomorphism two curves C_i can intersect in at most one point. Otherwise, the difference of the two intersection points would give a non-zero element in $\mathrm{Jac}(C_i) \cap \mathrm{Jac}(C_j)$.

Similarly, an non-transversal intersection would yield a non-zero group scheme in $\mathrm{Jac}(C_i) \cap \mathrm{Jac}(C_j)$. This implies that C is stable.

By induction on the genus we may assume that the theorem holds for lower dimensional abelian varieties, hence if C is reducible we are done. So we may assume that C is irreducible. It follows from the diagram that $\alpha(C, L)$ is an isomorphism of abelian varieties.

We must show that the principal polarization $\psi^*(L)$ is the canonical polarization $O(\Theta)$ of $\mathrm{Jac}(C)$. Recall that Θ is up to translation the divisor of effective divisors of degree $g-1$ in $\mathrm{Jac}^{g-1}(C)$.

For general $x \in X$ we have an identity $C \cdot t_x^* D = x_1 + \ldots + x_g$, where $x_1, \ldots, x_g$ are points of C (and X) up to order uniquely determined. This establishes a birational correspondence $b : C^{(g)} \to X$ which is the composition of the natural map $C^{(g)} \to \mathrm{Jac}(C)$ with q^{-1} and since we now know that q is an isomorphism b is a morphism. Then $x_g \in t_x^* D$, i.e. $x + x_g \in D$. Therefore we see that D contains the image of

$$\beta : C^{(g-1)} \times C \longrightarrow X \cong \mathrm{Jac}(C), \quad (x_1 + \ldots + x_{g-1}, x_g) \mapsto b(x_1, \ldots, x_g) + x_g.$$

We claim: D coincides with the image of β. Indeed, if D is larger than the image of β, then the closure of $D - \mathrm{Im}(\beta)$ is a divisor D' in $\mathrm{Jac}(C)$. A general translate of C intersects both D' and $\mathrm{Im}(\beta)$ outside the intersection $D' \cap \mathrm{Im}(\beta)$. We may then even assume that the translate is C and then have $C \cdot D = x_1 + \ldots + x_{g-1} + w$ with $w \in D'$. Then we have $\beta(x_1, \ldots, x_{g-1}, w) = w$, outside the image of β, a contradiction.

By the rigidity lemma the morphism β is of the form $\beta' + \beta''$ with $\beta' : C^{g-1} \to \mathrm{Jac}(C)$ and $\beta'' : C \to \mathrm{Jac}(C)$ morphisms. For fixed $y \in C$ the image of $C^{(g-1)} \times \{y\}$ under β has dimension $g-1$ since b is generically injective. It follows that $\beta(C^{(g-1)} \times \{y\}) = D$. Since D is a principal polarization no non-trivial translations leave D fixed and it follows that β'' contracts C and we may thus suppose that $\beta'' = 0$. We thus have for every point $(x_1 + \ldots + x_{g-1}, x_g) \in C^{(g-1)} \times C$ an equality

$$b(x_1 + \ldots + x_g) = \beta(x_1 + \ldots + x_{g-1}, x_g) - x_g.$$

We now fix $g-1$ points $c_1, \ldots, c_{g-1}$ on C. Then we find

$$\begin{aligned} \beta(x_1 + \ldots + x_{g-1}) - x_g &= b(x_1 + \ldots + x_g) = b(x_2 + \ldots + x_{g-1} + x_1) \\ &= \beta(x_2 + \ldots + x_g, x_1) - x_1 = \beta(x_2 + \ldots + x_g, c_1) - x_1 \\ &= b(x_2 + \ldots + x_g + c_1) + (c_1 - x_1) \end{aligned}$$

Repeating the argument gives

$$\begin{aligned} \beta(x_1 + \ldots + x_{g-1}) - x_g &= b(c_1 + \ldots + c_{g-1} + x_g) + \sum_{i=1}^{g-1} (c_i - x_i) \\ &= \beta'(c_1 + \ldots + c_{g-1}) - x_g + \sum_{i=1}^{g-1} (c_i - x_i). \end{aligned}$$

This shows that D is a translate of $(-1)^*\Theta$ and finishes the proof of the theorem. □

specofJac **(14.47) Corollary.** *A principally polarized abelian variety which is a specialization of a Jacobian is a Jacobian of a stable curve of compact type.*

Proof. A specialization of an effective 1 cycle is an effective 1 cycle. Also the degree $L \cdot C$ is preserved under specialization.

Intermezzo: the Moriwaki-Matsusaka endomorphism; hoort in Hoofdstuk over End

Let A and B be effective algebraic cycles on a g-dimensional abelian variety X of complementary dimension. That means, A (res. B) is an element of the free abelian group generated by the subvarieties of X of dimension a (resp. of dimension $b = g - a$. We now define an endomorphism $\alpha(A, B)$ to the pair (A, B) following Moriwaki and Matsusaka as follows. For a general point $x \in X$ the intersection of $t_x^* A$ and B will be a proper 0-cycle $\sum_{i=1}^{d} p_i$ of degree $d = \deg(A \cdot B)$. In this way we get a rational map that extends to a morphism (by ..) and after translation this becomes an endomorphism:

$$\begin{aligned} X &\longrightarrow X^d/S_d \xrightarrow{\text{sum}} X \xrightarrow{\text{translation}} X \\ x &\mapsto (A - x) \cap B \end{aligned}$$

Since $\alpha(A, B)(0) = 0$ we see that we can write

$$\alpha(A, B) = \text{sum}(t_x^*(A) \cdot B - A \cdot B),$$

whenever this is defined.

Lemma. *If A and A' are algebraically equivalent then $\alpha(A, B) = \alpha(A', B)$.*

Proof. Let A_s (with $s \in S$) be a family of algebraically equivalent cycles. We may assume that S is normal. Then we get a morphism

$$\beta(A, B) : X \times S \longrightarrow X, \quad (x, s) \mapsto \alpha(A_s, B)(x).$$

This satisfies $\beta(\{0\} \times S) = 0$. Define β' via $\beta'(x, s) = \beta(x, s) - \beta(x, s_0)$ for some fixed point $s_0 \in S$. Then $\beta'(X \times s_0) = \beta(\{0\} \times S) = 0$, hence by the Rigidity theorem β' is constant and this implies that β factors through p_X. □

§6 The genus of a simple abelian variety

Let X be an abelian variety of dimension g over an algebraically closed field k. If X is isomorphic to the Jacobian of a curve C then X carries a smooth proper curve of genus g. If X is simple, then X does not carry any curve of smaller genus. For if $i : C \to X$ is of genus γ then we get a homomorphism $X^t \to \text{Jac}(C)$ which is non-zero (an ample line bundle L on X is not in the kernel) which is not compatible with the assumption that X is simple. If X is isogenous to a Jacobian, say $r : \text{Jac}(C) \to X$ is an isogeny, then a suitable translate of the image of C under $\varphi : C \to \text{Jac}(C)$ has as image under r a curve of genus g.

Definition. Let X be a simple abelian variety over a field k. Then the *genus* of X is the smallest geometric genus of a complete irreducible reduced curve on X.

A first remark is that the genus of a simple abelian variety does not change under isogenies. In characteristic 0 we may therefore assume that X is principally polarized. Very little is known about this invariant. In [BCV] it is proved that the general 4-dimensional principally polarized abelian variety has genus 7 and the general 5-dimensional principally polarized abelian variety has genus 11. The question: what is the maximum genus of an abelian variety of dimension g

seems very interesting. A related invariant is the minimal effective class. If (X, Θ) is a principally polarized abelian variety then let

$$\theta = [\Theta^{g-1}/(g-1)!] \in H^2(X),$$

where cohomology means Betti cohomology with integral coefficients or ℓ-adic cohomology with $\ell \neq \mathrm{Char}(k)$. (Weyl cohomology) It follows from the Matsusaka-Ran criterion that a curve C on X that generates X has intersection number $\geqslant g$ with Θ. Therefore, if C is a curve on X and if $[C]$ is a rational multiple of θ then $[C]$ is an integral multiple of θ. We define

$$c(X, \Theta) = \min\{n \in \mathbb{Z}_{\geqslant 1} : c\theta \text{ is representable by an effective 1-cycle } C \text{ on } X\}.$$

For Jacobians $c(X, \Theta)$ equals 1. For Prym varieties is equals 2. It seems an interesting question to determine $c(X, \Theta)$ for the general principally polarized abelian variety of dimension g. We refere to papers by Debarre.

Exercises

Exercise. Let C be a complete non-singular curve over a field k. We denote by α: $C \times C^{(n-1)} \to C^{(n)}$ the natural map. Prove that $\Omega^1_{C^{(n)}}$ is isomorphic to $\alpha_*(p_1^*\Omega^1_C)$ with p_1: $C \times C^{(n-1)} \to C$ the first projection.

Exercise. Prove that for $n \geqslant 1$ the n-th symmetric product of $\mathbb{P}^1$ is isomorphic to $\mathbb{P}^n$. Show that for a smooth, absolutely irreducible curve over a field the variety $C^{(n)}$ is projective. (Hint: use a finite morphism $C \to \mathbb{P}^1$.)

Let C be a proper smooth absolutely irreducible complete curve over a field k and let $P \in C(k)$ be a point. Prove that the map $\varphi_P : C \to \mathrm{Jac}(C)$ induces by pulling back line bundles the isomorphism $(-\varphi_\Theta)^{-1} : \mathrm{Jac}(C)^t \longrightarrow \mathrm{Jac}(C)$

(Bij Poincaré Irreducibiliteit?) Let X,Y be subvarieties of the abelian variety Z with inclusions $\xi : X \to Z$ and $\eta : Y \to Z$ and $\xi(X) \cap \eta(Y)$ finite. If L is a polarization on Z then $\eta^t \varphi_L \xi = 0 : X \to Y^t$.

Exercise. Let α_1^* be the map $\mathrm{Pic}^0(\mathrm{Jac}^1(C)) \to \mathrm{Jac}(C)$ given by pulling back line bundles on $\mathrm{Jac}^1(C)$ to C via α_1. Show that α^* is an isomorphism.

Let X and Y be varieties and Z an abelian variety. Suppose that one of X and Y is complete. If $f : X \times Y \to Z$ is a morphism, then there exist morphisms $g : X \to Z$ and $h : Y \to Z$ such that $f = g + h$. Prove this. (In het hoofdstuk met het stijfheidslemma.)

Notes

For a long time the theory of abelian varieties was synonimous with the theory of Jacobians. The work of Riemann [R1, R2] was a milestone in the development. He introduced the theta divisor and interpreted the singularieties of the theta divisor on a Jacobian in terms of linear systems on the curve. Torelli made two key contributions to the theory. He showed that one can retrieve a curve from its Jacobian together with the theta divisor. Moreover, Torelli observed that every abelian variety is a quotient of a Jacobian. All these authors worked over the complex numbers. In the beginning of the 20th centure the need was felt for an algebraic theory of Jacobian variety in order to be able to deal with curves over number fields and over finite fields. This theory was created by A. Weil and in order to do this he had to lay new foundations

of algebraic geometry. He constructed the Jacobian of a curve C of genus g by starting from the symmetric power $C^{(g)}$ and by extending the birational group law. His celebrated proof of the Riemann hypothesis for curves over finite fields was a direct corollary. The present approach towards the Jacobian via representability of the Picard functor is due to Grothendieck. We refer to his exposés FGA. The criterion of Matsusaka-Ran was proved by Matsusaka for smooth curves in 19.., but a form of it is already in the work of Torelli, cf. [T?]. Ran extended it [R?]. We follow the clear proof of Collino [Co]. There are many proofs of the Torelli theorem in the literature. A sort of survey is found in Mumford (Curves and their Jacobians). We shall give another prove in the Chapter on the Geometry of the Theta Divisor. Yet another proof is in Polishchuck. We refer to (Andreotti, Beauville, Ciliberto, Collino, Matsusaka, Mattuck-Mayer, Weil). Our proof Riemann's theorem on the singularities of Θ follows [A-C-G-H].

References

A. Andreotti: On a theorem of Torelli. *Amer. J. of Math.* **80** (1958), p. 801–828.

A. Andreotti, A.L. Mayer: On period relations for abelian integrals on algebraic curves. *Ann. Scuola Norm. Pisa* **21** (1967), p. 189–238.

F. Bardelli, C. Ciliberto, A. Verra: Curves of minimal sogenies. on a general abelian variety. Compositio Mathematica 96: (1995) p. 115-147,

A. Beauville: Le problème de Torelli. Séminaire Bourbaki, Vol. 1985/86. Astérisque No. 145-146 (1987), 3, 7–20.

A. Collino: A new proof of the Ran-Matsusaka criterion for Jacobians. Proc. Amer. Math. Soc. 92 (1984), no. 3, 329–331.

A. Collino: A simple proof of the theorem of Torelli based on Torelli's approach. Proc. Amer. Math. Soc. 100 (1987), no. 1, 16–20

A. Grothendieck: Technique de descente et théorèmes d'existence en géométrie algébrique. FGA. Séminaire Bourbaki 190, 195, 212, 221, 232, 236.

G. Kempf: On the geometry of a theorem of Riemann. *Ann. of Math.* **98** (1973), p. 178–185.

T, Matsusaka: On a theorem of Torelli. *Amer. J. of Math.* **80** (1958), p. 784–800.

A. Mattuck, A. Mayer: The Riemann-Roch theorem for algebraic curves. *Ann. Scuola Norm. Pisa* **17** (1963), p. 223–237.

D. Mumford: Curves and their Jacobians.

E. Selmer: The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.* **85**, (1951). p. 203–362

R. Torelli: Sulle serie algebriche semplicemente infinite di gruppi di punti appartenenti a una curva algebrica. *Rend. Circ. Mat. Palermo* **37** (1914).

A. Weil: Zum Beweis des Torellischen Satzes. *Nachrichten der Akademie der Wissenschaften in Göttingen*, Math.-Phys. Klasse, 2 (1957), p. 33-53.

sem
ske
pol

§1. *Dieudonné theory for finite commutative group schemes and for p-divisible groups.*

W(k)Basics **(15.1)** Basics on Witt vectors, mainly to set up notation. Introduce σ = 'Frobenius' = endomorphism induced by $x \mapsto x^p$ on residue field. Introduce $\mathbb{Z}_{p^a} = W(\mathbb{F}_{p^a})$ and $\mathbb{Q}_{p^a}$.

SemiLinear **(15.2)** Let R be a commutative ring with identity. Let α be an endomorphism of R. If M_1 and M_2 are (left) R-modules then by an *α-linear* map $f\colon M_1 \to M_2$ we mean an additive map with the property that $f(rm) = \alpha(r) \cdot f(m)$ for all $r \in R$ and $m \in M_1$. If it is clear which α we are considering then such a map is also simply called a *semilinear* map.

A semilinear map can be linearized. For this we consider the R-module $M_1^{(\alpha)} := R \otimes_{R,\alpha} M_2$, obtained from M_1 by extension of scalars via $\alpha\colon R \to R$. Then an α-linear map $f\colon M_1 \to M_2$ gives rise to an R-linear homomorphism $f^\sharp\colon M_1^{(\alpha)} \to M_2$ by $f^\sharp(r \otimes m) = r \cdot f(m)$. Note that this is well-defined, as $f^\sharp(r \otimes sm) = r \cdot f(sm) = r\alpha(s) \cdot f(m) = f^\sharp(r\alpha(s) \otimes m)$. Conversely, to a homomorphism of R-modules $g\colon M_1^{(\alpha)} \to M_2$ we can associate the α-linear map $g^\flat\colon M_1 \to M_2$ defined by $g^\flat(m) := g(1 \otimes m)$. One readily checks that these constructions are mutually inverse: $(f^\sharp)^\flat = f$ and $(g^\flat)^\sharp = g$. Hence an α-linear map may also be described as an R-linear map $M_1^{(\alpha)} \to M_2$.

SkewPol **(15.3) Definition.** Let R be a ring with identity. Let α be an endomorphism of R, and let t be an indeterminate. Then the *skew polynomial ring* $R[t;\alpha]$ is the ring of polynomials in the variable t with coefficients in R, in which

(a) addition is as in the usual polynomial ring $R[t]$;
(b) the ring multiplication is distributive and satisfies $t \cdot c = \alpha(c) \cdot t$ for all $c \in R$.

In other words, the only new aspect is that the variable t does not commute with the coefficients (unless $\alpha = \mathrm{id}$), but is "α-linear".

By iteration of (b) we find that $t^n \cdot c = \alpha^n(t) \cdot t^n$ for all $n \in \mathbb{N}$ and $c \in R$. Clearly, if $\alpha = \mathrm{id}_R$ then $R[t;\alpha]$ is just the ordinary polynomial ring. If α is not the identity then $R[t;\alpha]$ is non-commutative.

In the sequel it will usually be clear which endomorphism α we are taking, and especially in the context of Dieudonné modules we shall occasionally drop the α from the notation.

DModDef **(15.4) Definition.** Definitie Dieud modules, category $\mathsf{DM}_{/k}$, full subcats $\mathsf{DM}_{/k}^{\mathrm{free}}$ and $\mathsf{DM}_{/k}^{\mathrm{tors}}$. Dual of a Dieud module.

DModFinThm **(15.5)** Main theorem on Dieud theory for finite flat group schemes + Cartier duality.

DModExa **(15.6)** Examples

DModConseq **(15.7)** Maybe something on consequences for finite group schemes. Eg, only simple group schemes over $k = \overline{k}$ are μ_p, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/\ell\mathbb{Z}$, α_p. Are there further things we need at some point?

DModBT **(15.8)** Dieud mod of a BT, Serre duality.

DTheoryRem **(15.9)** Some general comments on Dieud theory; covariant vs contravar; references to literature. cry iso

§2. *Classification up to isogeny.*

ClassIsogIntro **(15.10)** Throughout this section, k denotes a perfect field of characteristic $p > 0$. We write $W := W(k)$ for its ring of Witt vectors, L for the fraction field of W, and σ for the automorphism of W (and also of L) induced by the Frobenius automorphism $x \mapsto x^p$ of k.

If N is a finite dimensional L-vector space then by a W-lattice in L we mean a W-submodule $M \subset N$ such that the natural map $L \otimes_W M \to N$ is an isomorphism. (Equivalent: M is free of rank $\dim_L(N)$ as a W-module.) If M_1 and M_2 are W-lattices in N then so are $M_1 + M_2$ and $M_1 \cap M_2$. We define

$$\chi(M_1 : M_2) := \mathrm{length}_W(M/M_2) - \mathrm{length}_W(M/M_1)\,,$$

where M is any W-lattice in N containing both M_1 and M_2; this is easily seen to be independent of the chosen M. In particular, if $M_2 \subseteq M_1$ then we simply have $\chi(M_1 : M_2) = \mathrm{length}_W(M_1/M_2)$. If M_3 is a third lattice we have the relation $\chi(M_1 : M_3) = \chi(M_1 : M_2) + \chi(M_2 : M_3)$.

Our main goal in this section is to discuss a number of key results on the classification of p-divisible groups over k up to isogeny. Dieudonné theory allows us to translate this into a problem in semi-linear algebra. More precisely, we are led to consider finite dimensional L-vector spaces N together with a bijective σ-linear operator $F\colon N \to N$. We refer to such a pair (N, F) as an F-isocrystal over k. Not all F-isocrystals arise from a p-divisible group; a necessary and sufficient condition for this is that there exists a W-lattice $M \subset N$ with $p \cdot M \subseteq F(M) \subseteq M$. Still, it proves an advantage to work with general F-isocrystals, and in fact these naturally appear in the context of crystalline cohomology; cf. () below.

An F-isocrystal can be viewed as a module over the skew polynomial ring $L[F;\sigma]$. To be precise, the modules that we are interested in are those whose underlying L-vector space is finite dimensional and on which the action of F is bijective. This brings ring-theory into play, which in this context is very helpful, as $L[F;\sigma]$ is a non-commutative principal ideal domain and there is a good general theory of modules over such a ring; see Jacobson [1], Chap. 3.

Another possible approach—the one we shall take—is to exploit that two W-lattices in a finite dimensional L-vector space can be compared, and this gives rise to useful discrete invariants. If (N, F) is an F-isocrystal and $M \subset N$ is a W-lattice, we can measure the relative position of M and $F(M)$, and express it in a polygon, called the Hodge polygon of (M, F). Pushing this further, one may also look at $F^2(M)$, or the image under M under higher powers of F. To create the right context for this, we shall consider pairs (N, F) as before where the "Frobenius" F is not necessarily σ-linear but can be σ^a-linear, for some $a \in \mathbb{Z}$. Such objects are called σ^a-F-crystals.

Information about the asymptotic behaviour of F can be encoded in a second polygon, called the Newton polygon of (N, F). In contrast with the Hodge polygon, the Newton polygon only depends on (N, F), not on the choice of a lattice $M \subset N$. Among the main results of this section is a theorem of Dieudonné, Theorem (15.33), which says that over an algebraically closed field k an F-isocrystal is classified by its Newton polygon. In concrete terms this means that we

have a collection of explicitely defined F-isocrystals $\mathscr{N}_\lambda$, one for each $\lambda \in \mathbb{Q}$ (the Newton slope), such that any F-isocrystal over $k = \overline{k}$ is isomorphic to a direct sum of such objects $\mathscr{N}_\lambda$.

In the approach we take, Dieudonné's Theorem is preceded by another import result, valid over any perfect field k of characteristic p, which says that an F-isocrystal has a canonical decomposition into isoclinic pieces. See Theorem (15.30). An F-isocrystal (N, F) is called "isoclinic" if there exist a W-lattice $M \subset N$ and integers r and $s > 0$ such that $F^s(M) = p^r \cdot M$; the quotient r/s is then called the slope of (N, F). The proof of Theorem (15.30) requires some preparations, all completely elementary in nature, but once we are there Dieudonné's Theorem hardly requires further work. As a bonus we obtain a useful result about F-isocrystals over a finite field, that allows to calculate the Newton polygon in a very simple manner from the characteristic polynomial of a suitable power of F.

A final key result in this section... Mazur??

Though we are mainly interested in F-crystals, we shall state and prove results in the more general setting of σ^a-F-crystals. This is not just out of academic interest; it actually leads to much simpler proofs. A typical trick, that we shall use several times, is that we can pass from a σ^a-F-isocrystal (N, F) to a σ^{as}-F-isocrystal (N, F') with $F' = p^\nu F^s$ for suitable integers ν and s. By this, we can reduce several arguments to the isoclinic case with slope $= 0$, and in this we can often prove what we want by an easy direct argument. See the proofs of ... for nice examples of this.

Our exposition of the material in this section closely follows Zink [1].

FCrysDef **(15.11) Definition.** Let $a \in \mathbb{Z}$. Then a *σ^a-F-crystal over k* is a pair (M, F) consisting of a free W-module M of finite rank, together with a σ^a-linear injective map $F\colon M \to M \otimes_W L$.

A morphisms of σ^a-F-crystals $f\colon (M_1, F_1) \to (M_2, F_2)$ is a homomorphism $f\colon M_1 \to M_2$ of W-modules (so a *W-linear* map) such that $f \circ F_1 = F_2 \circ f$. We denote by σ^a-F-$\mathsf{Crys}_{/k}$ the category of σ^a-F-crystals over k that is thus obtained.

The map F is not required to take values in M itself; it is allowed to have "denominators". If $F(M) \subseteq M$ then we say that the crystal is *effective*. The condition that F is injective implies that the induced map $M \otimes_W L \to M \otimes_W L$ is bijective. We shall use the notation $M_{\mathbb{Q}} := M \otimes_W L = M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = M \otimes_{\mathbb{Z}} \mathbb{Q}$.

Note that in the definition of a morphism, the identity $f \circ F_1 = F_2 \circ f$ is an identity of maps $M_1 \to M_{2,\mathbb{Q}}$, so the "f" on the left has to be interpreted as the linear map $M_{1,\mathbb{Q}} \to M_{2,\mathbb{Q}}$ induced by the given $f\colon M_1 \to M_2$.

If $a = 0$ then a σ^a-F-crystal is of course just a finite free W-module M together with a *linear* injective map $M \to M_{\mathbb{Q}}$. We shall mainly be interested in the case $a = 1$. In this case one usually drops the prefix "σ"; so by an *F-crystal* we mean a σ-F-crystal, and we write F-$\mathsf{Crys}_{/k}$ for σ-F-$\mathsf{Crys}_{/k}$. The category $\mathsf{DM}_{/k}^{\mathrm{free}}$ of torsion-free Dieudonné modules is equivalent to the full subcategory of F-$\mathsf{Crys}_{/k}$ consisting of all F-crystal (M, F) with $p \cdot M \subseteq F(M) \subseteq M$, as these inclusions are equivalent to the existence of a map $V\colon M \to M$ with $FV = p \cdot \mathrm{id}_M = VF$.

A homomorphism of σ^a-F-crystals $f\colon (M_1, F_1) \to (M_2, f_2)$ is called an *isogeny* if the induced map $M_{1,\mathbb{Q}} \to M_{2,\mathbb{Q}}$ is bijective. If one wants to study σ^a-F-crystals only up to isogeny, it suffices to know the L-vector space $M_{\mathbb{Q}}$ together with its σ^a-linear Frobenius. Thus one is led to the following notion of an isocrystal.

FIsocDef **(15.12) Definition.** Let $a \in \mathbb{Z}$. Then a *σ^a-F-isocrystal over k* is a pair (N, F) consisting of an L-vector space N of finite dimension, together with a bijective, σ^a-linear endomorphism

$F\colon N \to N$.

A morphisms of F-isocrystals $f\colon (N_1, F_1) \to (N_2, F_2)$ is an L-linear map $f\colon N_1 \to N_2$ such that $f \circ F_1 = F_2 \circ f$. We denote by σ^a-F-$\mathsf{Isoc}_{/k}$ the category of σ^a-F-crystals over k that is thus obtained.

Note that σ^a-F-$\mathsf{Isoc}_{/k}$ can also be described as the category of modules over the ring $L[F, F^{-1}]$ with finite dimensional underlying L-vector space; here the F in $L[F, F^{-1}]$ is σ^a-linear, so $F \cdot c = \sigma^a(c) \cdot F$ for all $c \in L$. This category can also be identified with a full subcategory of the category of modules over the skew polynomial ring $L[F; \sigma^a]$, namely the subcategory of modules that are of finite L-dimension and on which the action of F is bijective.

As before, we are mainly interested in the case $a = 1$. By an *F-isocrystal* we mean a σ-F-isocrystal, and we shall abbreviate σ-F-$\mathsf{Isoc}_{/k}$ to F-$\mathsf{Isoc}_{/k}$.

If (M, F) is a σ^a-F-crystal then $(M_{\mathbb{Q}}, F)$ is a σ^a-F-isocrystal. In the other direction, if (N, F) is a σ^a-F-isocrystal then for any W-lattice $M \subset N$ the pair $(M, F_{|M})$ is a σ^a-F-crystal. Up to isogeny the σ^a-F-crystal thus obtained is independent of the choice of the lattice. Indeed, if M_1 and M_2 are W-lattices in N then there exists a $\nu \in \mathbb{Z}$ with $p^\nu M_1 \subseteq M_2$, and then $\cdot p^\nu\colon M_1 \to M_2$ gives an isogeny from $(M_1, F_{|M_1})$ to $(M_2, F_{|M_2})$. So indeed the isocrystals describe crystals up to isogeny, much in the same way as we can pass from abelian varieties over some basis to the category of abelian varieties up to isogeny. More formally, the category σ^a-F-$\mathsf{Isoc}_{/k}$ is equivalent to the localization of the category σ^a-F-$\mathsf{Crys}_{/k}$ ETC

We say that an isocrystal (N, F) is *effective* if there exists a W-lattice $M \subset N$ with $F(M) \subseteq M$.

The category σ^a-F-$\mathsf{Isoc}_{/k}$ is abelian. The category σ^a-F-$\mathsf{Crys}_{/k}$ is additive but not abelian. We still have, in an obvious way, notions like direct sums, kernels and sub-objects. Further, if (M, F) is a σ^a-F-crystal and $M' \subset M$ is a primitive W-submodule that is stable under F then M/M' with Frobenius induced by F is again a σ^a-F-crystal. Here we recall that a W-submodule $M' \subseteq M$ is called primitive if M/M' is torsion-free.

If $k \subset k'$ is an extension of perfect fields we have a functor

$$\text{“extension of scalars”}\colon \sigma^a\text{-}F\text{-}\mathsf{Crys}_{/k} \to \sigma^a\text{-}F\text{-}\mathsf{Crys}_{/k'}\,,$$

sending a pair (M, F) to $\big(W(k') \otimes_{W(k)} M, \sigma^a \otimes F\big)$. Note that if k is finite, this functor depends on the integer a, not only on the automorphism σ^a. The point is that if k has cardinality p^m then σ^a only depends on the class of a modulo m. A similar remark applies to isocrystals.

OrdIterate **(15.13)** Let (M, F) be a σ^a-F-crystal over k. The rank of M as a W-module is called the *height* of (M, F). Similarly, the height of a σ^a-F-isocrystal (N, F) is defined as the L-dimension of the underlying vector space N.

Writing $N := M_{\mathbb{Q}}$ we have that M and $F(M)$ are both W-lattices in N. Hence there exist integers $r < R$ such that $p^R \cdot M \subseteq F(M) \subseteq p^r \cdot M$, and we can define $\mathrm{ord}(F)$, the p-adic order of F, by

$$\mathrm{ord}(F) := \max\big\{r \in \mathbb{Z} \;\big|\; F(M) \subseteq p^r \cdot M\big\}\,.$$

We shall later re-encounter $\mathrm{ord}(F)$ as the first Hodge slope of (M, F); see (15.16) below. The p-adic order of F in general depends on the lattice $M \subset M_{\mathbb{Q}}$, i.e., it is not an isogeny-invariant.

For any $n \in \mathbb{Z}$ we may consider the *nth iterate* (M, F^n), which is a σ^{an}-F-crystal over k. Note that this also makes sense for $n \leqslant 0$. As we shall see later there is no simple rule to

calculate $\mathrm{ord}(F^n)$ from $\mathrm{ord}(F)$. The asymptotic behaviour of $\mathrm{ord}(F^n)$ for $n \to \infty$ is encoded in the first slope of the Newton polygon of (M, F); see (15.21) and () below.

Another useful way to construct new crystals out of a given one is simply to multiply F by a power of p. So, for any $m \in \mathbb{Z}$ we can consider $(M, p^m F)$, which is again a σ^a-F-crystal. It should be regarded as "(M, F), Tate-twisted by m", just as we can consider the Tate twists of a Hodge structure or a Galois representation. (Cf. ??) We have $\mathrm{ord}(p^m F) = m + \mathrm{ord}(F)$.

WedgeCrys **(15.14)** If (M_1, F_1) and (M_2, F_2) are two σ^a-F-crystals over k (for the same exponent a) then we define the tensor product $(M_1 \otimes M_2, F_1 \otimes F_2)$ to be the σ^a-F-crystal with underlying module $M_1 \otimes_W M_2$ and with Frobenius given by $(F_1 \otimes F_2)\big(m_1 \otimes m_2\big) = F_1(m_1) \otimes F_2(m_2)$. Note that $F_1 \otimes F_2$ is well-defined and is indeed again σ^a-linear.

The ith exterior power $\wedge^i_W M$, which by definition is a quotient of $M^{\otimes i}$, inherits the structure of a σ^a-F-crystal (M, F) with Frobenius given by $(\wedge^i F)\big(m_1 \wedge m_2 \wedge \cdots \wedge m_i\big) = F(m_1) \wedge F(m_2) \wedge \cdots \wedge F(m_i)$.

Analogously we can define tensor products and exterior powers of isocrystals.

If (N, F) is a σ^a-F-isocrystal of height h then $\det(N) := \wedge^h_L N$ is an L-vector space of dimension 1. Write $\det(F) = \wedge^h F$, and choose any $0 \neq e \in \det(N)$. Then there is a non-zero $c \in L$ with $\det(F)\big(e\big) = c \cdot e$. The actual value of c depends on the chosen generator, but its valuation does not. Indeed, a different generator is of the form $e' = b \cdot e$ for some $b \in L^*$, and then $F(e') = c' \cdot e'$ with $c' = \big(\sigma^a(b)/b\big) \cdot c$, which has the same order as c. Hence we can define $\mathrm{ord}\det(F) := \mathrm{ord}_p(c)$, where $\mathrm{ord}_p \colon L^* \to \mathbb{Z}$ is the p-adic valuation with $\mathrm{ord}_p(p) = 1$. If $M \subset N$ is any W-lattice in N then the number $\mathrm{ord}\det(F)$ defined in this way equals $\mathrm{ord}\big(\det(F_M)\big)$ as defined above; here we write $F_M := F_{|M}$ and $\det(F_M) := \wedge^h F_M$. So, whereas in general $\mathrm{ord}(F_M)$ depends on the lattice M, for the determinant the p-adic order only depends on the isocrystal. Also note that, using the notation introduced in (15.10), we have $\mathrm{ord}\det(F_M) = \chi\big(M : F(M)\big)$; see Exercise (15.1).

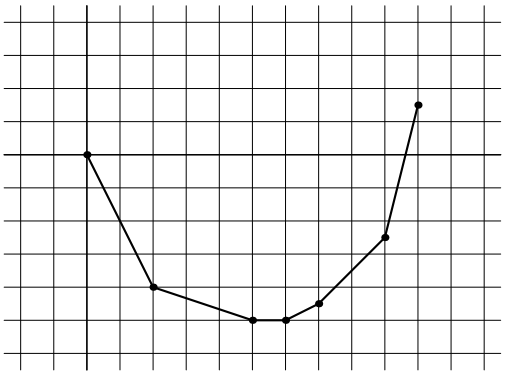
Polygons **(15.15)** To a σ^a-F-crystal we shall associate a Hodge polygon and a Newton polygon. Such a polygon is given by a finite sequence of rational numbers $r_1 \leqslant r_2 \leqslant \cdots \leqslant r_n$. One can also describe it by giving a strictly increasing sequence $\lambda_1 < \lambda_2 < \cdots < \lambda_t$ together with multiplicities $m_1, m_2 \ldots, m_t$ (in $\mathbb{Z}_{>0}$), where the λ_j are the values that occur in the sequence of r_i, and m_j is the number of times that λ_j occurs. So we have

$$\begin{cases} r_1 = r_2 = \cdots = r_{m_1} = \lambda_1 \\ r_{m_1+1} = \cdots = r_{m_1+m_2} = \lambda_2 \\ r_{m_1+m_2+1} = \cdots = r_{m_1+m_2+m_3} = \lambda_3 \\ \cdots \\ r_{m_1+\cdots+m_{t-1}+1} = \cdots = r_{m_1+\cdots m_t} = \lambda_t \end{cases} .$$

The numbers λ_j are called the *slopes* of the polygon.

In practice it is often convenient to have a graphical representation of a polygon. For this we consider the graph of the piecewise linear continuous function $\varphi \colon [0, n] \to \mathbb{R}$ that has $\varphi(0) = 0$ and $\varphi(i) = r_1 + r_2 + \cdots + r_i$ for $1 \leqslant i \leqslant n$, and that is extended linearly between consecutive integers. In terms of the slopes λ_i this means that φ is linear with slope λ_j on the interval $[m_1 + \cdots + m_{j-1}, m_1 + \cdots + m_j]$. In other words, we start at the point $(0, 0)$, draw a line segment to the point $(m_1, m_1\lambda_1)$, from there draw a line segment to $(m_1+m_2, m_1\lambda_1+m_2\lambda_2)$, etc.

Thus, for instance, if the polygon is given by the sequence -2, -2, $-1/3$, $-1/3$, $-1/3$, 0, $1/2$, 1, 1, 4 then the slopes are -2, $-1/3$, 0, $1/2$, 1, and 4, with multiplicities 2, 3, 1, 1, 2 and 1, respectively, and the graphical representation of the polygon is



The points $(m_1 + \cdots + m_j, m_1\lambda_1 + \cdots + m_j\lambda_j)$ are called the *break points* of the polygon. (Indicated in the figure by dots.) By definition, the polygon starts at $(0,0)$, and it ends at the point $(n, \sum r_i) = (\sum m_j, \sum m_j\lambda_j)$.

Note that, because we order the slopes in increasing order, the region of points $(x,y) \in [0,n] \times \mathbb{R}$ lying above the polygon is convex.

HodgePol **(15.16)** Let (M,F) be a σ^a-F-crystal of height h over k. Note that both M and $F(M)$ are W-lattices in $M_{\mathbb{Q}}$. By the theory of modules over a principal ideal domain (see e.g. Bourbaki [1], Chap. 7, § 4, Prop. 4, or Curtis and Reiner [1], § 16) there exist ordered W-bases $\{e_1, \ldots, e_h\}$ and $\{f_1, \ldots, f_h\}$ for M, together with integers $r_1 \leqslant r_2 \leqslant \cdots \leqslant r_h$, such that $F(e_i) = p^{r_i} \cdot f_i$ for all i. The sequence of integers r_i does not depend on the chosen bases. The polygon defined by this sequence is called the *Hodge polygon* of (M,F). We shall denote the Hodge slopes of (M,F) by $\mu_1 < \mu_2 < \cdots < \mu_t$; if necessary we write $\mu_i(M)$ or $\mu_i(M,F)$.

Note that, by construction, all slopes of the Hodge polygon are integers; in particular also the break points of the polygon have integral coordinates. The smallest Hodge slope, $\mu_1 = r_1$, is the largest integer r such that $p^r \cdot M$ contains $F(M)$, and we recognize this as the integer $\mathrm{ord}(F)$ defined previously. The largest Hodge slope, r_h, is the smallest integer s such that $p^s \cdot M$ is contained in $F(M)$.

Let $h_i = h_i(M,F)$ be the multiplicity of $i \in \mathbb{Z}$ as Hodge slope. The numbers h_i are called the *Hodge numbers* of the crystal (M,F). See Example () below for the relation with the classically defined Hodge numbers of a variety.

The Hodge polygon can also be expressed in terms of the orders of the exterior powers of F. For this we just have to remark that $\mathrm{ord}(\wedge^i F)$, which is the smallest Hodge slope of $(\wedge^i M, \wedge^i F)$, equals $r_1 + r_2 + \cdots + r_i$. So the Hodge polygon is obtained by starting at $(0,0)$, plotting the points $\big(i, \mathrm{ord}(\wedge^i F)\big)$ for $1 \leqslant i \leqslant h$, and joining consecutive points by line segments. In particular, the end point of the Hodge polygon of (M,F) is the point $\big(h, \mathrm{ord}\det(F)\big)$.

HodgePolExa **(15.17) Example.** Consider the F-crystal (M,F) over k corresponding to the $W[F]$-module $W[F]/W[F]\cdot(p^2 + pF + pF^2 - F^3)$, where $W[F] := W[F;\sigma]$. In other words, M is free of rank 3 as a W-module, and Frobenius is given on a basis $\{e_1, e_2, e_3\}$ (corresponding to the classes of 1,

F and F^2, respectively) by

$$F(e_1) = e_2$$
$$F(e_2) = e_3$$
$$F(e_3) = p^2 \cdot e_1 + p \cdot e_2 + p \cdot e_3 \,.$$

Then $\{e_1, e_2, e_3' := e_3 - p \cdot e_1 - p \cdot e_2\}$ and $\{e_2, e_3, e_1\}$ are ordered W-bases for M and F is in diagonal form for these bases:

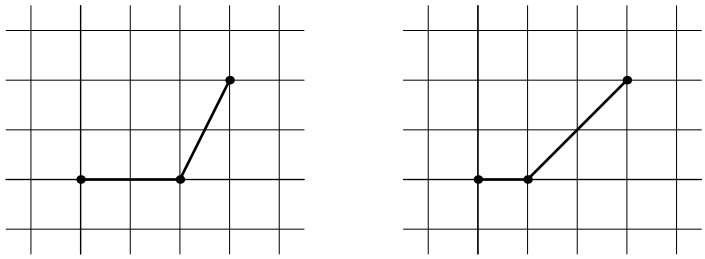
$$F(e_1) = e_2$$
$$F(e_2) = e_3$$
$$F(e_3') = p^2 \cdot e_1 \,.$$

Hence the Hodge slopes of (M, F) are 0 with multiplicity 2 and 2 with multiplicity 1.

If we take $M' \subset M_{\mathbb{Q}}$ the W-lattice generated by $\varepsilon_1 := p \cdot e_1$, $\varepsilon_2 := e_2$ and $\varepsilon_3 := e_3$ then we have

$$F(\varepsilon_1) = p \cdot \varepsilon_2$$
$$F(\varepsilon_2) = \varepsilon_3$$
$$F(\varepsilon_3) = p \cdot \varepsilon_1 + p \cdot \varepsilon_2 + p \cdot \varepsilon_3 \,.$$

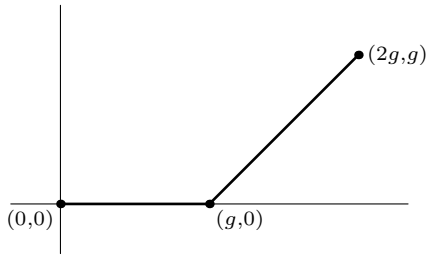
In this case we find, by passing to the basis $\{\varepsilon_1, \varepsilon_2, \varepsilon_3 - p^2\varepsilon_1 - p\varepsilon_2\}$, that the Hodge slopes are 0 with multiplicity 1 and 1 with multiplicity 2.



HP(M) HP(M')

So although (M, F) and (M', F) are isogenous, their Hodge polygons are different.

HodgePolBT **(15.18) Example.** Let G be a p-divisible group over a perfect field k of characteristic p. We define the Hodge polygon of G to be the Hodge polygon of its Dieudonné module. The only slopes that can occur are 0 and 1, say with multiplicities h_0 and h_1. We have $h_0 + h_1 = h$, the height of G, and $h_1 = \dim(G)$, the dimension of G as defined in ??. In particular, the Hodge polygon of an abelian variety X of dimension g is the polygon



with g times slope 0 and g times slope 1.

HiCrysExa **(15.19) Example.** Let X be a proper smooth k-scheme. Crystalline cohomology theory (see e.g. Berthelot [1], Berthelot and Ogus [1], as well as the reports by Illusie [1], [2], [3], [4]) gives

us finitely generated W-modules $H^i_{\mathrm{crys}}(X/W)$ with all the usual functorialities. The relative Frobenius $F_{X/k}\colon X \to X^{(p)}$ induces W-linear maps $F^\sharp\colon H^i_{\mathrm{crys}}(X^{(p)}/W) \to H^i_{\mathrm{crys}}(X/W)$.

If X is an abelian variety over k then the F-crystal obtained in this way from $H^1_{\mathrm{crys}}(X/W)$ can be identified with the Dieudonné module of (the p-divisible group of) X as defined in ??. See ??.

We now start investigating the p-adic order of the iterates of F. We start with an elementary lemma.

FirstNewtLem **(15.20) Lemma.** *Let k be a perfect field of characteristic p.*

(i) *Let (M, F) be a σ^a-F-crystal of height h over k. Then for all $n \in \mathbb{N}$ we have*

DTheory;ordord
$$\operatorname{ord}(F) \leqslant \frac{\operatorname{ord}(F^n)}{n} \leqslant \frac{\operatorname{ord}\det(F)}{h}\,. \tag{1}$$

(ii) *Let (N, F) be a σ^a-F-isocrystal over k. For any W-lattice $M \subset N$ the limit*

DTheory;limord
$$\lim_{n\to\infty} \frac{\operatorname{ord}(F^n_M)}{n} \tag{2}$$

exists, and this limit is independent of the choice of the lattice M.

Proof. (i) Let $r = \operatorname{ord}(F)$. Then $F(M) \subseteq p^r \cdot M$, and by induction on n this gives that $F^n(M) \subseteq p^{rn} \cdot M$. Hence $\operatorname{ord}(F^n) \geqslant rn$, which is the first inequality in (1). For the second inequality we note that $\det(F^n) = \det(F)^n$; hence $\operatorname{ord}\det(F^n) = n \cdot \operatorname{ord}\det(F)$. (Cf. Exercise (15.1).) So it suffices to show that for any σ^a-F-crystal (Λ, φ) of height h we have $h \cdot \operatorname{ord}(\varphi) \leqslant \operatorname{ord}\det(\varphi)$; we then apply this with $\varphi = F^n$. But if $\operatorname{ord}(\varphi) = r$ then $\varphi(\Lambda) \subseteq p^r \cdot \Lambda$. This readily implies that $\det(\varphi)\big(\det(\Lambda)\big) \subseteq p^{hr} \cdot \det(\Lambda)$; so indeed $\operatorname{ord}\det(\varphi) \geqslant hr$.

(ii) Fix a lattice $M \subset N$, and write $F_M := F_{|M}$. It follows from (i) that for any $m \in \mathbb{N}$ the limit $\lambda(m) := \lim_{n\to\infty} \operatorname{ord}(F_M^{m^n})/m^n$ exists. Fix m. Given $\varepsilon > 0$, choose an integer $\nu > 0$ such that $\operatorname{ord}(F_M^{m^\nu})/m^\nu > \lambda(m) - \varepsilon/2$. If $a \in \mathbb{N}$, write $a = q \cdot m^\nu + r$ with $0 \leqslant r < m^\nu$. It follows directly from the definitions that $\operatorname{ord}(F_M^{b+c}) \geqslant \operatorname{ord}(F_M^b) + \operatorname{ord}(F_M^c)$ for all b, $c \in \mathbb{N}$. Using this we find

$$\begin{aligned}
\operatorname{ord}(F^a_M) &\geqslant q \cdot \operatorname{ord}(F_M^{m^\nu}) + r \cdot \operatorname{ord}(F_M) \\
&\geqslant a \cdot \Big(\lambda(m) - \frac{\varepsilon}{2}\Big) + r \cdot \Big(\operatorname{ord}(F_M) - \big(\lambda(m) - \frac{\varepsilon}{2}\big)\Big) \\
&\geqslant a \cdot \Big(\lambda(m) - \frac{\varepsilon}{2}\Big) - m^\nu \cdot \Big|\operatorname{ord}(F_M) - \big(\lambda(m) - \frac{\varepsilon}{2}\big)\Big|\,.
\end{aligned}$$

Hence there exists an $A > 0$ such that $\operatorname{ord}(F^a_M)/a \geqslant \lambda(m) - \varepsilon$ for all $a \geqslant A$. In particular, it follows that $\lambda(m)$ is independent of m. Further, if we have $\operatorname{ord}(F^a_M)/a > \lambda(m)$ for some a then it follows from (i) that $\lambda(a) > \lambda(m)$, contradicting the conclusion just obtained. Hence indeed $\lambda(m) = \lim_{a\to\infty} \operatorname{ord}(F^a_M)/a$.

Next we want to show that the limit in (2) is independent of the chosen lattice. Suppose we have W-lattices M_1 and M_2. Write $F_i := F_{|M_i}$. Choose integers c and d such that $p^c \cdot M_1 \subseteq M_2$ and $p^d \cdot M_2 \subseteq M_1$. We claim that $|\operatorname{ord}(F_1) - \operatorname{ord}(F_2)| \leqslant c + d$. Applying this to the iterates of F (which does not change c and d), this claim implies that the limit in (2) is independent of M. By symmetry it suffices to show that $\operatorname{ord}(F_2) \geqslant \operatorname{ord}(F_1) - c - d$. But this is clear, because if $\operatorname{ord}(F_1) = r$ then

$$F(M_2) \subseteq p^{-d} \cdot F(M_1) \subseteq p^{-d+r} \cdot M_1 \subseteq p^{-c-d+r} \cdot M_2\,,$$

so indeed $\operatorname{ord}(F_2) \geqslant -c-d+r$. □

FirstNewtDef **(15.21) Definition.** Let (N,F) be a σ^a-F-isocrystal over k. Then we define the *first Newton slope* of (N,F), notation $\lambda_1 = \lambda_1(N,F)$, to be the number $\lim_{n\to\infty} \operatorname{ord}(F_M^n)/n$, where $M \subset N$ is any W-lattice.

As we shall prove in Proposition (15.25), the first Newton slope is actually a rational number.

After some preparations we shall define, in (15.31), the Newton polygon of an isocrystal. The first Newton slope as defined here shall appear as the smallest of the Newton slopes; this explains the terminology, which otherwise at this point might seem a bit strange. For a σ^a-F-crystal (M,F) we let $\lambda_1(M,F) := \lambda_1(M_{\mathbb{Q}},F)$.

mu1lambda1Rem **(15.22) Remark.** Let (M,F) be a σ^a-F-crystal of height h. By (1) we have $\operatorname{ord}(F) \leqslant \lambda_1(M,F) \leqslant \operatorname{ord}\det(F)/h$. Now $\operatorname{ord}(F)$ is just the first Hodge slope of (M,F), which we usually denote by $\mu_1 = \mu_1(M,F)$. Using this notation we have

$$\mu_1(M,F) \leqslant \lambda_1(M,F) \leqslant \frac{\operatorname{ord}\det(F)}{h}\,.$$

Note that for $h=1$ this says that $\mu_1(M,F) = \lambda_1(M,F)$.

FirstNewtpmFn **(15.23) Lemma.** *Let (N,F) be a σ^a-F-isocrystal over k. Then we have $\lambda_1(N,p^mF^n) = n\cdot\lambda_1(N,F)+m$ for all m, $n \in \mathbb{Z}$.*

Proof. The relation $\lambda_1(N,F^n) = n\cdot\lambda_1(N,F)$ readily follows from the definition of the first Newton slope. The relation $\lambda_1(N,p^mF) = \lambda_1(N,F)+m$ follows from the relation $\operatorname{ord}(p^{mn}F_M^n) = \operatorname{ord}(F_M^n)+mn$. By combining these two cases we obtain the lemma. □

LatticeLem **(15.24) Lemma.** *Let (N,F) be a σ^a-F-isocrystal of height h over k.*

(i) *If there exists a W-lattice $M \subset N$ such that $F^{h+1}(M) \subseteq p^{-1}\cdot M$ then (N,F) is effective.*

(ii) *Let r and s be integers with $s>0$ and $\lambda_1(N,F) \geqslant r/s$. Then there exists a W-lattice $M \subset N$ with $F^s(M) \subseteq p^rM$.*

Proof. (i) Let $M' := M + F(M) + F^2(M) + \cdots + F^h(M)$, which is again a W-lattice in N. We have

$$\sum_{j=0}^{h+1} F^j(M') = \sum_{j=0}^{2h+1} F^j(M) = M' + \sum_{j=0}^{h+1} F^j\big(F^{h+1}(M)\big) \subseteq p^{-1}\cdot M'\,.$$

Now consider the ascending chain

$$M' \subseteq M' + F(M') \subseteq \cdots \subseteq \sum_{j=0}^{h+1} F^j(M') \subseteq p^{-1}\cdot M'\,.$$

As $p^{-1}M'/M'$ is a k-vector space of dimension h, there exists an index $n \in \{0,1,\ldots,h\}$ with $\sum_{j=0}^{n} F^j(M') = \sum_{j=0}^{n+1} F^j(M')$. Then $M'' := \sum_{j=0}^{n} F^j(M')$ is a lattice with $F(M'') \subseteq M''$, so (N,F) is effective.

(ii) Let $F' := p^{1-r(h+1)}F^{s(h+1)}$. By Lemma (15.23) we have $\lambda_1(N,F') = s(h+1)\lambda_1(N,F) + 1 - r(h+1) \geqslant 1$. Hence there exists a W-lattice $M \subset N$ and an $n \in \mathbb{N}$ such that $(F')^n\big(M\big) \subseteq M$. Let $M' := M + F'(M) + (F')^2(M) + \cdots + (F')^{n-1}$. Clearly $F'(M') \subseteq M'$, which can be

rewritten as $(p^{-r}F^s)^{h+1}(M') \subseteq p^{-1}\cdot M'$. Hence by (i) there exists a lattice $M'' \subset N$ with $p^{-r}F^s(M'') \subseteq M''$. □ iso

We are now ready to prove that the first Newton slope is a rational number, and that, for a suitable choice of a lattice, the limit value $\lambda_1 = \lim_{n\to\infty} \operatorname{ord}(F_M^n)/n$ is already attained for a finite n.

ordFs=rProp **(15.25) Proposition.** *Let (N,F) be a σ^a-F-isocrystal of height h over k. Let $d := \operatorname{ord}\det(F)$. Then there exist integers r and s with $0 < s \leqslant h$ and $r \leqslant d$ and a W-lattice $M \subset N$ such that $\lambda_1(N,F) = r/s$ and $\operatorname{ord}(F_M^s) = r$. In particular, $\lambda_1 \in \mathbb{Q}_{\leqslant d/h}$.*

Proof. We begin by choosing integers r and s with $1 \leqslant s \leqslant h$ and $|\lambda_1 - (r/s)| \leqslant 1/s(h+1)$; see Exercise (15.2) for the existence of such r and s. Let $F' := p^{-r}F^s$. By Lemma (15.23) we have $|\lambda_1(N,F')| = |s\lambda_1(N,F) - r| \leqslant 1/(h+1)$. By (ii) of Lemma (15.24) the inequality $\lambda_1(F') \geqslant -1/(h+1)$ implies that there exists a W-lattice $M' \subset N$ with $(F')^{h+1}\big(M'\big) \subseteq p^{-1}\cdot M'$. Then part (i) of the lemma tells us that there also exists a W-lattice $M \subset N$ with $F'(M) \subseteq M$, so in particular $\lambda_1(F') \geqslant 0$. Precisely the same argument applies to $F'' := (F')^{-1}$; this gives that $\lambda_1(F') = -\lambda_1(F'') \leqslant 0$. Hence $\lambda_1(F') = 0$, and because by the first inequality in (1) we have $0 \leqslant \operatorname{ord}(F'_M) \leqslant \lambda_1(F')$ it also follows that $\operatorname{ord}(F'_M) = 0$. Translating back to the original F, again using Lemma (15.23), we find that $\lambda_1(F) = r/s$ and $\operatorname{ord}(F_M^s) = r$. In particular $\lambda_1 \in \mathbb{Q}$, and because $\lambda_1 \leqslant d/h$ and $1 \leqslant s \leqslant h$ we must have $r \leqslant d$. □

ordFs=rCor **(15.26) Corollary.** *Situation as in* (15.25). *If there exists integers r and $s > 0$ and a lattice $M \subset N$ with $F^s(M) = p^r \cdot M$ then $\lambda_1(N,F) = r/s = d/h$ and $F^h(M) = p^d \cdot M$. Conversely, if $\lambda_1(N,F) = d/h$ then there exists a lattice $M \subset N$ such that $F^h(M) = p^d \cdot M$.*

Proof. If $F^s(M) = p^r \cdot M$ then it follows directly from the definition that $\lambda_1(N,F) = r/s$. Further we have

$$rh = \chi(M : p^r \cdot M) = \chi\big(M : F^s(M)\big) = s \cdot \chi\big(M : F(M)\big) = sd\,,$$

where we recall that $\chi\big(M : F(M)\big) = \operatorname{ord}\det(F_M)$. (See also Exercise (15.1).) Conversely, if $\lambda_1(N,F) = d/h$ then by (ii) of Lemma (15.24) there exists a W-lattice M with $F^h(M) \subseteq p^d \cdot M$. But

$$\chi\big(p^d M : F^h(M)\big) = \chi\big(M : F^h(M)\big) - \chi(M : p^d M) = h \cdot \chi\big(M : F(M)\big) - dh = 0$$

so indeed $F^h(M) = p^d \cdot M$. □

IsoclinicDef **(15.27) Definition.** Let (N,F) be a σ^a-F-isocrystal of height h over k, and let $d := \operatorname{ord}\det(F)$. Then (N,F) is said to be *isoclinic, of slope d/h,* if $\lambda_1(N,F) = d/h$, or, equivalently, if there exist integers r and $s > 0$ (necessarily with $r/s = d/h$) and a lattice $M \subset N$ such that $F^s(M) = p^r \cdot M$.

As we shall discuss in () below, if (N,F) is isoclinic and $M \subset N$ is a lattice with $F^s(M) = p^r \cdot M$ then the Hodge polygon of (M,F) coincides with its Newton polygon, and this polygon has only one slope, viz. d/h.

HomIsoclinics **(15.28) Proposition.** *Let k be a perfect field of characteristic p.*

(i) *If (N,F) is an isoclinic σ^a-F-isocrystal over k then any sub-isocrystal and quotient-isocrystal of (N,F) is isoclinic too, of the same slope.*

(ii) *If (N_1, F_1) and (N_2, F_2) are isoclinic σ^a-F-isocrystals over k of different slopes then* $\mathrm{Hom}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}\big((N_1,F_1),(N_2,F_2)\big) = 0$.

(iii) *Given a σ^a-F-isocrystal (N, F) over k and a slope $\lambda \in \mathbb{Q}$, there exists a unique maximal sub-isocrystal of (N, F) that is isoclinic of slope λ.*

Proof. (i) Let $M \subset N$ be a W-lattice with $F^h(M) = p^d \cdot M$. If $N' \subset N$ is an F-stable subspace, let $M' := N' \cap M$, which is a W-lattice in N'. Then $F^h(M') = F^h(N' \cap M) = N' \cap F^h(M) = N' \cap p^d \cdot M = p^d \cdot (N' \cap M) = p^d \cdot M'$, so indeed $(N', F_{|N'})$ is again isoclinic of slope d/h. Similarly, if $q\colon N \twoheadrightarrow N''$ is a quotient then $M'' := q(M)$ is a lattice in N'' and $F^h(M'') = F^h\big(q(M)\big) = q\big(F^h(M)\big) = q(p^d \cdot M) = p^d \cdot q(M) = p^d \cdot M''$. The assertions in (ii) and (iii) readily follow from (i). □

NlambdaExa **(15.29) Example.** Let $\lambda \in \mathbb{Q}$, and write $\lambda = d/h$ with $h > 0$ and $\gcd(d, h) = 1$. Define, for $a \in \mathbb{Z} \setminus \{0\}$, a σ^a-F-crystal $\mathscr{M}_\lambda$ over k by taking $\mathscr{M}_\lambda := W \cdot e_1 \oplus \cdots \oplus W \cdot e_h$ with

$$F(e_i) = \begin{cases} e_{i+1} & \text{if } 1 \leqslant i < h; \\ p^d \cdot e_1 & \text{if } i = h. \end{cases}$$

In terms of (left) modules over the ring $W[F] = W[F; \sigma^a]$ we can also say that we take $\mathscr{M}_\lambda := W[F]/W[F] \cdot (F^h - p^d)$. It is clear that $F^h = p^d$ on $\mathscr{M}_\lambda$, so $\mathscr{M}_\lambda$ is isoclinic of slope λ. It follows from (i) of the proposition that the corresponding isocrystal $\mathscr{N}_\lambda := L \otimes_W \mathscr{M}_\lambda$ is simple, because if $\mathscr{N}' \subset \mathscr{N}_\lambda$ is a subobject, say of height h' and with $\mathrm{ord}\det(F_{|\mathscr{N}'}) = d'$, then $d'/h' = d/h$, which by the assumption that $\gcd(d, h) = 1$ is possible only if $h' = h$, so $\mathscr{N}' = \mathscr{N}_\lambda$.

If there is a risk of confusion we shall use the notation $\mathscr{N}_\lambda^{(a)}$ to indicate the exponent a.

Using the description $\mathscr{N}_\lambda = L[F]/L[F] \cdot (F^h - p^d)$ with $L[F] = L[F; \sigma^a]$ it is not hard to calculate the endomorphism algebra of $\mathscr{N}_\lambda$. We shall first do this under the assumption that k contains a field with p^{ah} elements.

An endomorphism $\alpha \in \mathrm{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}(\mathscr{N}_\lambda)$ is completely determined by $\alpha(\bar{1})$, and this should be a class representable by a polynomial $f = c_0 + c_1F + \cdots + c_{h-1}F^{h-1}$ with $(F^h - p^d) \cdot f \in L[F] \cdot (F^h - p^d)$. But $(F^h - p^d) \cdot f$ is the class represented by

$$\big(\sigma^{ah}(c_0) - c_0\big)p^d + \big(\sigma^{ah}(c_1) - c_1\big)p^d \cdot F + \cdots + \big(\sigma^{ah}(c_{h-1}) - c_{h-1}\big)p^d \cdot F^{h-1}\,,$$

so as a necessary and sufficient condition for f to give an endomorphism we find that $\sigma^{ah}(c_i) = c_i$ for all $i \in \{0, 1, \ldots, h_1\}$. Note that if α is the endomorphism sending $\bar{1}$ to $\bar{f}$ and β is the endomorphism sending $\bar{1}$ to $\bar{g}$, then $\beta \circ \alpha$ sends $\bar{1}$ to the class of fg. The fixed field of σ^{ah} in L can be identified with $\mathbb{Q}_{p^{ah}}$, the fraction field of $W(\mathbb{F}_{p^{ah}})$. (Here we use the assumption that $k \supseteq \mathbb{F}_{p^{ah}}$.) Then the conclusion is that

$$\mathrm{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}(\mathscr{N}_\lambda) = \Big(\mathbb{Q}_{p^{ah}}[F; \sigma^a]/(F^h - p^d)\Big)^{\mathrm{opp}}\,.$$

Note that $F^h - p^d$ lies in the centre of $\mathbb{Q}_{p^{ah}}[F; \sigma^a]$, so it generates a 2-sided ideal. One recognizes $\mathbb{Q}_{p^{ah}}[F; \sigma^a]/(F^h - p^d)$ as the cyclic algebra $(\mathbb{Q}_{p^{ah}}/\mathbb{Q}_{p^a}, \sigma^a, p^d)$, which is the division algebra with centre $\mathbb{Q}_{p^a}$ and invariant $\lambda = d/h$ in the Brauer group $\mathrm{Br}(\mathbb{Q}_{p^a})$; cf. Appendix A, especially (A.5) and (A.6). Hence $\mathrm{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}(\mathscr{N}_\lambda)$ is the central simple algebra over $\mathbb{Q}_{p^a}$ with Brauer invariant $-d/h$. Note that in this case we know that the endomorphism algebra is a division algebra (and not just a simple algebra) because $\mathscr{N}_\lambda$ is simple.

The situation is a little more subtle if we work over a field k that does not contain $\mathbb{F}_{p^{ah}}$. For instance, suppose $a = 1$. Let $k_0 \subset k$, the algebraic part of the extension $\mathbb{F}_p \subset k$, be the

largest subfield of k that is finite. Let p^m be the cardinality of k_0 and let $h' := \gcd(h, m)$. The fixed field of σ^h in L can be identified with $\mathbb{Q}_{p^{h'}}$, and the above calculation now gives that $\mathrm{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}(\mathscr{N}_\lambda)$ is the opposite of the algebra $\mathbb{Q}_{p^{h'}}[F;\sigma]/(F^h - p^d)$. The latter is the cyclic algebra $(\mathbb{Q}_{p^{h'}}/\mathbb{Q}_p, \sigma, p^d)$, which is the division algebra with centre $\mathbb{Q}_p$ and Brauer invariant d/h'. For the general case see Exercise (15.3).

SlopeDec **(15.30) Theorem.** (Slope decomposition) *Let (N, F) be a σ^a-F-isocrystal over a perfect field k of characteristic p. For $\lambda \in \mathbb{Q}$ let (N_λ, F) be the maximal sub-isocrystal that is isoclinic of slope λ. Then we have a decomposition of σ^a-F-isocrystals $(N, F) = \oplus_{\lambda\in\mathbb{Q}}(N_\lambda, F)$.*

The decomposition thus obtained is referred to as the *slope decomposition* of (N, F). Note that this is a theorem about isocrystals, i.e., crystals up to isogeny. If (M, F) is a σ^a-F-crystal and if we write $N := M_\mathbb{Q}$ then $M_\lambda := M \cap N_\lambda$ is a W-lattice in N_λ and (M_λ, F) is a sub-crystal of (M, F). However, in general the inclusion $\oplus_{\lambda\in\mathbb{Q}} M_\lambda \hookrightarrow M$ is not an isomorphism, only an isogeny. Under some further assumptions it is sometimes possible to obtain a decomposition at the level of the crystal; see for instance Katz [2], Thm. 1.6.1 on "Newton-Hodge decompositions".

Proof. Write $\lambda_1(N, F) = r/s$. Consider the isocrystal $(N', F') := (N, p^{-r}F^s)$, which by Lemma (15.23) has first Newton slope $\lambda_1(N') = 0$. Suppose we know the theorem for (N', F'); so we have a slope decomposition $N' = \oplus_{\nu\in\mathbb{Q}} N'_\nu$. By (ii) of Proposition (15.28) the endomorphism $F \in \mathrm{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}\big((N', F')\big)$ respects this slope decomposition, so (N'_ν, F) is a sub-isocrystal of (N, F). Writing $\nu = a/b$ there exists a W-lattice $M \subset N'_\nu$ with $(F')^b\big(M\big) = p^a \cdot M$. Hence $F^{bs}(M) = p^{a+rb}\cdot M$, so (N'_ν, F) is isoclinic of slope $(a+rb)/sb = (\nu+r)/s$. If we set $N_\lambda := N'_{s\lambda-r}$ then $N = \oplus_{\lambda\in\mathbb{Q}} N_\lambda$ is the desired slope decomposition of N.

In the rest of the proof we may assume that $\lambda_1(N, F) = 0$. Using induction on the height of (N, F) we are done if we can show that there is a decomposition of isocrystals $(N, F) = (N_{\text{ét}}, F) \oplus (N', F)$ with $(N_{\text{ét}}, F)$ isoclinic of slope 0 and $\lambda_1(N', F) > 0$.

By (ii) of Lemma (15.24) there exists a W-lattice $M \subset N$ such that $F(M) \subseteq M$. (I.e., (N, F) is effective.) For each $n \in \mathbb{N}$ we have that M/p^nM is a module of finite length over the ring $W[F;\sigma^a]$. Put

$$(M/p^nM)_{\text{ét}} := \cap_{i\geqslant 1}\,\mathrm{Im}(F^i) \qquad \text{and} \qquad (M/p^nM)' := \cup_{i\geqslant 1}\,\mathrm{Ker}(F^i)\,.$$

Then $(M/p^nM)_{\text{ét}}$ and $(M/p^nM)'$ are stable under F, and we have a Fitting Decomposition

$$M/p^nM = (M/p^nM)_{\text{ét}} \oplus (M/p^nM)'\,;$$

see e.g. Lam [1], Thm (19.16). It follows that $(M/p^nM)_{\text{ét}}$ is the largest submodule of M/p^nM on which F is bijective.

Let π: $M/p^{n+1}M \to M/p^nM$ be the canonical map. It is clear that π maps $(M/p^{n+1}M)_{\text{ét}}$ to $(M/p^nM)_{\text{ét}}$ and $(M/p^{n+1}M)'$ to $(M/p^nM)'$. Hence by passing to the limit we obtain a decomposition

$$M = \varprojlim M/p^nM = M_{\text{ét}} \oplus M' \qquad \text{with} \quad M_{\text{ét}} := \varprojlim (M/p^nM)_{\text{ét}} \quad \text{and} \quad M' := \varprojlim (M/p^nM)'\,.$$

By construction this gives a decomposition of σ^a-F-crystals $(M, F) = (M_{\text{ét}}, F) \oplus (M', F)$ with F bijective on $M_{\text{ét}}$, so $(M_{\text{ét}}, F)$ is isoclinic of slope 0. Further, for r sufficiently big we have $F^r = 0$ on $(M/pM)'$, as M/pM has finite length. This means that $F^r(M') \subset pM'$, so $\lambda_1(M'_\mathbb{Q}, F) > 0$. Hence by passing to isocrystals we obtain the desired decomposition of (N, F). □

NPDef **(15.31) Definition.** Let (N,F) be a σ^a-F-isocrystal over k. Consider its slope decoposition $(N,F) = \oplus_{\lambda\in\mathbb{Q}}(N_\lambda,F)$. We define the *Newton polygon* of (N,F) to be the polygon whose slopes are the numbers $\lambda\in\mathbb{Q}$ with $N_\lambda\neq 0$, and where we take each λ with multiplicity m_λ equal to the height of (N_λ,F) (i.e, the L-dimension of N_λ). New New

If (M,F) is a σ^a-F-crystal then we define its Newton polygon to be the Newton polygon of the associated isocrystal $(M_{\mathbb{Q}},F)$.

By its very definition, the Newton polygon is an isogeny invariant. There are subtle relations between the Hodge polygon and the Newton polygon of a crystal; we shall further investigate these in ?? below. The Newton polygon is invariant under extension of the base field.

We refer to the slopes in the Newton polygon of an isocrystal simply as the *Newton slopes* and we denote by $m_\lambda = m_\lambda(N,F)\in\mathbb{Z}_{\geqslant 0}$ the multiplicity of λ as a slope in the Newton polygon of (N,F).

Observe that the breakpoints of the Newton polygon are integral, i.e., lie in $\mathbb{Z}^2$. Indeed, if (N,F) is isoclinic of slope λ and height h then we have seen in Corollary (15.26) that $h\lambda = \operatorname{ord}\det(F)\in\mathbb{Z}$. So each isoclinic piece contributes to the Newton polygon a segment of integral horizontal length (the height) and integral vertical length (the p-adic order of $\det(F)$).

Intuitively, the Newton slopes are the valuations of the eigenvalues of F. Note that, because the map $F\colon N\to N$ is σ^a-linear, there is no well-defined notion of an eigenvalue. In order to make precise in what way we can still talk about the valuations of the eigenvalues, we consider a purely ramified extension $L\subset L' = L\big[\sqrt[e]{p}\big]$ where the ramification index e is chosen such that $e\lambda_i\in\mathbb{Z}$ for all Newton slopes λ_i. We extend σ to an automorphism of L' by the requirement that $\sigma\big(\sqrt[e]{p}\big) = \sqrt[e]{p}$. Then we can find a basis of $L'\otimes_L N$ on which the matrix of $\sigma^a\otimes F$ is upper triangular of the form

$$\begin{pmatrix}
p^{\lambda_1} & * & * & * & * & * & * & * & * & * \\
 & \ddots & * & * & * & * & * & * & * & * \\
 & & p^{\lambda_1} & * & * & * & * & * & * & * \\
 & & & p^{\lambda_2} & * & * & * & * & * & * \\
 & & & & \ddots & * & * & * & * & * \\
 & & & & & p^{\lambda_2} & * & * & * & * \\
 & & & & & & & * & * & * \\
 & & \mathbf{0} & & & & \ddots & * & * & * \\
 & & & & & & & & & * \\
 & & & & & & & & & p^{\lambda_t}
\end{pmatrix}$$

with $p^{\lambda_i} := \big(\sqrt[e]{p}\big)^{e\lambda_i}$. See Exercise (15.4). So in this sense the Newton slopes may indeed be thought of as the valuations of the eigenvalues of F. Some care has to be taken here, though. If we simple choose any basis for N, let Φ be the matrix of F with respect to this basis, and then calculate the eigenvalues of Φ in some algebraic closure $\overline{L}$ of L, then it is not true, in general, that the valuations of these eigenvalues give the correct Newton slopes. See however Theorem (15.35) below, where we obtain a positive result in this direction for isocrystals over a finite field.

Our next goal is to prove an important theorem of Dieudonné [1] that gives a complete and explicit classification of isocrystals over an algebraically closed field. As explained earlier, the advantage of working with general σ^a-F-isocrystals is that we can easily reduce the proof to a problem about isocrystals of slope 0. In that case everything boils down to a concrete statement in semilinear algebra, which we now prove first.

DThmLemma **(15.32) Lemma.** *Let k be an algebraically closed field of characteristic p. Let $\nu \in \mathbb{Z} \setminus \{0\}$, and write $\mathbb{F} \subset k$ for the unique subfield with $p^{|\nu|}$ elements.*

(i) *Let V be a finite dimensional k-vector space, and let $\varphi\colon V \to V$ be a bijective Frob_k^ν-linear map. Further let $V_0 := \{v \in V \mid \varphi(v) = v\}$, which is an $\mathbb{F}$-subspace of V. Then the natural map $k \otimes_{\mathbb{F}} V_0 \to V$ is an isomorphism.*

(ii) *Let M be a free $W(k)$-module of finite rank, and let $F\colon M \to M$ be a bijective σ^ν-linear map. Further let $M_0 := \{m \in M \mid F(m) = m\}$, which is a $W(\mathbb{F})$-submodule of M. Then the natural map $W(k) \otimes_{W(\mathbb{F})} M_0 \to M$ is an isomorphism.*

Proof. (i) We assume that $V \neq 0$; otherwise there is nothing to prove. Further we can assume that $\nu > 0$, as the assertion about (V, φ) follows from the statement for (V, φ^{-1}). We begin by showing that $V_0 \neq 0$. Start with any $0 \neq v \in V$. Let n be the largest positive integer such that the vectors $v, \varphi(v), \dots, \varphi^n(v)$ are linearly independent. Then there is a relation

$$\varphi^{n+1}(v) = c_n\varphi^n(v) + c_{n-1}\varphi^{n-1}(v) + \cdots + c_1\varphi(v) + c_0 v\,.$$

For $0 \leqslant i \leqslant n$, let $d_i := c_i + c_{i-1}^p + \cdots + c_0^{p^i}$. By direct calculation one finds that $w := \sum_{i=0}^n d_i\varphi^i(v)$ satisfies $\varphi(w) = w$. Further, as the coefficients c_i are not all zero, the same is true for the coefficients d_i, so w is a nonzero element in V_0.

The natural map $k \otimes_{\mathbb{F}} V_0 \to V$ is injective. Write kV_0 for the image. If $kV_0 \subsetneq V$ then $\overline{V} := V/kV_0$ is a nonzero k-vector space, on which we have an induced map $\overline{\varphi}$. Applying what we have just proved to the pair $(\overline{V}, \overline{\varphi})$, there is a nonzero $w \in \overline{V}$ with $\varphi(w) = w$. We are done if we can show that w can be lifted to an element $v \in V$ with $\varphi(v) = v$. Start with any $v \in V$ lifting w. Then $x := \varphi(v) - v \in kV_0$. For any $y \in kV_0$ the element $v' = v + y$ is again a lifting of w, and $\varphi(v') - v' = \varphi(v) - v + \varphi(y) - y = x + \varphi(y) - y$. So it suffices to show that the map $kV_0 \to kV_0$ given by $y \mapsto \varphi(y) - y$ is surjective. But this is clear, for if $e_1, \dots, e_r$ is an $\mathbb{F}$-basis of V_0 then $kV_0 \cong ke_1 + \cdots + ke_r$, with φ given by $(y_1, \dots, y_r) \mapsto (y_1^{p^\nu}, \dots, y_r^{p^\nu})$. So if $x = (x_1, \dots, x_r)$ then we have to solve the equations $y_i^{p^\nu} - y_i + x_i = 0$, and this can be done because $\nu > 0$ and $k = \overline{k}$.

(ii) As in the proof of (i) we may assume that $\nu > 0$. Let $W := W(k)$, and let $\tau := \sigma^\nu$. As the map $W \otimes_{W(\mathbb{F})} M_0 \to M$ is injective, we are done if we can show that M_0 spans M over W.

Write $V := M/pM$, and let $\varphi\colon V \to V$ be the map induced by F. Let $\varepsilon = \{e_1, \dots, e_r\}$ be a W-basis for M such that the elements $e_i \bmod p$ form a k-basis for V_0; this is possible by (i). Let Φ be the matrix of F with respect to the basis ε. By construction $\Phi \equiv \mathrm{id} \bmod p$. If $A = (a_{ij})$ is a matrix in $\mathrm{GL}_r(W)$ then the matrix of F with respect to the basis $A\varepsilon$ is $A^{-1}\Phi\ {}^\tau A$; here ${}^\tau A = \big(\tau(a_{ij})\big)$. By induction on n we construct matrices $A_n \in \mathrm{GL}_r(W)$ such that $A_{n+1} \bmod p^n = A_n \bmod p^n$ and $A_n^{-1}\Phi\ {}^\tau A_n \equiv \mathrm{id} \bmod p^n$. For $n = 1$ we can take $A_1 = \mathrm{id}$. Suppose we have already found $A_1, \dots, A_n$ with the desired properties. Let $\Psi = (\psi_{ij}) \in M_n(W)$ be the matrix with $A_n^{-1}\Phi\ {}^\tau A_n = \mathrm{id} + p^n \cdot \Psi$. Because $k = \overline{k}$ there exist elements $b_{ij} \in W$ such that their reductions $\overline{b}_{ij}$ modulo p satisfy $\overline{b}_{ij}^{p^\nu} - \overline{b}_{ij} + \overline{\psi}_{ij} = 0$. Set $A_{n+1} := A_n \cdot (\mathrm{id} + p^n B)$ with $B = (b_{ij})$. Note that A_{n+1} is again invertible because $\det(A_{n+1}) \equiv \det(A_n) \bmod p^n$ and $n \geqslant 1$. Also note that $A_{n+1}^{-1} \equiv (\mathrm{id} - p^n B) \cdot A_n^{-1} \bmod p^{n+1}$. Hence calculating modulo p^{n+1} we find

$$A_{n+1}^{-1}\Phi\ {}^\tau A_{n+1} \equiv (\mathrm{id} - p^n B)(\mathrm{id} + p^n\Psi)(\mathrm{id} + p^n \cdot {}^\tau B) \equiv \mathrm{id} + p^n \cdot (\Psi + {}^\tau B - B)\,,$$

and by our choice of the matrix B the term $(\Psi + {}^\tau B - B)$ vanishes modulo p. So we can take A_{n+1} as the next term in the sequence.

Finally let $A_\infty \in \mathrm{GL}_r(W)$ be the limit of the sequence (A_n), where we note that this limit is again invertible because $\det(A_\infty) \equiv \det(A_1) = 1 \bmod p$. By construction, the matrix of F

on the basis $A_\infty \cdot \varepsilon$ is the identity matrix. So M has a W-basis contained in M_0 and we are done. □

ThmDieudonne **(15.33) Theorem.** (Dieudonné) *Let $k = \overline{k}$ be an algebraically closed field of characteristic p, and let $a \in \mathbb{Z} \setminus \{0\}$. Then the category σ^a-F-$\mathsf{Isoc}_{/k}$ is semisimple. The simple objects are the isocrystals $\mathscr{N}_\lambda$, for $\lambda \in \mathbb{Q}$, defined in* Example (15.29). *If (N, F) is any σ^a-F-isocrystal over k then we have*

$$(N, F) \cong \bigoplus_{\lambda \in \mathbb{Q}} \mathscr{N}_\lambda^{\oplus \frac{m_\lambda}{h(\lambda)}} ,$$

where $h(\lambda) = \dim_L(\mathscr{N}_\lambda)$ is the height of $\mathscr{N}_\lambda$, and where $m_\lambda = \dim_L(N_\lambda) \in \mathbb{Z}_{\geqslant 0}$ is the multiplicity of λ as a Newton slope of (N, F).

Proof. We already know that the isocrystals $\mathscr{N}_\lambda$ are simple, so it suffices to show that every σ^a-F-isocrystal (N, F) is isomorphic to a direct sum of objects $\mathscr{N}_\lambda$. By Theorem (15.30) it suffices to prove this under the additional assumption that (N, F) is isoclinic, of slope λ.

Write $\lambda = d/h$ with $h > 0$ and $\gcd(d, h) = 1$, and write $\mathscr{N}_\lambda = L[F; \sigma^a]/(F^h - p^d)$. (So $h = h(\lambda)$ is the height of $\mathscr{N}_\lambda$, not of (N, F).) Write $H := \mathrm{Hom}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}\big(\mathscr{N}_\lambda, (N, F)\big)$. We have an isomorphism $H \xrightarrow{\sim} N_0 := \big\{n \in N \;\big|\; F^h(n) = p^d \cdot n\big\}$ by sending f to $f(\overline{1})$. This is an isomorphism of left modules over the ring

$$B := \mathbb{Q}_{p^{ah}}[F; \sigma^a]/(F^h - p^d) = \mathrm{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}(\mathscr{N}_\lambda)^{\mathrm{opp}} ,$$

which, as we have seen in Example (15.29), is the division algebra with centre $\mathbb{Q}_{p^a}$ and Brauer invariant d/h.

The main point of the proof is that the B-dimension of N_0 equals m_λ/h, with $m_\lambda = \dim_L(N)$, the height of (N, F). As B has dimension h over its subfield $\mathbb{Q}_{p^{ah}}$ this is equivalent to the assertion that $\dim_{\mathbb{Q}_{p^{ah}}}(N_0) = \dim_L(N)$. To see this, consider $F' := p^{-d} \cdot F^h$. Then (N, F') is an isoclinic σ^{ah}-F-isocrystal of slope 0, so there exists a W-lattice $M \subset N$ with $F'(M) = M$. Now $M_0 := N_0 \cap M$ is a $W(\mathbb{F}_{p^{ah}})$-lattice in N_0, and by (ii) of Lemma (15.32) the rank of M_0 over $W(\mathbb{F}_{p^{ah}})$ equals $\mathrm{rank}_W(M) = \dim_L(N)$. So indeed $\dim_B(N_0) = m_\lambda/h$.

To conclude the argument, write $t := m_\lambda/h$ and choose a B-basis $e_1, \ldots, e_t$ for $H \cong N_0$. We claim that the map $\rho\colon \mathscr{N}_\lambda^{\oplus t} \to (N, F)$ given by $(y_1, \ldots, y_t) \mapsto e_1(y_1) + \cdots + e_t(y_t)$ is injective. By what we have shown, $\mathscr{N}_\lambda^t$ and N have the same dimension, so the claim implies that ρ is an isomorphism, which is what we want to prove.

We view ρ as a homomorphism of modules over the ring $L[F; \sigma^a]$, which is artinian because it has finite dimension over L. Suppose $\mathrm{Ker}(\rho) \neq 0$. Choose a simple submodule $\mathscr{N}' \subset \mathrm{Ker}(\rho)$. Because $\mathscr{N}_\lambda$ is simple, the Jordan-Hölder Theorem (see e.g. ??) implies that $\mathscr{N}' \cong \mathscr{N}_\lambda$ as $L[F; \sigma^a]$-modules. Hence they are also isomorphic as σ^a-F-isocrystals, say by an isomorphism $\gamma\colon \mathscr{N}_\lambda \xrightarrow{\sim} \mathscr{N}'$. If $j\colon \mathscr{N}' \hookrightarrow \mathscr{N}_\lambda^t$ is the inclusion, the composition $j \circ \gamma\colon \mathscr{N}_\lambda \hookrightarrow \mathscr{N}_\lambda^t$ is given by a t-tuple $(b_1, \ldots, b_t) \in B^t$ with $b_i \neq 0$ for at least one index i. By construction, $b_1 e_1 + \cdots b_t e_t = 0$. This contradicts the assumption that the elements e_i form a B-basis for H. Hence ρ is injective, and this finishes the proof. □

ThmDieudRem **(15.34) Remarks.** (i) The statements in the theorem do not hold for $a = 0$!

(ii) Let k be an arbitrary perfect field of characteristic p. Let (N, F) be a σ^a-F-isocrystal over k. In general there is no finite extension of k over which (N, F) becomes isomorphic to a direct sum of objects $\mathscr{N}_\lambda$. Further the category σ^a-F-$\mathsf{Isoc}_{/k}$ is in general not semisimple. For

instance, consider the F-isocrystal (N,F) over $\mathbb{F}_p$ with $N=\mathbb{Q}_p^2$ and F given on the standard basis $\{e_1,e_2\}$ by the matrix $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. Then (N,F) is isoclinic of slope 0 (note that F maps the standard lattice $\mathbb{Z}_p^2$ bijectively to itself), and it is clear that $(\mathbb{Q}_p e_1,F)$ is a sub-isocrystal. Now we extend scalars to a finite field $\mathbb{F}_q$ with $q=p^m$, and we try to find a $\gamma\in L=\mathbb{Q}_{p^m}$ such that $\big(L\cdot(\gamma e_1+e_2),F\big)$ is a complementary sub-isocrystal. The condition we find is that $\gamma=\sigma(\gamma)+1$. In $W(\mathbb{F}_q)$ this has no solution, because by iteration we get

$$\gamma=\sigma(\gamma)+1=\sigma^2(\gamma)+2=\cdots=\sigma^m(\gamma)+m=\gamma+m\,,$$

which leads to a contradiction. So (N,F) is not a semisimple object in $F\text{-}\mathsf{Isoc}_{/\mathbb{F}_q}$ for any q, and in particular it is not isomorphic to $\mathscr{N}_0^{\oplus 2}$. The equation $\gamma=\sigma(\gamma)+1$ does have a solution in $W(\overline{\mathbb{F}}_p)$, but if we write a solution γ as a Witt vector, $\gamma=(\gamma_0,\gamma_1,\ldots)$ then the coefficients $\gamma_i\in\overline{\mathbb{F}}_p$ have unbounded degrees over $\mathbb{F}_p$.

NewtPol/Fq **(15.35) Theorem.** *Let (N,F) be a σ^a-F-isocrystal of height h over a finite field $\mathbb{F}_q$ with $q=p^m$. Let $\pi:=F^m$, which is an L-linear endomorphism of N, and let $f=\det(t\cdot\mathrm{id}_N-\pi)$ be its characteristic polynomial, which is a monic polynomial of degree h. Let $\{\alpha_a,\ldots,\alpha_h\}$ be the multiset of roots of f in some fixed algebraic closure $L\subset\overline{L}$. If* $\mathrm{ord}\colon\overline{L}^*\to\mathbb{Q}$ *is the valuation with* $\mathrm{ord}(p)=1$ *then the slopes of the Newton polygon of (N,F) are the numbers* $\mathrm{ord}(\alpha_i)/\mathrm{ord}(q)$*, counted with their multiplicities.*

Proof. Without loss of generalization we may assume that (N,F) is isoclinic, say of slope $\lambda=d/h$. We have to show that for all roots α of h we have $h\cdot\mathrm{ord}(\alpha)=d\cdot\mathrm{ord}(q)$. Write $F':=p^{-d}F^h$. Then (N,F') is isoclinic of slope 0 and $q^{-d}\alpha^h$ is a root of the characteristic polynomial of $\pi':=(F')^m=q^{-d}\cdot\pi^h$. On the other hand, because (N,F') is isoclinic of slope 0 there exists a $W(\mathbb{F}_q)$-lattice $M\subset N$ with $F'(M)=M$. Hence also $\pi'(M)=M$, so all eigenvalues of π' are units in $O_{\overline{L}}$, as both π' and $(\pi')^{-1}$ are integral over $W(\mathbb{F}_q)$. This gives the desired relation $-d\cdot\mathrm{ord}(q)+h\cdot\mathrm{ord}(\alpha)=0$. □

We now combine the theorem with a classical method, called the Newton polygon method, to determine the valuations of the roots of a polynomial over a p-adic field in terms of its coefficients. See for instance Neukirch [1], Chap. II, § 6. This gives us the following efficient way of calculating the Newton polygon of (N,F) over $\mathbb{F}_q$ once we know the characteristic polynomial of $\pi=F^m$.

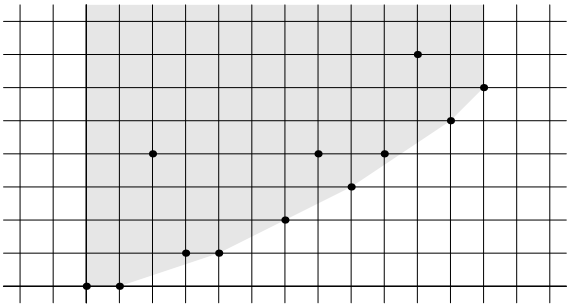
NPFqAlgo **(15.36) Corollary.** *Situation as in* (15.35)*. Write the characteristic polynomial of π as $f=c_ht^h+c_{h-1}t^{h-1}+\cdots+c_1t+c_0$; in particular $c_h=1$. Then the Newton polygon of (N,F) is obtained by taking the lower convex hull of the set of points $\big(i,\frac{\mathrm{ord}(c_{h-i})}{\mathrm{ord}(q)}\big)$ for $i=0,1,\ldots,h$ with $c_{h-i}\neq 0$.*

NPFqExa **(15.37) Example.** Suppose we work over $\mathbb{F}_p$ and the characteristic polynomial of $F=\pi$ is

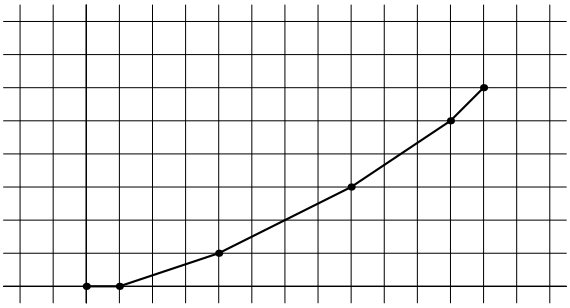
$$f=t^{12}+t^{11}+p^4t^{10}+pt^9+pt^8+p^2t^6+p^4t^5+p^3t^4+p^4t^3+p^7t^2+p^5t+p^6\,.$$

We draw in the plane the points $\big(i,\mathrm{ord}(c_{12-i})\big)$, where c_i is the coefficient of t^i, and, within the region $\big\{(x,y)\in\mathbb{R}^2\;\big|\;0\leqslant x\leqslant 12\big\}$, we take the lower convex hull of this set of points. Note that we simply omit the point $\big(5,\mathrm{ord}(c_7)\big)$, as $c_7=0$; if we wanted to give meaning to this point it

would have to be $(5, \infty)$, which has no effect on the lower convex hull anyway.



Then the Newton polygon of (N, F) is the boundary of this region, discarding the vertical halflines at $x = 0$ and $x = 12$.



So the conclusion is that after extension of scalars to $\overline{\mathbb{F}}_p$, our isocrystal (N, F) is isomorphic to $\mathscr{N}_0 + \mathscr{N}_{1/3} + \mathscr{N}_{1/2}^{\oplus 2} + \mathscr{N}_{2/3} + \mathscr{N}_1$.

FIsocFqRem **(15.38) Remark.** Let (N_1, F_1) and (N_2, F_2) be two F-isocrystals over a finite field $\mathbb{F}_q$, with $q = p^m$. Let $\pi_i := F_i^m$, for $i = 1$, 2, be the associated linear automorphism of N_i, and regard N_i as a module over $\mathbb{Q}_{p^m}[t]$ by letting t act as π_i. Then (N_1, F_1) and (N_2, F_2) are isomorphic as F-isocrystals if and only if N_1 and N_2 are isomorphic as $\mathbb{Q}_{p^m}[t]$-modules. For a proof, by purely ring-theoretic methods, see Jacobson [1], Corollary to Thm. 33.

Newton>Hodge **(15.39) Theorem.** *Let (M, F) be a σ^a-F-crystal of height h over k. Then the Newton polygon of (M, F) lies on or above its Hodge polygon, and the two polygons have the same begin point, namely $(0, 0)$, and end point, namely $\big(h, \operatorname{ord}\det(F)\big)$.*

Proof. We may assume that $k = \overline{k}$. Let $r_1 = \mu_1(M, F) \leqslant r_2 \leqslant \cdots \leqslant r_h$ be the Hodge slopes and $s_1 = \lambda_1(M, F) \leqslant s_2 \leqslant \cdots \leqslant s_h$ the Newton slopes. Let Hodge: $[0, h] \to \mathbb{R}$ and Newton: $[0, h] \to \mathbb{R}$ be the functions whose graphs are the Hodge and Newton polygons, respectively. Both functions are linear on intervals $[i, i+1]$, and by definition we have $\text{Hodge}(i) = r_1 + \cdots + r_i$ and $\text{Newton}(i) = s_1 + \cdots + s_i$. As remarked in (15.16) we have $\text{Hodge}(i) = \mu_1(\wedge^i M, \wedge^i F)$, the first Hodge slope of $\wedge^i M$. We claim that, similarly, we have $\text{Newton}(i) = \lambda_1(\wedge^i M, \wedge^i F)$, the first Newton slope of $\wedge^i M$. To see this, let R be a common denominator for the Newton slopes. By Theorem (15.33) there is an L-basis $e_1, \ldots, e_h$ for $M_{\mathbb{Q}}$ on which F^R is given by the diagonal matrix with diagonal coefficients p^{Rs_i}. From this our claim readily follows, using that $(\wedge^i F)^R = \wedge^i (F^R)$, and using Lemma (15.23).

As remarked in (15.22) we have $\lambda_1 \geqslant \mu_1$ for any σ^a-F-crystal. Applying this to the exterior powers of (M, F) we find that $\text{Newton}(i) \geqslant \text{Hodge}(i)$ for all $i \in \{0, 1, \ldots, h\}$, so indeed the

Newton polygon is on or above the Hodge polygon. By definition both polygons start at $(0,0)$. Taking $i = h$ in the above, we find that the assertion that the polygons have the same end point just means that $\mu_1(\det M, \det F) = \lambda_1(\det M, \det F)$, which is clear as $\det M$ has rank 1; cf. Remark (15.22). □

ord

sup

§3. *The Newton polygon of an abelian variety.*

OrdSSDef **(15.40) Definition.** Let X be an abelian variety of dimension g over a field of characteristic $p > 0$. Then X is said to be *ordinary* if its Newton polygon is given by $0^g 1^g$; this is equivalent to the condition that $f(X) = g$. We say that X is *supersinguar* if its Newton polygon is given by $(1/2)^{2g}$.

In Figures 1 and 2 we give, for dimensions up to 4, the complete list of possible Newton polygons. The arrows indicate which specializations are possible according to ??; as we shall discuss in ?? these specializations all indeed occur. The dotted polygons are the Hodge polygons. For $g = 4$ we also give the p-rank.

Exercises.

Ex:chiMFsM **(15.1)** Let (M, F) be a σ^a-F-crystal over a perfect field k.

(i) Show that $\chi\big(M : F(M)\big) = \operatorname{ord}\det(F)$.

(ii) Show that $\chi\big(M : F^s(M)\big) = s \cdot \chi\big(M : F(M)\big)$ for all $s \geqslant 1$.

Ex:Approximate **(15.2)** Let λ be a real number, and let $h \geqslant 1$ be an integer. Show that there exist integers r and s with $1 \leqslant s \leqslant h$ and $|\lambda - (r/s)| \leqslant 1/s(h+1)$.

Ex:EndNlambda **(15.3)** Let $\lambda = d/h$ with $h > 0$ and $\gcd(d,h) = 1$. Let $a \in \mathbb{Z} \setminus \{0\}$, let k be a perfect field of characteristic p, and consider the σ^a-F-isocrystal $\mathscr{N}_\lambda$ defined in Example (15.29). Let $k_0 \subset k$ be the largest subfield that is finite, and let p^m be its cardinality. Define $\delta := \gcd(a,m)$. Show that $\operatorname{End}_{\sigma^a\text{-}F\text{-}\mathsf{Isoc}_{/k}}(\mathscr{N}_\lambda)$ is the division algebra with centre $\mathbb{Q}_{p^\delta}$ and Brauer invariant $-d/[(a/\delta)\cdot\gcd(h, m/\delta)]$.

Ex:Fuptriang **(15.4)** Consider a σ^a-F-isocrystal (N, F) over a perfect field k of characteristic p. Let L be the fraction field of $W(k)$ and let σ be its Frobenius automorphism.

(i) If (N, F) is isoclinic of slope 0, show that there exists a basis for N on which the matrix of F is upper triangular with all diagonal coefficients equal to 1. [*Hint:* Look at the proof of Lemma (15.32), part (i).]

(ii) For a general (N, F), let $\lambda_1 < \lambda_2 < \cdots < \lambda_t$ be the Newton slopes, and let e be a common denominator of the λ_i. (So $e\lambda_i \in \mathbb{Z}$ for all i; for instance one can take $e = h!$, where h is the height). Consider the purely ramified extension $L \subset L' := L[X]/(X^e - p)$. Let $u \in L'$ be the class of X; so " $u = \sqrt[e]{p}$ ". For any $\lambda \in \mathbb{Q}$ with $e\lambda \in \mathbb{Z}$, write $p^\lambda := u^{e\lambda}$. Extend σ to an automorphism of L' by the requirement that $\sigma(u) = u$. Show that there is a basis of $L' \otimes_L N$ on which the matrix of $\sigma^a \otimes F$ is upper triangular with diagonal coefficients p^{λ_i}. [*Hint:* First reduce to the isoclinic case. If (N, F) is isoclinic of slope r/s, first apply (i) to find a vector $n \in N$ with $F^s(n) = p^r \cdot n$. Now argue as in the proof of Lemma (15.32),

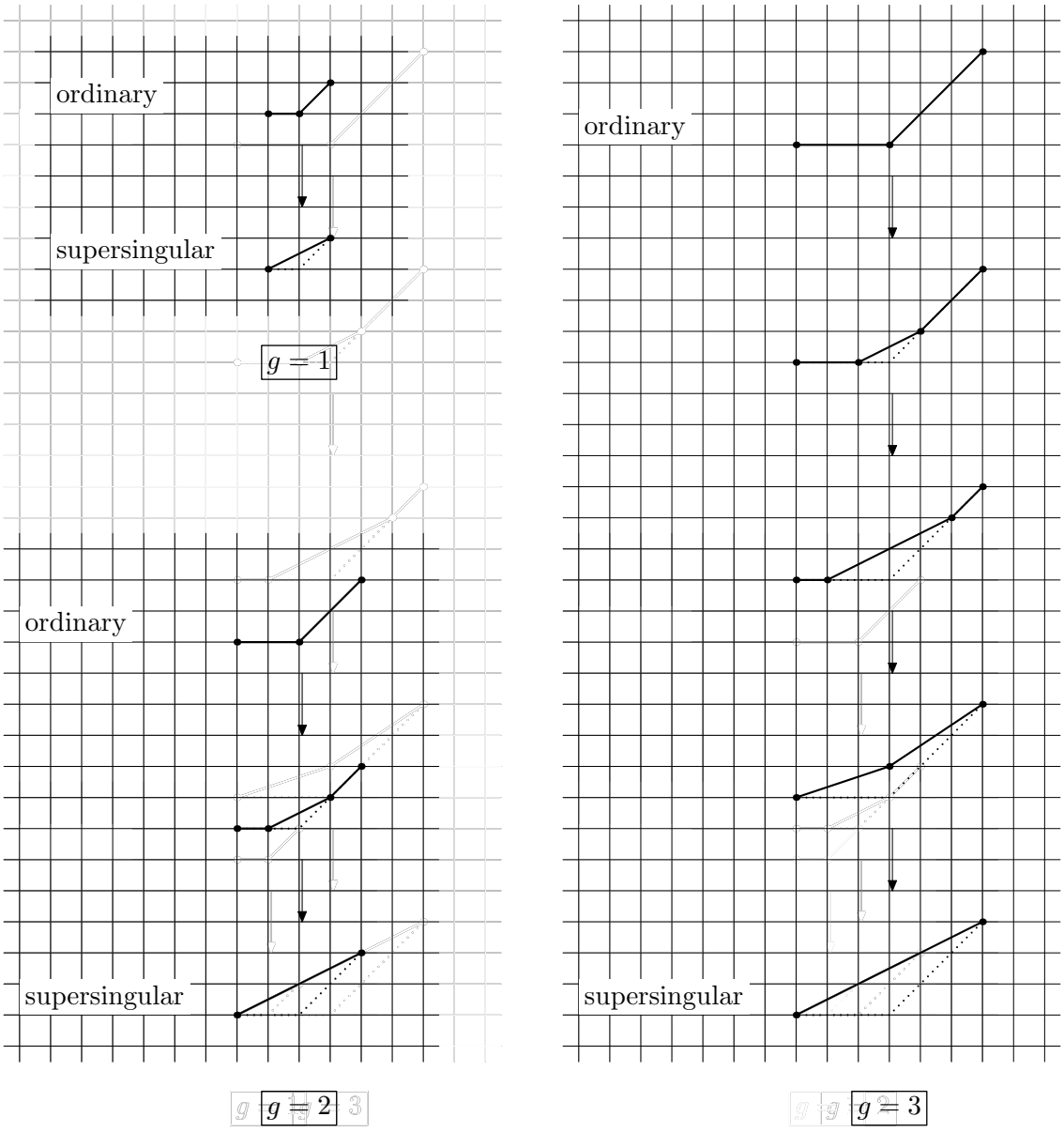


Figure 1. Newton polygons and their specializations for $g = 1$, 2 and 3.

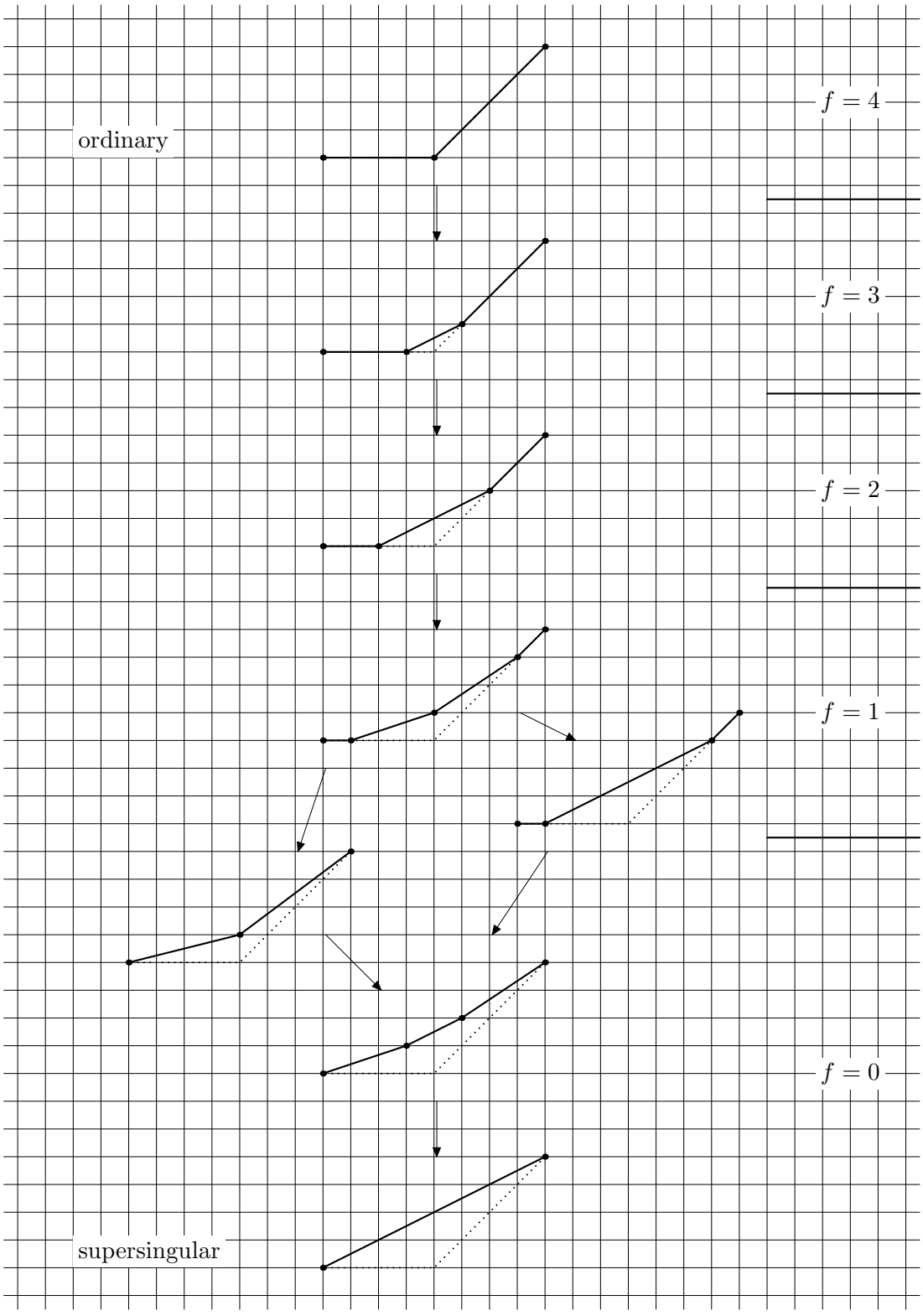


Figure 2. Newton polygons and their specializations for $g = 4$.

part (i).]

cry
iso

As the theme of this chapter is that of abelian varieties over a finite field k, it will come as no surprise that the main character of this chapter is the geometric Frobenius morphism π_X of an abelian variety X relative to k (which raises the coordinates of a point to the exponent $\#k$).

The first goal is to understand the eigenvalues of the induced action by Frobenius on the Tate modules of an abelian variety and on the p-visible group with $p = \mathrm{char}(k)$. Then we characterize the homomorphisms between abelian varieties by the induced Galois module homomorphisms of the corresponding Tate modules and we study the endomorphism algebras. After this we describe which numbers occur as eigenvalues of Frobenius. We also deal with the question which rings occur as endomorphism rings. We illustrate the result with the case of elliptic curves. We finish with a description of the category of abelian varieties over a finite field using the canonical lift.

The finiteness of the ground field plays an important role in the following way. If we fix the cardinality of the finite field k then it is a fundamental fact that the number of k-isomorphism classes of g-dimensional abelian varieties with a polarization of degree d^2 defined over k is finite. This follows from the fact that if $\lambda\colon X \to X^t$ denotes such a polarization of degree d^2 then 3λ defines an embedding of X into a fixed projective space of dimension $3^g d - 1$ as a variety of degree $3^g d\,(g!)$. A general theorem (cf. ??) says that there exists a scheme (Chow scheme) of finite type that parametrizes all varieties of fixed dimension g and fixed degree in projective space. This scheme has only finitely many points over k. Alternatively, the existence of a moduli space of abelian varieties with a given polarization implies the result.

§1. *The eigenvalues of Frobenius.*

GeomFrobDef **(16.1)** Let $q = p^m$ be a power of a prime number. As customary, $\mathbb{F}_q$ denotes the field with q elements. We fix an algebraic closure $\mathbb{F}_q \subset \overline{\mathbb{F}}_q$. For any $n \in \mathbb{Z}_{>0}$ we take $\mathbb{F}_{q^n}$ to be the unique subfield of $\overline{\mathbb{F}}_q$ with q^n elements.

For any scheme X over $\mathbb{F}_q$ we have a morphism $\pi_X\colon X \to X$ over $\mathbb{F}_q$, called the *geometric Frobenius of* X, which is defined to be the identity on the underlying topological space and is given by $f \mapsto f^q$ on (sections of) the structure sheaf O_X. In particular, on affine schemes $\mathrm{Spec}(A)$ the geometric Frobenius corresponds to the endomorphism of A given by $a \mapsto a^q$. If there is a need to indicate the ground field, we shall write $\pi_{X/\mathbb{F}_q}$ instead of π_X.

As is clear from the definitions, for a finite extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ the geometric Frobenius of $X \otimes \mathbb{F}_{q^n}$ over $\mathbb{F}_{q^n}$ equals π_X^n, the nth power of π_X. More formally, we have the relation $\pi_{(X\otimes\mathbb{F}_{q^n})/\mathbb{F}_{q^n}} = \pi^n_{X/\mathbb{F}_q} \otimes \mathrm{id}$ as morphisms from $X \otimes \mathbb{F}_{q^n}$ to itself.

We can also describe the geometric Frobenius as an "iterated relative Frobenius". To be precise, if $q = p^m$ then π_X equals the composition

$$X \xrightarrow{F_{X/\mathbb{F}_q}} X^{(p)} \xrightarrow{F_{X^{(p)}/\mathbb{F}_q}} X^{(p^2)} \xrightarrow{F_{X^{(p^2)}/\mathbb{F}_q}} \quad \dots \quad \xrightarrow{F_{X^{(p^{m-1})}/\mathbb{F}_q}} X^{(p^m)},$$

where we note that $X^{(p^m)} = X^{(q)} = X$. So in the notation of (5.21) we have $\pi_X = F^m_{X/\mathbb{F}_q}$.

If $f\colon X \to Y$ is any morphism of $\mathbb{F}_q$-schemes then $\pi_Y \circ f = f \circ \pi_X$. In particular, if $\mathbb{F}_q \subset k$ is a field extension then π_X acts on the set $X(k)$ of k-valued points by sending $x\colon \operatorname{Spec}(k) \to X$ to $\pi_X \circ x$, which equals the composition

$$\operatorname{Spec}(k) \xrightarrow{\pi_{\operatorname{Spec}(k)}} \operatorname{Spec}(k) \xrightarrow{x} X\,.$$

More concretely, if we have an embedding $X \hookrightarrow \mathbb{P}^N$ over $\mathbb{F}_q$ then π_X acts by raising all coordinates to the qth power, i.e., $\pi_X\big((a_0 : \cdots : a_N)\big) = (a_0^q : \cdots : a_N^q)$. As $\mathbb{F}_{q^n} = \big\{a \in \overline{\mathbb{F}}_q \;\big|\; a^{q^n} = a\big\}$, it follows that $X(\mathbb{F}_{q^n})$ is the set of fixed points of π_X^n acting on $X(\overline{\mathbb{F}}_q)$; so

$$X(\mathbb{F}_{q^n}) = \big\{x \in X(\overline{\mathbb{F}}_q) \;\big|\; \pi_X^n(x) = x\big\}\,.$$

GeomFrobAV **(16.2)** Let X be an abelian variety of dimension g over $\mathbb{F}_q$. As the origin of X is an $\mathbb{F}_q$-rational point, it is fixed under π_X. Hence π_X is an endomorphism of X as an abelian variety. The description of π_X as an iterated relative Frobenius, together with Proposition (5.15), shows that π_X is a purely inseparable isogeny of degree q^g.

As mentioned above, for any morphism $f\colon X \to Y$ of schemes over $\mathbb{F}_q$ we have $f \circ \pi_X = \pi_Y \circ f$. In particular, π_X commutes with all endomorphisms of X, and lies therefore in the centre of the endomorphism algebra $\operatorname{End}^0(X)$.

We write $f_X = P_{\pi_X}$ for the characteristic polynomial of π_X. It is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$, and for any $n \in \mathbb{Z}$ we have $f_X(n) = \deg(n - \pi_X)$. For any prime number $\ell \neq p$ we know by Theorem (12.18) that f_X is also the characteristic polynomial of the induced endomorphism $T_\ell(\pi_X)$ of the Tate module $T_\ell X$. We usually refer to f_X as *the characteristic polynomial of Frobenius*, with the understanding that the "Frobenius" in question is the geometric Frobenius endomorphism.

piXsemisimple **(16.3) Proposition.** *Let X be an abelian variety over $\mathbb{F}_q$.*

(i) *Let ℓ be a prime number, $\ell \neq p$. Then $V_\ell(\pi_X)$ is a semisimple automorphism of $V_\ell X$.*

(ii) *Assume X is elementary over $\mathbb{F}_q$ (i.e., isogenous to a power of a simple abelian variety). Then $\mathbb{Q}[\pi_X] \subset \operatorname{End}^0(X)$ is a field, and f_X is a power of the minimum polynomial $f_{\mathbb{Q}}^{\pi_X}$ of π_X over $\mathbb{Q}$.*

Proof. (i) As remarked above, π_X lies in the centre of $\operatorname{End}^0(X)$, which is a product of number fields. Hence $\mathbb{Q}[\pi_X] \subset \operatorname{End}^0(X)$ is a product of (number) fields, too. It follows that also $\mathbb{Q}_\ell[\pi_X] \subset \mathbb{Q}_\ell \otimes \operatorname{End}^0(X)$ is a product of fields; in particular $\mathbb{Q}_\ell[\pi_X]$ is a semisimple ring. Now $V_\ell X$ is a module of finite type over $\mathbb{Q}_\ell[\pi_X]$, with π_X acting as the automorphism $V_\ell(\pi_X)$. Hence $V_\ell X$ is a semisimple $\mathbb{Q}_\ell[\pi_X]$-module, and this means that $V_\ell(\pi_X)$ is a semisimple automorphism.

(ii) If X is elementary then the centre of $\operatorname{End}^0(X)$ is a field, so also $\mathbb{Q}[\pi_X]$ is a field. Let $g := f_{\mathbb{Q}}^{\pi_X}$ be the minimum polynomial of π_X over $\mathbb{Q}$. If $\alpha \in \overline{\mathbb{Q}}_\ell$ is an eigenvalue of $V_\ell(\pi_X)$ then $g(\alpha)$ is an eigenvalue of $g\big(V_\ell(\pi_X)\big) = V_\ell\big(g(\pi_X)\big) = V_\ell(0) = 0$; hence $g(\alpha) = 0$. Note that these eigenvalues (the roots of f_X) are algebraic over $\mathbb{Q}$, as f_X has rational coefficients. So every root of f in $\overline{\mathbb{Q}}$ is also a root of g, which just means that f_X divides a power of g. Because g is irreducible this implies that f is a power of g. □

HasseWeil **(16.4) Theorem.** *Let X be an abelian variety of dimension g over $\mathbb{F}_q$.*

(i) *Every complex root α of f_X has absolute value $|\alpha| = \sqrt{q}$.*

(ii) *If α is a complex root of f_X then so is $\bar\alpha = q/\alpha$, and the two roots occur with the same multiplicity. If $\alpha = \sqrt{q}$ or $\alpha = -\sqrt{q}$ occurs as a root then it occurs with even multiplicity.*

Proof. (i) We first reduce to the case that X is simple (over $\mathbb{F}_q$). For this, choose an isogeny $h\colon X \to X' = X_1 \times \cdots \times X_s$ where the factors X_i are simple. Then h induces an isomorphism $V_\ell(h)\colon V_\ell X \xrightarrow{\sim} V_\ell X' = V_\ell X_1 \oplus \cdots \oplus V_\ell X_s$, and because $h \circ \pi_X = \pi_{X'} \circ h$ the automorphism $V_\ell(h) \circ V_\ell(\pi_X) \circ V_\ell(h)^{-1}$ of $V_\ell X_1 \oplus \cdots \oplus V_\ell X_s$ is the one given by

$$(\xi_1, \dots, \xi_s) \mapsto \big(V_\ell(\pi_{X_1})(\xi_1), \dots, V_\ell(\pi_{X_s})(\xi_s)\big)\,.$$

Hence $f_X = f_{X_1} \cdots f_{X_s}$ and we find that it suffices to prove the theorem for simple abelian varieties.

Let λ be any polarization of X, and let $\dagger$ denote the associated Rosati involution on $\mathrm{End}^0(X)$. We first show that $\pi_X \cdot \pi_X^\dagger = q$. Because $\pi_X \cdot \pi_X^\dagger = \pi_X \cdot \lambda^{-1} \cdot \pi_X^t \cdot \lambda = \lambda^{-1} \cdot \pi_{X^t} \cdot \pi_X^t \cdot \lambda$, it suffices to show that $\pi_{X^t} \cdot \pi_X^t = [q]_{X^t}$. But $\pi_X = F^m_{X/\mathbb{F}_q}$, so by Proposition (7.34) we have $\pi_X^t = V^m_{X^t/\mathbb{F}_q}$, and as in (5.21) it follows that $\pi_{X^t} \cdot \pi_X^t = F^m_{X^t/\mathbb{F}_q} \cdot V^m_{X^t/\mathbb{F}_q} = [p^m]_{X^t} = [q]_{X^t}$.

Because X is simple, $\mathbb{Q}[\pi_X]$ is a number field, and as f_X is a power of the minimum polynomial of π_X over $\mathbb{Q}$ the complex roots of f_X are precisely the complex numbers of the form $\iota(\pi_X)$ for some embedding $\iota\colon \mathbb{Q}[\pi_X] \to \mathbb{C}$. The relation $\pi_X^\dagger = q/\pi_X$ shows that $\mathbb{Q}[\pi_X] \subset \mathrm{End}^0(X)$ is stable under the Rosati involution, which by ?? is a positive involution. This leaves two possible cases:

(a) Totally real case: $\mathbb{Q}[\pi_X]$ is a totally real field and $\dagger$ is the identity on $\mathbb{Q}[\pi_X]$.
(b) CM case: $\mathbb{Q}[\pi_X]$ is a CM-field and for every complex embedding $\iota\colon \mathbb{Q}[\pi_X] \to \mathbb{C}$ we have $\iota(x^\dagger) = \overline{\iota(x)}$, for all $x \in \mathbb{Q}[\pi_X]$.

In either case the relation $\pi_X \cdot \pi_X^\dagger = q$ implies that all complex roots α of f_X have absolute value $|\alpha| = \sqrt{q}$.

(ii) The first two assertions are trivial, because f_X has real (even rational) coefficients. The only non-trivial point is that $\sqrt{q}$ and $-\sqrt{q}$ can only occur as root with even multiplicity, and again it suffices to show this under the assumption that X is simple. Because a CM field has no real embeddings, $\pm\sqrt{q}$ can only occur as a root of f_X in the totally real case, and in that case they are the only possible roots, because of the relation $\alpha\bar{\alpha} = q$. If $\sqrt{q}$ occurs with multiplicity n then $-\sqrt{q}$ occurs with multiplicity $2g - n$, so $f_X(0) = (-1)^n q^g$. But $f_X(0) = \deg(-\pi_X) = q^g$, so n is even. □

HasseWeilRem **(16.5) Remarks.** (i) An alternative argument showing that $\pi_X \cdot \pi_X^\dagger = q$ is the following. Let $L := (\mathrm{id}, \lambda)^* \mathscr{P}_X$, which is an ample bundle on X. By Proposition (11.1) we have $\varphi_L = 2\lambda$, and $\dagger$ is also the polarization associated to φ_L. Hence $\pi_X^\dagger \cdot \pi_X = \varphi_L^{-1} \cdot \pi_X^t \cdot \varphi_L \cdot \pi_X$, so we want to show that $\pi_X^t \cdot \varphi_L \cdot \pi_X = \varphi_L \cdot q$. Because L is a line bundle on X (over $\mathbb{F}_q$) we have $\pi_X^* L = L^q$, as π_X sends the transition functions to their qth powers. (Caution: This only works for line bundles on X itself, not for line bundles on X_T with T an arbitrary $\mathbb{F}_q$-scheme.) For any $x \in X(T)$ we then have

$$\begin{aligned}\big(\pi_X^t \cdot \varphi_L \cdot \pi_X\big)(x) &= \big[\pi_X^*\big(t^*_{\pi_X(x)} L \otimes L^{-1}\big)\big] \\ &= \big[t_x^* \pi_X^* L \otimes \pi_X^* L^{-1}\big] \\ &= \big[t_x^* L^q \otimes L^{-q}\big] = \varphi_{L^q}(x) = q \cdot \varphi_L(x)\,,\end{aligned}$$

which proves the desired relation.

(ii) Given a prime power q, let $f \in \mathbb{Z}[t]$ be a monic polynomial of degree $2g$ such that all complex roots have absolute value $\sqrt{q}$, and such that if $\pm\sqrt{q}$ is a root of f then it has even multiplicity. It is not always the case that f occurs as the characteristic polynomial of Frobenius of an abelian variety over $\mathbb{F}_q$. However, we shall see in ?? below that there is always some power

of f that occurs as f_X for some abelian variety X. Also we shall see there that the totally real case is a very exceptional one.

(iii) The theorem implies that the characteristic polynomial of Frobenius satisfies the identity $t^{2g} \cdot f_X(q/t) = q^g \cdot f_X(t)$. (To see this, note that f_X can be written over $\mathbb{R}$ as a product of quadratic factors of the form $h = (t-\alpha)(t-\bar{\alpha})$ with $\alpha\bar{\alpha} = q$; for such a factor we have $t^2 \cdot h(q/t) = q \cdot h(t)$.) If we write

$$f_X = t^{2g} + c_{2g-1}t^{2g-1} + \cdots + c_2 t^2 + c_1 t + c_0$$

then this identity for f_X just says that $c_i = q^{2g-i} \cdot c_{2g-i}$.

As we shall see later, the isogeny class of an abelian variety X over a finite field is completely determined by the associated characteristic polynomial f_X, and every algebraic integer π that has absolute value $\sqrt{q}$ under all embeddings $\mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$ occurs, in a suitable sense, as Frobenius of an abelian variety over $\mathbb{F}_q$. See § 6 of this Chapter.

ZetaFunction **(16.6)** If Y is a scheme of finite type over $\mathbb{F}_q$ then for any positive integer n the number $N_n := \#Y(\mathbb{F}_{q^n})$ of $\mathbb{F}_{q^n}$-rational points of Y is finite. The sequence of numbers N_n is conveniently encoded in the zeta function of Y, defined by

$$Z(Y;t) := \exp\left(\sum_{n=1}^{\infty} N_n \cdot \frac{t^n}{n}\right) \qquad \in \mathbb{Q}[\![t]\!]\,.$$

For an alternative definition, let $|Y|_{\mathrm{cl}}$ denote the set of closed points of Y, and for $y \in |Y|_{\mathrm{cl}}$ let $\deg(y) := \big[\mathbb{F}_q(y) : \mathbb{F}_q\big]$. Then $Z(Y;t)$ can also be written as an infinite product:

$$Z(Y;t) = \prod_{y \in |Y|_{\mathrm{cl}}} \big(1 - t^{\deg(y)}\big)^{-1}\,.$$

ZetaAVFF **(16.7) Theorem.** *Let X be an abelian variety of dimension g over $\mathbb{F}_q$. Let $\{\alpha_1, \ldots, \alpha_{2g}\}$ be the multiset of complex roots of the characteristic polynomial f_X, so that we have $f_X = \prod_{i=1}^{2g}(t-\alpha_i)$. If I is a subset of $\{1, \ldots, 2g\}$, define $\alpha_I := \prod_{i\in I}\alpha_i$.*

(i) *For any positive integer n we have*

$$\#X(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1-\alpha_i^n) = \sum_{j=0}^{2g}(-1)^j \cdot \mathrm{trace}(\pi_X^n; \wedge^j V_\ell X)\,,$$

where ℓ is any prime number different from p and where by $\mathrm{trace}(\pi_X^n; \wedge^j V_\ell X)$ we mean the trace of the automorphism $\wedge^j V_\ell(\pi_X^n)$ of $\wedge^j V_\ell X$.

(ii) *The zeta function of X is given by*

$$Z(X;t) = \prod_{j=0}^{2g} P_j^{(-1)^{j+1}} = \frac{P_1 P_3 \cdots P_{2g-1}}{P_0 P_2 \cdots P_{2g}}\,,$$

where $P_j \in \mathbb{Z}[t]$ is the polynomial given by

$$P_j = \prod_{\substack{I \subset \{1,\ldots,2g\} \\ \#I = j}} \big(1 - t \cdot \alpha_I\big) = \det\big(\mathrm{id} - t \cdot \pi_X; \wedge^j V_\ell X\big)\,,$$

the reciprocal characteristic polynomial of $\wedge^j V_\ell(\pi_X)$.

(iii) *The zeta function satisfies the functional equation* $Z\big(X;\frac{1}{q^g t}\big) = Z(X;t)$.

Proof. (i) The characteristic polynomial $P_{\pi_X^n}$ of π_X^n is equal to $\prod_{i=1}^{2g}(t-\alpha_i^n)$. By what was explained in (16.1) the kernel of $\mathrm{id}-\pi_X^n$ in $X(\overline{\mathbb{F}}_q)$ is precisely $X(\mathbb{F}_{q^n})$. As this is finite, $\mathrm{id}-\pi_X^n$ is an isogeny. Because π_X is purely inseparable it induces the zero map on the tangent space. Hence $\mathrm{id}-\pi_X^n$ induces the identity on the tangent space, so it is a separable isogeny. This implies that $\#X(\mathbb{F}_{q^n}) = \deg(\mathrm{id}-\pi_X^n) = P_{\pi_X^n}(1) = \prod_{i=1}^{2g}(1-\alpha_i^n)$.

The eigenvalues of $\wedge^j V_\ell(\pi_X^n)$ are the numbers α_I^n where I runs over all subsets of $\{1,\dots,2g\}$ of cardinality j. The second identity in (i) therefore follows from the elementary relation

$$\prod_{i=1}^{2g}(1-\alpha_i^n) = \sum_{j=0}^{2g}\Big((-1)^j \cdot \sum_{\substack{I\subset\{1,\dots,2g\}\\ \#I=j}} \alpha_I^n\Big)\,.$$

(ii) We use the general fact (see HAG, Appendix C, Lemma 4.1) that for an endomorphism φ of a finite dimensional vector space V over a field K we have an identity of formal power series

$$\exp\left(\sum_{n=1}^{\infty}\mathrm{trace}(\varphi^n;V)\cdot\frac{t^n}{n}\right) = \det(\mathrm{id}-t\cdot\varphi;V)^{-1}\,. \tag{1}$$

VFF:fpsidentity

Applying (i) then gives

$$\begin{aligned} Z(X;t) &= \exp\left(\sum_{n=1}^{\infty}\sum_{j=0}^{2g}(-1)^j\cdot\mathrm{trace}(\pi_X^n;\wedge^j V_\ell X)\cdot\frac{t^n}{n}\right)\\ &= \prod_{j=0}^{2g}\exp\left(\sum_{n=1}^{\infty}\mathrm{trace}(\pi_X^n;\wedge^j V_\ell X)\cdot\frac{t^n}{n}\right)^{(-1)^j} = \prod_{j=0}^{2g}\det(\mathrm{id}-t\cdot\pi_X;\wedge^j V_\ell X)^{(-1)^{j+1}}\,. \end{aligned}$$

The eigenvalues of $\wedge^j V_\ell(\pi_X)$ are the numbers α_I for $I\subset\{1,\dots,2g\}$ of cardinality j, so

$$\det(\mathrm{id}-t\cdot\pi_X;\wedge^j V_\ell X) = \prod_{\substack{I\subset\{1,\dots,2g\}\\ \#I=j}}\big(1-t\cdot\alpha_I\big) =: P_j\,.$$

As $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ naturally acts on the multiset $\{\alpha_I\}_{I\subset\{1,\dots,2g\},\#I=j}$ this polynomial has rational coefficients. As furthermore P_j is a monic and all its roots are algebraic integers we have $P_j\in\mathbb{Z}[t]$.

(iii) For any $j\in\{0,\dots,2g\}$ the eigenvalues of $\wedge^{2g-j}V_\ell(\pi_X)$ are the numbers α_K where K runs over all subsets of $\{1,\dots,2g\}$ of cardinality $2g-j$. Because $\prod_{i=1}^{2g}=q^g$, these are also the numbers q^g/α_I where I runs over all subsets of $\{1,\dots,2g\}$ of cardinality j. So

$$P_{2g-j} = \prod_{\substack{I\subset\{1,\dots,2g\}\\ \#I=j}}\left(1-\frac{tq^g}{\alpha_I}\right) = \prod_{\substack{I\subset\{1,\dots,2g\}\\ \#I=j}} -\frac{tq^g}{\alpha_I}\cdot\left(1-\frac{\alpha_I}{tq^g}\right)\,.$$

The number of subsets $I\subset\{1,\dots,2g\}$ with $\#I=j$ equals the dimension of $\wedge^j V_\ell X$, which is $\binom{2g}{j}$. Further,

$$\prod_{\substack{I\subset\{1,\dots,2g\}\\ \#I=j}}\alpha_I = (\alpha_1\cdots\alpha_{2g})^{\frac{j}{2g}\cdot\binom{2g}{j}} = q^{\frac{j}{2}\cdot\binom{2g}{j}}\,,$$

as each α_i occurs $\binom{2g-1}{j-1} = \frac{j}{2g} \cdot \binom{2g}{j}$ times as a factor. Hence

$$P_{2g-j} = (-t)^{\binom{2g}{j}} \cdot q^{\frac{2g-j}{2} \cdot \binom{2g}{j}} \cdot P_j\big(\frac{1}{q^g t}\big)\,.$$

Because $\sum_{j=0}^{2g}(-1)^{j+1}\binom{2g}{j} = 0$ and also $\sum_{j=0}^{2g}(-1)^{j+1}\frac{2g-j}{2} \cdot \binom{2g}{j} = g \cdot \sum_{j=0}^{2g-1}(-1)^{j+1}\binom{2g-1}{j} = 0$, taking the product over all j gives the relation

$$Z(X;t) = \prod_{j=0}^{2g} P_{2g-j}^{(-1)^{j+1}} = \prod_{j=0}^{2g}\Big(P_j\big(\frac{1}{q^g t}\big)\Big)^{(-1)^{j+1}} = Z\big(X;\frac{1}{q^g t}\big)\,,$$

which is the desired functional equation. □

WeilConj **(16.8)** Theorems (16.4) and (16.7) prove the Weil conjectures for abelian varieties, and in order to put these results in their proper context it is worthwile to include a brief discussion of the Weil conjectures. As this is only intended to give some background material, the reader may jump ahead to (16.12) without missing much.

In his 1949 paper Weil [4], André Weil formulated some beautiful conjectures about the zeta functions of varieties over $\mathbb{F}_q$, which have had an enormous influence on the development of abstract algebraic geometry. To state his conjectures, consider a smooth projective variety Y over $\mathbb{F}_q$ of dimension d. Let the zeta function $Z(Y;t)$ be defined as in (16.6), and let $\chi(Y)$ be the topological Euler characteristic of Y, which can be defined for instance as the self-intersection number of the diagonal $\Delta_Y \subset Y \times Y$.

Weil conjectured that the zeta function $Z(Y;t)$ is a rational function for which there is an expression

$$Z(Y;t) = \frac{P_1 P_3 \cdots P_{2d-1}}{P_0 P_2 \cdots P_{2d}}\,,$$

where the P_i are polynomials with integral coefficients that in $\mathbb{C}[t]$ can be written as $P_i = \prod_{j=1}^{b_i}(t - \alpha_{ij})$, with all roots α_{ij} of P_i algebraic integers of absolute value $|\alpha_{ij}| = q^{i/2}$. (These properties uniquely determine the polynomials P_i, if they exist.) Further Weil conjectured that $Z(Y;t)$ satisfies a functional equation

$$Z\big(Y;\frac{1}{q^d t}\big) = \pm \cdot q^{\frac{d\cdot\chi(Y)}{2}} \cdot t^{\chi(Y)} \cdot Z(Y;t)\,.$$

When Weil stated these conjectures, he could prove them for curves (Bijdrage FK Schmidt?), and not long thereafter he gave a complete proof for abelian varieties. (Historisch correct? Vergelijk met ons bewijs??). The rationality of the zeta function and the functional equation were proved by Dwork in 1960, using p-adic analysis, and later again by Grothendieck as application of the machinery of ℓ-adic cohomology that he had developped in collaboration with M. Artin, among others. The remaining assertion that all roots of P_i are algebraic integers of absolute value $q^{i/2}$ is known as the Riemann Hypothesis for varieties over finite fields and turned out to be much harder. It was proved by a beautiful combination of techniques by Deligne in 1973; see Deligne [3]. We refer to HAG, Appendix C or Katz [1] for a further introduction to the Weil conjectures and Deligne's proof.

Weil himself already realised that his conjectures could be proven once one had a sufficiently good cohomology theory, satisfying analogues of a number of properties that are known to hold for singular cohomology of smooth projective varieties over $\mathbb{C}$. See Kleiman [1] for a precise

description of the mechanism one needs. The way one uses cohomology is as follows. (We shall formulate everything using ℓ-adic cohomology.)

As already explained in (16.1), $\#Y(\mathbb{F}_{q^n})$ equals the number of fixed points of π_Y^n in $Y(\overline{\mathbb{F}}_q)$. Let $\Gamma_n \subset Y_{\overline{\mathbb{F}}_q} \times Y_{\overline{\mathbb{F}}_q}$ be the graph of π_Y^n. Because the tangent map of π_Y^n is everywhere zero, all intersections of Γ_n with the diagonal $\Delta \subset Y_{\overline{\mathbb{F}}_q} \times Y_{\overline{\mathbb{F}}_q}$ are transversal. Hence the number of fixed points of π_Y^n equals the intersection number $\Gamma_n \cdot \Delta$. By the Lefschetz trace formula, this intersection number also equals the alternating sum of traces of π_Y^n acting on the cohomology of $Y_{\overline{\mathbb{F}}_q}$; so we find that

$$\#Y(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d} (-1)^i \cdot \operatorname{trace}\bigl(\pi_Y^n, H^i(Y_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)\bigr)\,.$$

Using the identity (1) we find that if we define polynomials P_i by

$$P_i := \det\bigl(\mathrm{id} - t \cdot \pi_Y; H^i(Y_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)\bigr)\,,$$

we get the identity

$$Z(Y;t) = \prod_{i=0}^{2d} P_i^{(-1)^{i+1}} = \frac{P_0 P_2 \cdots P_{2d}}{P_1 \cdots P_{2d-1}}\,.$$

The rationality of the zeta function now follows from the fact that $\mathbb{Q}[\![t]\!] \cap \mathbb{Q}_\ell(t) = \mathbb{Q}(t)$. The functional equation for $Z(Y;t)$ follows by elementary arguments from Poincaré duality; see HAG, Appendix C, Section 4. If $d := \dim(Y)$ is odd then the sign in the functional equation is $+1$, if d is even the sign is $(-1)^N$, where N is the multiplicity of $q^{d/2}$ as an eigenvalue of π_Y acting on $H^d(Y_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$. Note that a priori the polynomials P_i are in $\mathbb{Q}_\ell[t]$; the fact that they are in $\mathbb{Z}[t]$ is part of the Riemann Hypothesis. Further note that $P_0 = 1 - t$ and $P_{2d} = 1 - q^d t$.

The proof of the Riemann Hypothesis requires deeper results than merely the existence of a Weil cohomology theory. In the years before Deligne's proof the general expectation was that the Riemann Hypothesis should be obtained as a consequence of two further properties of ℓ-adic cohomology, namely the hard (or "strong") Lefschetz Theorem and an analogue of the Hodge Index Theorem. (These are part of Grothendieck's "standard conjectures".) This, however, turned out not to be the easiest route. Deligne proved the hard Lefschetz Theorem *using* the Riemann Hypothesis, whereas the Hodge Index Theorem in this setting is at present still an open problem. See also Katz [1] and Messing [2].

Looking at our proofs of Theorems (16.4) and (16.7) we recognize that part of what we have been doing fits nicely with the general approach sketched here, where we have the advantage that we can do without any reference to ℓ-adic cohomology, using the Tate module instead. (Cf. Corollary (10.39). Note that the Tate module is the first homology, rather than cohomology.) For example, the equality between the first and third term in (i) of Theorem (16.7) is just an instance of the Lefschetz trace formula. But the most interesting part is the Riemann Hypothesis, and as sketched above, for general varieties this is far from an automatic consequence of the existence of a Weil cohomology theory. For abelian varieties, the proofs we have given ultimately boil down to results about the structure of the endomorphism algebra, and in particular the positivity of the Rosati involution. Note that for abelian varieties we do know that the Hodge Index Theorem holds (see ??) but that we do not directly use it here. Morally speaking its role is taken over by the positivity of the Rosati involution, which, like the Hodge Index Theorem, is a result about the signature of a quadratic form.

NPX/Fq **(16.9)** Let X be an abelian variety over a finite field $\mathbb{F}_q$. By () the characteristic polynomial of π_X on the rational Dieudonné module $M_{\mathbb{Q}}(X)$ equals f_X. Theorem (15.35) and its Corollary (15.36) give us a quick way to read off the Newton polygon of X from f_X. To summarize, if $\{\alpha_1, \ldots, \alpha_{2g}\}$ is the multiset of roots of f_X in $\overline{\mathbb{Q}}$ then, with conventions as in ??, we have the following information about the valuations of the α_i:

(1) If v is a prime of $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g})$ of residue characteristic $\ell \neq p$ then $\mathrm{ord}_v(\alpha_i) = 0$ for all i. This follows from the relation $\alpha_i \bar{\alpha}_i = q$ since α_i and $\bar{\alpha}_i$ are both integral.

(2) If v is a prime of K above p then the multiset $\{\mathrm{ord}_v(\alpha_1)/\mathrm{ord}_v(q), \ldots, \mathrm{ord}_v(\alpha_{2g})/\mathrm{ord}_v(q)\}$ is the (unordered) collection of slopes, counted with multiplicity, of the Newton polygon of X. This is Theorem (15.35).

(3) If v is an infinite prime of K then $\mathrm{ord}_v(\alpha_i)/\mathrm{ord}_v(q) = 1/2$ for all i. This is (i) of Theorem (16.4).

By Remark (15.38), the action of π_X on $M_{\mathbb{Q}}(X)$ actually determines the $\mathbb{F}_q$-isogeny class of the p-divisible group $X[p^\infty]$. This class carries finer information than just the Newton polygon, which only depends on $X_{\overline{\mathbb{F}}_p}$, but this additional information is more difficult to exploit. We shall come back to this in the proof of Corollary (16.30), where we determine the precise structure of the endomorphism algebra of X in terms of π_X. The hardest part in that calculation is to determine the local invariants of the endomorphism algebra at the places above p, and by a theorem of Tate (see Theorem (16.24)) this boils down to the calculation of $\mathrm{End}_{\mathsf{DM}}\big(M_{\mathbb{Q}}(X)\big)$.

§2. *The Hasse-Weil-Serre bound for curves.*

Let C be a nonsingular complete curve over a finite field $\mathbb{F}_q$. The discussion in (16.8) tells us what to expect for the zeta function of C. Namely, we should have $Z(C;t) = P_1/(1-t)(1-qt)$ where P_1 is the reciprocal characteristic polynomial of Frobenius acting on the H^1 of the curve. Further, the Riemann Hypothesis should hold and $Z(C;t)$ should satisfy a functional equation. Keeping the cohomological interpretation of the Weil conjectures in mind, it should come as no surprise that the proof of these assertions can be reduced to the Weil conjectures for the Jacobian of C. In fact, as we shall see in (16.14) below, C always has $\mathbb{F}_q$-rational points, and if we choose $P \in C(\mathbb{F}_q)$ then by ?? the map $\varphi_P\colon C \to \mathrm{Jac}(C)$ induces an isomorphism $\varphi_P^*\colon H^1(\mathrm{Jac}(C)_{\overline{\mathbb{F}}_q}, \mathbb{Z}_\ell) \xrightarrow{\sim} H^1(C_{\overline{\mathbb{F}}_q}, \mathbb{Z}_\ell)$ on cohomology in degree 1, compatible with the actions of the geometric Frobenii. So all the relevant information should be contained in the Tate module of the Jacobian with its action of the geometric Frobenius. To turn this philosophy into a solid theorem we first prove a special case of the Lefschetz trace formula, in terms of the Tate module of the Jacobian.

LefTraceCurve **(16.10) Proposition.** *Let C be a nonsingular complete curve over a finite field $\mathbb{F}_q$. Let $J := \mathrm{Jac}(C)$ be its Jacobian, and let $\{\alpha_1, \ldots, \alpha_{2g}\}$ be the complex roots of the polynomial f_J. Then for every positive integer n we have*

$$\#C(\mathbb{F}_{q^n}) = 1 - \mathrm{trace}(\pi_J^n) + q^n = 1 - \sum_{i=1}^{2g} \alpha_i^n + q^n\,.$$

Proof. It suffices to prove this for $n = 1$, as the assertion for arbitrary n then follows by considering $C \otimes \mathbb{F}_{q^n}$. As already explained in (16.8) we have $\#C(\mathbb{F}_q) = \Delta_C \cdot \Gamma$, where $\Gamma \subset C \times C$

is the graph of the geometric Frobenius π_C. To prove the identity $\Delta_C \cdot \Gamma = 1 - \mathrm{trace}(\pi_J) + q$ we may work over $k := \overline{\mathbb{F}}_q$. Choose a point $P \in C(k)$ and let $\alpha\colon C \to J$ be the map given on points by $Q \mapsto [Q - P]$. [NOG AFMAKEN - bewijs v Gerard is niet goed]

WeilCCurve **(16.11) Theorem.** *Let C be a nonsingular complete curve of genus g over a finite field $\mathbb{F}_q$, and let $J := \mathrm{Jac}(C)$ be its Jacobian. Let $\{\alpha_1, \ldots, \alpha_{2g}\}$ be the multiset of complex roots of the characteristic polynomial f_J of the geometric Frobenius of J. Let $P_0 := 1 - t$ and $P_2 := 1 - qt$, and let $P_1 := \prod_{i=1}^{2g}(1 - \alpha_i \cdot t)$ be the reciprocal of the polynomial f_J. Then we have*

$$Z(C;t) = \frac{P_1}{P_0 P_2} = \frac{P_1}{(1-t)(1-qt)}\,.$$

All complex roots of the polynomial P_i are algebraic integers of absolute value $q^{i/2}$. Further, $Z(C;t)$ satisfies the functional equation

$$Z(C;t) = q^{g-1} \cdot t^{2g-2} \cdot Z\big(C; \frac{1}{qt}\big)\,.$$

Proof. The identity $Z(C;t) = P_1/P_0P_2$ readily follows from Proposition (16.10) together with identity (1). The assertion about the roots of the polynomials P_i is obvious for $i = 0$ and $i = 2$, and for $i = 1$ it is just (i) of Theorem (16.4). For the functional equation, note that by (ii) of Theorem (16.4) there is an involution $\iota \in \mathfrak{S}_{2g}$ such that $\alpha_{\iota(i)} = \bar{\alpha}_i = q/\alpha_i$ for all i. We then have

$$\begin{aligned} P_1 = \prod_{i=1}^{2g}\big(\alpha_{\iota(i)} \cdot t - 1\big) &= \prod_{j=1}^{2g} \alpha_j \cdot t^{2g} \cdot \prod_{i=1}^{2g}\big(1 - \frac{1}{\alpha_{\iota(i)} \cdot t}\big) \\ &= q^g \cdot t^{2g} \cdot \prod_{i=1}^{2g}\big(1 - \frac{\alpha_i}{qt}\big) = q^g \cdot t^{2g} \cdot P_1\big(\frac{1}{qt}\big)\,. \end{aligned}$$

As $P_0P_2 = q \cdot t \cdot P_0\big(\frac{1}{qt}\big)P_2\big(\frac{1}{qt}\big)$ we obtain the functional equation. □

We note that the zeta function of C can also be written as

$$Z_C(t) = \sum_{n=0}^{\infty} D_n t^n\,,$$

where D_n is the number of effective divisors of degree n on C that are defined over $\mathbb{F}_q$, see Exercise 16.1.

By Proposition (16.10), to count the number of $\mathbb{F}_q$-rational points of C, it suffices to know $\mathrm{trace}(\pi_J) = \sum_{i=1}^{2g} \alpha_i$, which is minus the coefficient of t^{2g-1} in f_J. Because all α_i have absoulte value $\sqrt{q}$ we have the estimate $|\mathrm{trace}(\pi_J)| \leqslant \lfloor 2g\sqrt{q} \rfloor$ (the Hasse-Weil bound). Serre showed that one can improve this a bit, as follows.

SerreHW **(16.12) Theorem.** *Let X be an abelian variety of dimension g over $\mathbb{F}_q$. Then* $\mathrm{trace}(\pi_X)$ *satisfies*

AVFF:HWSineq
$$|\mathrm{trace}(\pi_X)| \leqslant g \cdot \lfloor 2\sqrt{q} \rfloor\,. \tag{2}$$

This is an equality if and only if either $\alpha_i + \bar{\alpha}_i = \lfloor 2\sqrt{q} \rfloor$ for all i or $\alpha_i + \bar{\alpha}_i = -\lfloor 2\sqrt{q} \rfloor$ for all i.

Proof. We number the complex roots of f_X such that $\alpha_{g+i} = \bar{\alpha}_i$ for $i = 1, \ldots, g$. Write $a_i = \alpha_i + \bar{\alpha}_i$. These are real numbers with $|a_i| < \lfloor 2\sqrt{q} \rfloor + 1$. Hence the numbers $b_i := \lfloor 2\sqrt{q} \rfloor + 1 + a_i$ are positive algebraic integers. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ naturally acts on the multiset $\{b_1, \ldots, b_g\}$. It follows that the product $b_1 \cdots b_g$ is an element of $\mathbb{Z}_{>0}$. Now we use the arithmetic-geometric mean inequality

$$\frac{b_1 + \cdots + b_g}{g} \geqslant (b_1 \cdots b_g)^{1/g},$$

with equality if and only if all b_i are equal. So $\lfloor 2\sqrt{q} \rfloor + 1 + \sum_{i=1}^{g} a_i/g \geqslant 1$, i.e., $\mathrm{trace}(\pi_X) = \sum_{i=1}^{g} a_i \geqslant -g \cdot \lfloor 2\sqrt{q} \rfloor$. Repeating the same argument for $-\pi_X$ gives the estimate $\mathrm{trace}(\pi_X) \leqslant g \cdot \lfloor 2\sqrt{q} \rfloor$. If we have equality in (2) then all a_i are equal, and this readily gives the last assertion. □

Applying this to the Jacobian $\mathrm{Jac}(C)$ gives the following bound on the number of rational points on a curve.

HWSbound **(16.13) Corollary.** (Hasse-Weil-Serre) *Let C be a complete nonsingular curve over $\mathbb{F}_q$. Then for the number of $\mathbb{F}_q$-rational points of C we have the inequalities*

$$q + 1 - g\lfloor 2\sqrt{q} \rfloor \leqslant \#C(\mathbb{F}_q) \leqslant q + 1 + g\lfloor 2\sqrt{q} \rfloor .$$

Note that in order to determine the g roots α_i of $f_{\mathrm{Jac}(C)}$ it suffices to calculate $\#C(\mathbb{F}_{q^i})$ for $i = 1, \ldots, g$. We give some examples.

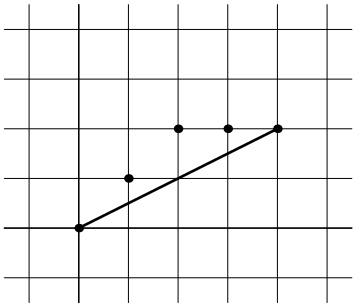
ZetaExa **(16.14) Examples.** (1) If C is a complete nonsingular curve of genus g over $\mathbb{F}_q$ then $\#C(\mathbb{F}_q) \geqslant q + 1 - 2\sqrt{q} = \left(\sqrt{q} - 1\right)^2 > 0$, so C has an $\mathbb{F}_q$-rational point.

In particular, a curve of genus 1 over $\mathbb{F}_q$ always has an $\mathbb{F}_q$-rational point and, taking such a point as the origin, can be given the structure of an elliptic curve.

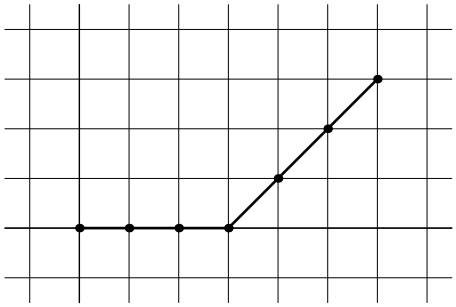
(2) Consider the complete nonsingular curve C of genus 2 over $\mathbb{F}_2$ with affine equation $y^2 + y = x^5 + x^2 + 1$. We easily find by explicit computation $\#C(\mathbb{F}_2) = 1$ and $\#C(\mathbb{F}_4) = 9$. Using the identities $\sum \alpha_i^n = 2^n + 1 - \#C(\mathbb{F}_{2^n})$ and $\alpha_i \bar{\alpha}_i = 2$ we find for $J := \mathrm{Jac}(C)$ the characteristic polynomial $f_J = t^4 - 2t^3 + 4t^2 - 4t + 4$. We have $\#J(\mathbb{F}_2) = f_J(1) = 3$ and this fits, since there are three $\mathbb{F}_2$-rational divisors of degree 2 on C.

In a similar fashion, the genus 3 curve D over $\mathbb{F}_2$ given by the affine equation $y^2 + y = (x^4 + x^2 + 1)/(x^4 + x^3 + x^2 + x + 1)$ has no points over $\mathbb{F}_2$, has 10 rational points over $\mathbb{F}_4$ (the maximum possible for a hyperelliptic curve over $\mathbb{F}_4$), and 6 points over $\mathbb{F}_8$; hence the characteristic polynomial of its Jacobian is $t^6 - 3t^5 + 7t^4 - 13t^3 + 14t^2 - 12t + 8$.

Applying Corollary (15.36) we find that the curve C is supersingular and that D is ordinary.



NP(C)



NP(D)

(The dots represent the points $\big(i, \mathrm{ord}_p(c_{2g-i})\big)$, where the c_i are the coefficients of the characteristic polynomial.)

(3) Let $r = p^m$ and $q = r^2 = p^{2m}$. Let $a \in \mathbb{F}_q$ be a non-zero element satisfying $a^r + a = 0$. Then the complete nonsingular curve with affine equation $y^p - y = ax^{r+1}$ has genus $g = (p-1)r/2$ and has $1 + pq = 1 + p^{2m+1}$ rational points over $\mathbb{F}_q$. Note that $1 + p^{2m+1} = q + 1 + 2g\sqrt{q}$, so these curves attain the Hasse-Weil bound $q + 1 + 2g\sqrt{q}$. This shows that the Hasse-Weil bound is sharp for certain g and q. It is not sharp if g is large with respect to q, see Exercise 16.2.

(4) Let $C \subset \mathbb{P}^2$ be the nonsingular quartic curve over $\mathbb{F}_2$ given by the homogeneous equation $X^3Y + Y^3Z + Z^3X = 0$, also known as the Klein curve. The genus of C is 3 and one easily checks that $\#C(\mathbb{F}_2) = 3$, that $\#C(\mathbb{F}_4) = 5$, and $\#C(\mathbb{F}_8) = 24$. The characteristic polynomial of Frobenius is $f_J = t^6 + 5t^3 + 8$ and C is ordinary. This curve reaches the Serre bound $q + 1 + g\lfloor 2\sqrt{q} \rfloor$ over $\mathbb{F}_8$. Note that in this case Serre's bound is better than the original Hasse-Weil bound: $8 + 1 + 3\lfloor 2\sqrt{8} \rfloor = 24$, whereas $8 + 1 + \lfloor 6\sqrt{8} \rfloor = 25$.

(5) Consider the Jacobian $J_0(103)$ of the modular curve $X_0(103)$. The curve $X_0(103)$ has genus 8 and has an (Atkin-Lehner) involution w. The Jacobian splits, up to isogeny, as a product of two abelian varieties, J_+ and J_-, with $J_\pm = \mathrm{Im}\big(w \pm \mathrm{id}_{J_0(103)}\big)$, the + and − part of w, of dimensions 2 and 6, respectively. The minus part J_- is attached to a normalized cusp form f of weight 2 on the congruence subgroup $\Gamma_0(103)$, an eigenform for the Hecke operators. It has a Fourier expansion $f = \sum_{n=1}^{\infty} a(n)q^n$ with the coefficients $a(n)$ that are algebraic integers in a totally real number field K of degree 6 over $\mathbb{Q}$ and normalized such that $a(1) = 1$. The trace of Frobenius acting on the Tate module T_ℓ of $J_- \otimes \mathbb{F}_p$ for $p \neq 103$ and $\ell \neq p$ is given by the Fourier coefficient $b(p)$ of the form $\mathrm{trace}(f) = \sum_{n=1}^{\infty} b(n)q^n = \sum_{\sigma\colon K \to \mathbb{R}} \sum_{n=1}^{\infty} \sigma\big(a(n)\big)q^n$. This form has Fourier series starting

$$6\,q + 4\,q^2 + 6\,q^4 + 3\,q^5 - 3\,q^6 - 2\,q^7 + 9\,q^8 + 8\,q^9 - 10\,q^{10} - q^{11} - 13\,q^{12} \\ - q^{13} - 9\,q^{14} - 9\,q^{15} + 2\,q^{16} + 21\,q^{17} - 3\,q^{18} + \cdots$$

We observe that for $p = 2$ (resp. $p = 17$) the expression $p + 1 - b(p)$ equals -1 (resp. -3). Therefore, $J_- \otimes \mathbb{F}_2$ and $J_- \otimes \mathbb{F}_{17}$ cannot be (isogenous to) a Jacobian since then the corresponding curve would have a negative number of $\mathbb{F}_2$-rational (resp. $\mathbb{F}_{17}$-rational) points. (Note that isogenous abelian varieties have the same zeta function; see Corollary (16.25).)

§3. *The theorem of Tate.*

The topic of this section is an important theorem of Tate, asserting that for abelian varieties X and Y over a finite field k and any prime number $\ell \neq \mathrm{char}(k)$ the natural map

AVFF:HomHom
$$\mathbb{Z}_\ell \otimes \mathrm{Hom}_{\mathsf{AV}}(X, Y) \to \mathrm{Hom}_{\mathrm{Gal}(\overline{k}/k)}(T_\ell X, T_\ell Y) \tag{3}$$

is an isomorphism. Here the RHS of (3) denotes the group of $\mathbb{Z}_\ell$-linear maps $T_\ell X \to T_\ell Y$ that are equivariant with respect to the natural Galois actions on the two terms. Equivalently, these are the homomorphisms of $\mathbb{Z}_\ell\big[\mathrm{Gal}(\overline{k}/k)\big]$-modules, or also the $\mathrm{Gal}(\overline{k}/k)$-invariant elements in $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y) = (T_\ell X)^\vee \otimes_{\mathbb{Z}_\ell} T_\ell Y$; therefore the RHS of (3) is also sometimes denoted by $\mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Gal}(\overline{k}/k)]}(T_\ell X, T_\ell Y)$ or $\mathrm{Hom}(T_\ell X, T_\ell Y)^{\mathrm{Gal}(\overline{k}/k)}$.

Tate's theorem should be seen as an analogue of ??, with Galois representations taking over the role of Hodge structures. There are other types of ground fields for which the analogue of

Tate's theorem is true. Zarhin proved that it is true for function field over finite fields; later Faltings, in his spectacular 1983 breakthrough, proved that the map (3) is an isomorphism for abelian varieties over any field k that is finitely generated over its prime field (e.g., number fields). At the same time, there are also types of ground fields for which we cannot hope to have such a result. E.g., if $k = \overline{k}$ or also if k is a local field then (3) is not, in general, surjective. We shall further discuss Faltings's results in ??.

Over the years the proof that Tate gave has been improved, mainly by Zarhin, and there are several steps in the proof that work over an arbitrary field. We shall state and prove results in a general setting. The assumption that we work over a finite field will enter only in Proposition (16.19), from which Tate's Theorem (16.20) follows by some general results. Still, there is one aspect that is special to the case of a finite ground field. Namely, if k is a finite field, say of cardinality $q = p^m$, then the action of $\mathrm{Gal}(\overline{k}/k)$ on $T_\ell X$ is completely determined by the single automorphism $T_\ell(\pi_X)$. (Note that $T_\ell(\pi_X)$ is indeed an automorphism for any $\ell \neq p$.) The reason for this is that $\mathrm{Gal}(\overline{k}/k)$ is isomorphic, as a topological group, to $\widehat{\mathbb{Z}}$, the pro-finite completion of $\mathbb{Z}$, and is topologically generated by the element $\varphi \in \mathrm{Gal}(\overline{k}/k)$ given by $\varphi(x) = x^q$. Furthermore, φ acts on $T_\ell X$ as the automorphism $T_\ell(\pi_X)$, since φ and π_X both give the action "raising all coordinates to the power q" on $X(\overline{k})$. Hence the elements of $\mathrm{Hom}_{\mathrm{Gal}(\overline{k}/k)}(T_\ell X, T_\ell Y)$ are also the $\mathbb{Z}_\ell$-linear maps $f\colon T_\ell X \to T_\ell Y$ for which $T_\ell(\pi_Y) \circ f = f \circ T_\ell(\pi_X)$. As in our proof of Tate's theorem we focus on general arguments, this aspect will not play a role there, but once we pass to applications it is again the geometric Frobenius endomorphism that plays a key role.

TateZlQl **(16.15) Lemma.** *Let k be a field, k_s a separable closure, and let ℓ be a prime number different from* $\mathrm{char}(k)$.

(i) *If X and Y are abelian varieties over k then the map*

$$T_\ell\colon \mathbb{Z}_\ell \otimes \mathrm{Hom}_{\mathsf{AV}}(X,Y) \to \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y)$$

is an isomorphism if and only if the map

AVFF:HomHomQl
$$V_\ell\colon \mathbb{Q}_\ell \otimes \mathrm{Hom}_{\mathsf{AV}}(X,Y) \to \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(V_\ell X, V_\ell Y) \tag{4}$$

is an isomorphism.

(ii) *Assume that for every abelian variety Z over k the map*

$$\mathbb{Q}_\ell \otimes \mathrm{End}_{\mathsf{AV}}(Z) \to \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell Z)$$

is an isomorphism. Then also for any two abelian varieties X and Y over k the map (4) *is an isomorphism.*

Proof. (i) By Theorem (12.10) the map T_ℓ is injective and $\mathrm{Coker}(T_\ell)$ is torsion-free (hence free). Hence T_ℓ is an isomorphism if and only if $\mathbb{Q}_\ell \otimes \mathrm{Coker}(T_\ell) = 0$. Now use that $\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$, so the map V_ℓ is again injective and $\mathrm{Coker}(V_\ell) = \mathbb{Q}_\ell \otimes \mathrm{Coker}(T_\ell)$.

(ii) Take $Z := X \times Y$. We have a decomposition of vector spaces

$$\mathrm{End}^0(Z) = \mathrm{End}^0(X) \oplus \mathrm{Hom}^0(X,Y) \oplus \mathrm{Hom}^0(Y,X) \oplus \mathrm{End}^0(Y)\,.$$

Likewise we have, writing $\Gamma := \mathrm{Gal}(k_s/k)$, a decomposition

$$\mathrm{End}_\Gamma(V_\ell Z) = \mathrm{End}_\Gamma(V_\ell X) \oplus \mathrm{Hom}_\Gamma(V_\ell X, V_\ell Y) \oplus \mathrm{Hom}_\Gamma(V_\ell Y, V_\ell X) \oplus \mathrm{End}_\Gamma(V_\ell Y)\,.$$

The map $V_{\ell,Z}\colon \mathbb{Q}_\ell \otimes \mathrm{End}(Z) \to \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell Z)$ respects these decompositions. In particular it follows that if $V_{\ell,Z}$ is an isomorphism then so is the map $\mathbb{Q}_\ell \otimes \mathrm{Hom}_{\mathsf{AV}}(X,Y) \to \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(V_\ell X, V_\ell Y)$. □

FinitenessI **(16.16)** As fuel for Tate's theorem we need a finiteness property for the number of isomorphism classes within a given isogeny class. We shall state it here in an axiomatic form. Given a field k, an abelian variety X over k, and a prime number $\ell \neq \mathrm{char}(k)$, consider the condition

$$\mathrm{Fin}(X/k,\ell)\colon \qquad \begin{array}{c}\text{up to isomorphism there are finitely many abelian varieties } Y \text{ over } k\\ \text{for which there is an isogeny } X \to Y \text{ of degree a power of } \ell.\end{array}$$

This finiteness property is used in an essential way in the following lemma. Once we have this lemma the proof of Tate's Theorem will be easy. For brevity we shall write $\mathbb{Q}_\ell\mathrm{End}(X)$ for $\mathbb{Q}_\ell \otimes \mathrm{End}(X)$, and we view it as a subalgebra of $\mathrm{End}(V_\ell X)$. For $u \in \mathbb{Q}_\ell\mathrm{End}(X)$ we shall write $u \cdot V_\ell X$ instead of $V_\ell(u)\big(V_\ell X\big)$.

FinIuV=W **(16.17) Lemma.** *Let X an abelian variety over a field k, and let ℓ be a prime number different from* $\mathrm{char}(k)$. *Assume that condition* $\mathrm{Fin}(X/k,\ell)$ *holds. Then for every $\mathbb{Q}_\ell$-subspace $W \subset V_\ell X$ that is stable under the action of* $\mathrm{Gal}(k_s/k)$ *there exists an element $u \in \mathbb{Q}_\ell\mathrm{End}(X)$ such that $W = u \cdot V_\ell X$.*

Proof. For $n \in \mathbb{Z}_{\geqslant 0}$ define $U_n := (W \cap T_\ell X) + \ell^n \cdot T_\ell X$, which is a Galois-stable lattice in $V_\ell X$ with $\ell^n \cdot T_\ell X \subset U_n \subset T_\ell X$. Let $\mathscr{K}_n \subset X[\ell^n]\big(k_s\big) = T_\ell X/\ell^n T_\ell X$ be the image of U_n. Then $\mathscr{K}_n$ is stable under the action of $\mathrm{Gal}(k_s/k)$ on $X[\ell^n]\big(k_s\big)$, and using Proposition (3.26) it follows that $\mathscr{K}_n = K_n(k_s)$ for some subgroup scheme $K_n \subset X[\ell^n]$. Let $\pi_n\colon X \to Y_n := X/K_n$ be the quotient, and let $\iota_n\colon Y_n \to X$ be the unique isogeny such that $\iota_n \circ \pi_n = [\ell^n]_X$. Using Proposition (10.6) we find that $T_\ell Y \cong U_n$ as $\mathbb{Z}_\ell$-modules with Galois action; taking this as an identification $T_\ell(\pi_n)\colon T_\ell X \to T_\ell Y = U_n$ is the map induced by multiplication by ℓ^n on $T_\ell X$ and $T_\ell(\iota_n)\colon U_n = T_\ell Y \to T_\ell X$ is the inclusion map.

Assumption $\mathrm{Fin}(X/k,\ell)$ implies that we can find a sequence $n = n_1 < n_2 < \cdots$ such that we have isomorphisms $\alpha_i\colon Y_n \xrightarrow{\sim} Y_{n_i}$. Define $u_i := \iota_{n_i} \circ \alpha_i \circ q_n$, which is an endomorphism of X. The induced map $T_\ell(u_i)$ is the composition

$$T_\ell X \xrightarrow{\cdot \ell^n} U_n \xrightarrow{T_\ell \alpha_i} U_{n_i} \hookrightarrow T_\ell X\,.$$

Because $\mathbb{Z}_\ell\mathrm{End}(X)$ $(:= \mathbb{Z}_\ell \otimes \mathrm{End}(X))$ is a free $\mathbb{Z}_\ell$-module of finite rank, it is compact for the ℓ-adic topology. Hence possibly after replacing the sequence of integers n_i by a subsequence, the elements u_i converge ℓ-adically to an element $u \in \mathbb{Z}_\ell\mathrm{End}(X)$. As $U_{n_1} \supset U_{n_2} \supset \cdots$ the endomorphism $T_\ell(u)$ maps $T_\ell X$ to $\big(\cap_{i\geqslant 1} U_{n_i}\big) = W \cap T_\ell X$. On the other hand, we claim that the image of $T_\ell(u)\colon T_\ell X \to (W \cap T_\ell X)$ contains $\ell^n \cdot (W \cap T_\ell X)$. To see this note that an element $x \in W \cap T_\ell X$ lies in U_{n_i} for every i, so it follows from the given description of $T_\ell(u_i)$ that $\ell^n \cdot x$ lies in the image of $T_\ell(u_i)$ for every i. Hence $\ell^n \cdot x$ can be approximated arbitrarily closely by an element in the image of $T_\ell(u)$; but this image is closed so $\ell^n \cdot x$ actually lies in $\mathrm{Im}\big(T_\ell(u)\big)$. Now pass to $\mathbb{Q}_\ell$-coefficients and note that $\mathbb{Q}_\ell \cdot (W \cap T_\ell X) = \mathbb{Q}_\ell \cdot \big(\ell^n \cdot (W \cap T_\ell X)\big) = W$; it follows that the image of $V_\ell(u)$ is precisely W. □

FinItoTate **(16.18) Theorem.** *Let X an abelian variety over a field k, and let ℓ be a prime number different from* $\mathrm{char}(k)$. *Assume that* $\mathrm{Fin}(X/k,\ell)$ *and* $\mathrm{Fin}(X^2/k,\ell)$ *are true. Then the representation*

$$\rho_\ell\colon \mathrm{Gal}(k_s/k) \to \mathrm{GL}(V_\ell X)$$

is semisimple and the map

$$\mathbb{Q}_\ell \otimes \mathrm{End}_{\mathsf{AV}}(X) \to \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell X)$$

is an isomorphism.

Proof. To prove that ρ_ℓ is a semisimple representation, suppose we have a Galois-stable subspace $W \subset V_\ell X$. As just shown, there exists an element $u \in \mathbb{Q}_\ell\mathrm{End}(X)$ with $W = u \cdot V_\ell X$. Because $\mathbb{Q}_\ell\mathrm{End}(X)$ is semisimple the right ideal $u \cdot \mathbb{Q}_\ell\mathrm{End}(X)$ is generated by an idempotent e. Write $u = e \cdot a$ and $e = u \cdot b$ for some a, $b \in \mathbb{Q}_\ell\mathrm{End}(X)$; this gives $u \cdot V_\ell X = e \cdot (a \cdot V_\ell X) \subseteq e \cdot V_\ell X = u \cdot (b \cdot V_\ell X) \subseteq u \cdot V_\ell X$. Hence $W = e \cdot V_\ell X$. Then $W' := (1-e) \cdot V_\ell X$ is a complement for W, and W' is again Galois-stable because $\rho_\ell(g)$ commutes with $(1-e)$ for every $g \in \mathrm{Gal}(k_s/k)$. This proves that ρ_ℓ is semisimple.

We already know from Theorem (12.10) that the map $\mathbb{Q}_\ell\mathrm{End}(X) \to \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell X)$ is injective. If $C = \mathrm{End}_{\mathbb{Q}_\ell\mathrm{End}(X)}(V_\ell X)$ then the Bicommutant Theorem (A.2) tells us that $\mathbb{Q}_\ell\mathrm{End}(X) = \mathrm{End}_C(V_\ell X)$. Hence it suffices to show that for every $\varphi \in \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell X)$ and $c \in C$ we have $\varphi c = c\varphi$. The graph $\Gamma_\varphi \subset V_\ell X \oplus V_\ell X$ is a Galois-stable subspace. Applying Lemma (16.17) to X^2 it follows that there exists an element $u \in \mathbb{Q}_\ell\mathrm{End}(X^2) = M_2\big(\mathbb{Q}_\ell\mathrm{End}(X)\big)$ such that $\Gamma_\varphi = u \cdot V_\ell X^2$. But $\gamma := \left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) \in M_2\big(\mathbb{Q}_\ell\mathrm{End}(X)\big)$ commutes with u, so $\gamma \cdot \Gamma_\varphi = \gamma \cdot u \cdot V_\ell X^2 = u \cdot \gamma \cdot V_\ell X^2 \subseteq \Gamma_\varphi$. This means precisely that for every $v \in V_\ell X$ we have $c \cdot \varphi(v) = \varphi(c \cdot v)$; hence $\varphi c = c\varphi$ and the theorem is proved. □

By the Bicommutant Theorem it follows that $\mathbb{Q}_\ell\big[\mathrm{Im}(\rho_\ell)\big]$, the $\mathbb{Q}_\ell$-subalgebra of $\mathrm{End}(V_\ell X)$ generated by the image of ρ_ℓ, is the commutant of $\mathbb{Q}_\ell \otimes \mathrm{End}(X)$. It is much more difficult, in general, to determine the image of the representation ρ_ℓ as a subgroup of $\mathrm{GL}(V_\ell X)$, or even to determine the algebraic envelope of this image. See ???

Now we prove the finiteness condition $\mathrm{Fin}(X/k, \ell)$ for abelian varieties over a finite field. In fact, this is relatively easy and we obtain something quite a bit stronger.

FinitenessFq **(16.19) Proposition.** *Let $q = p^m$ be a prime power. Given an integer $g \geqslant 0$ there are only finitely many isomorphism classes of abelian varieties of dimension g over $\mathbb{F}_q$.*

Proof. If X is an abelian variety of dimension g over $\mathbb{F}_q$ then $Y := X^4 \times (X^t)^4$ has dimension $8g$ and by Zarhin's Trick (11.29) Y admits a principal polarization. By Theorem (??), up to isomorphism there are finitely many abelian varieties over $\mathbb{F}_q$ that can be embedded as an abelian subvariety of Y, and X is one of them. Hence it suffices to show that, given $h \geqslant 0$, there are (up to isomorphism) finitely many abelian varieties Y over $\mathbb{F}_q$ of dimension h such that Y admits a principal polarization. Moreover, by Proposition (1.14) the isomorphism class of Y as an abelian variety only depends on the isomorphism class of Y as a variety.

If (Y, μ) is a principally polarized abelian variety then $L := (\mathrm{id}, \mu)^* \mathscr{P}_Y$ is an ample line bundle on Y and by ??? L^3 is very ample. Let $N := 6^h - 1$. Choosing an $\mathbb{F}_q$-basis of $H^0(Y, L^3)$, which has dimension $6^h = N + 1$, we obtain a closed embedding $\iota\colon X \hookrightarrow \mathbb{P}^N$ with Hilbert polynomial $\Phi = 6^h \cdot t^h$. Hence Y, viewed as a closed subscheme of $\mathbb{P}^N$ via ι, gives an $\mathbb{F}_q$-valued point of the Hilbert scheme $\mathrm{Hilb}_\Phi(\mathbb{P}^N)$. But $\mathrm{Hilb}_\Phi(\mathbb{P}^N)$ is a scheme of finite type over $\mathbb{Z}$ (see FGA, n° 221 or ??), so it has finitely many $\mathbb{F}_q$-rational points. So there are only finitely many varieties Y of dimension h that admit the structure of an abelian variety with a principal polarization, and as explained this implies the proposition. □

Combining Theorem (16.18) and Proposition (16.19), we obtain the Theorem of Tate.

TateThm **(16.20) Theorem.** *Let k be a finite field. Let ℓ be a prime number with $\ell \neq \mathrm{char}(k)$.*

(i) *For any abelian variety X over k the representation*

$$\rho_\ell = \rho_{\ell,X} \colon \mathrm{Gal}(k_s/k) \to \mathrm{GL}(V_\ell X)$$

is semisimple.

(ii) *For any two abelian varieties X and Y over k the map*

$$\mathbb{Z}_\ell \otimes \mathrm{Hom}_{\mathsf{AV}}(X,Y) \to \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y)$$

is an isomorphism.

TateThmRem **(16.21) Remark.** Let us again note that

$$\mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y) = \left\{ h \in \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y) \;\middle|\; T_\ell(\pi_Y) \circ h = h \circ T_\ell(\pi_X) \right\},$$

and similarly with $\mathbb{Q}_\ell$-coefficients. The reason is that $\mathrm{Gal}(k_s/k)$ is isomorphic to $\widehat{\mathbb{Z}}$ and is topologically generated by the element $\varphi \in \mathrm{Gal}(\overline{k}/k)$ given by $\varphi(x) = x^q$; furthermore, for any abelian variety X over $\mathbb{F}_q$ we have $\rho_{\ell,X}(\varphi) = T_\ell(\pi_X)$. If $h \colon T_\ell X \to T_\ell Y$ is a $\mathbb{Z}_\ell$-linear map then $G_h := \left\{ \gamma \in \mathrm{Gal}(k_s/k) \;\middle|\; \rho_{\ell,Y}(\gamma) \circ h = h \circ \rho_{\ell,X}(\gamma) \right\}$ is a closed subgroup of $\mathrm{Gal}(k_s/k)$, so if $T_\ell(\pi_Y) \circ h = h \circ T_\ell(\pi_X)$ then this means that $\varphi \in G_h$; but because the subgroup generated by φ is dense in $\mathrm{Gal}(k_s/k)$ this implies that $G_h = \mathrm{Gal}(k_s/k)$.

With the same argument we also see that $V_\ell X$ is still semisimple as a representation of $\langle \varphi \rangle \subset \mathrm{Gal}(\overline{k}/k)$, as the two groups give the same collection of stable subspaces. The subalgebra $\mathbb{Q}_\ell\big[\mathrm{Im}(\rho_\ell)\big] \subset \mathrm{End}(V_\ell X)$ generated by the image of $\rho_{\ell,X}$ equals $\mathbb{Q}_\ell[\pi_X]$; see also Exercise (16.4).

If X and Y are abelian varieties over $\mathbb{F}_q$ the rank of $\mathrm{Hom}(X,Y)$ can easily be computed from the characteristic polynomials f_X and f_Y. This is based on the following general result.

rffprime **(16.22) Lemma.** *Let K be a field.*

(i) *Given polynomials $f_1,\ f_2 \in K[t]$, define*

$$r(f_1,f_2) = r_K(f_1,f_2) := \sum_P \mathrm{mult}_P(f_1) \cdot \mathrm{mult}_P(f_2) \cdot \deg(P)\,,$$

where P runs over all monic irreducible polynomials in $K[t]$ and where $\mathrm{mult}_P(f_i)$ denotes the multiplicity of P as an irreducible factor of f_i. Then $r(f_1,f_2)$ is independent of the field in which we compute it, i.e., for any field extension $K \subset L$ we have $r_K(f_1,f_2) = r_L(f_1,f_2)$.

(ii) *Let V_1 and V_2 be finite dimensional K-vector spaces, and let $\pi_i \in \mathrm{End}_K(V_i)$ be a semisimple endomorphism of V_i. We give V_i the structure of a $K[t]$-module by setting $t \cdot v := \pi_i(v)$. Consider the K-vector space*

$$\mathrm{Hom}_{K[t]}(V_1,V_2) = \left\{ h \in \mathrm{Hom}_K(V_1,V_2) \;\middle|\; \pi_2 \circ h = h \circ \pi_1 \right\}.$$

If f_i is the characteristic polynomial of π_i then we have $\dim_K\big(\mathrm{Hom}_{K[t]}(V_1,V_2)\big) = r(f_1,f_2)$.

Proof. Consider the situation as in (ii). Define $W_i := \oplus_P \big(K[t]/(P)\big)^{\mathrm{mult}_P(f_i)}$, where again P runs over all monic irreducible polynomials in $K[t]$. The assumption that the π_i are semisimple implies that $V_i \cong W_i$ as $K[t]$-modules. If P and P' are monic irreducible polynomials in $K[t]$ with $P \neq P'$ then it is easily seen that $\mathrm{Hom}_{K[t]}\big(K[t]/(P), K[t]/(P')\big) = 0$. On the other hand, $K(P) :=$

$K[t]/(P)$ is a finite field extension of K and $\mathrm{End}_{K[t]}\big(K[t]/(P)\big) = \mathrm{End}_{K(P)}\big(K(P)\big) \cong K(P)$, which has K-dimension equal to $\deg(P)$. From this (ii) readily follows. For (i), consider the modules $V_i := \oplus_P \big(K[t]/(P)\big)^{\mathrm{mult}_P(f_i)}$, and note that $\mathrm{Hom}_{L[t]}(V_{1,L}, V_{2,L}) = L \otimes_K \mathrm{Hom}_{K[t]}(V_1, V_2)$. Applying (ii) twice (once over K, once over L) gives that $r_K(f_1, f_2) = r_L(f_1, f_2)$. □

Note that we can also calculate $r(f_1, f_2)$ over any subfield of K that contains all coefficients of f_1 and f_2. The actual calculation of $r(f_1, f_2)$ will of course depend on the field, but the number that comes out does not.

RkHom **(16.23) Corollary.** *Let X and Y be abelian varieties over $\mathbb{F}_q$, with characteristic polynomials f_X and f_Y, respectively. Define $r(f_X, f_Y)$ as above. Then* $\mathrm{Hom}(X, Y)$ *has rank $r(f_X, f_Y)$.*

Proof. By Tate's Theorem (16.20) the rank of $\mathrm{Hom}(X, Y)$ equals the $\mathbb{Q}_\ell$-dimension of the space $\big\{h\colon V_\ell X \to V_\ell Y \;\big|\; V_\ell(\pi_Y)\circ h = h \circ V_\ell(\pi_X)\big\}$. Now apply (ii) of the Lemma. □

Our next goal is to prove a p-adic version of Tate's Theorem. As discussed in Chapter 10 the p-adic analogue of the Tate-ℓ-module of X is the p-divisible group $X[p^\infty]$. The proof of Theorem (16.20) that we have given does not immediately carry over to the p-adic context. The main obstacle lies in the fact that $X[p^\infty]$ is not simply a vector space with some additional structure, which makes it difficult to apply the results from Algebra that we used in the proof of Theorem (16.18). To overcome this we can use Dieudonné theory. By ?? we know that for an abelian variety X over a finite field $\mathbb{F}_q$, the characteristic polynomial of π_X acting on the Dieudonné module $M(X)$ is equal to f_X. This already gives enough information to deduce the p-adic Tate Theorem from the ℓ-adic results by a simple dimension count, as follows.

pTateThm **(16.24) Theorem.** *Let X and Y be abelian varieties over a finite field k of characteristic p. Then the map*

$$\Phi\colon \mathbb{Z}_p \otimes \mathrm{Hom}_{\mathsf{AV}}(X, Y) \to \mathrm{Hom}_{\mathsf{BT}}\big(X[p^\infty], Y[p^\infty]\big)$$

is an isomorphism.

Proof. By exactly the same argument as in the proof of Lemma (16.15), it suffices to show that the map $\mathbb{Q}_p\mathrm{Hom}(X, Y) \to \mathrm{Hom}^0\big(X[p^\infty], Y[p^\infty]\big)$ is an isomorphism. By Theorem (12.10) this map is injective, so it suffices to prove that the $\mathbb{Q}_p$-dimension of $\mathrm{Hom}^0\big(X[p^\infty], Y[p^\infty]\big)$ is at most the rank of $\mathrm{Hom}(X, Y)$.

Let K be the fraction field of $W(k)$. Write $M_\mathbb{Q}(X)$ and $M_\mathbb{Q}(Y)$ for the F-isocrystals associated to $X[p^\infty]$ and $Y[p^\infty]$, respectively. The Dieudonné functor $M_\mathbb{Q}$ gives an isomorphism $\mathrm{Hom}^0\big(X[p^\infty], Y[p^\infty]\big) \xrightarrow{\sim} \mathrm{Hom}_{F\text{-}\mathsf{Isoc}}\big(M_\mathbb{Q}(Y), M_\mathbb{Q}(X)\big)$. Consider the K-vector space

$$H := \big\{h \in \mathrm{Hom}_K(M_\mathbb{Q}(Y), M_\mathbb{Q}(X)) \;\big|\; h \circ M(\pi_Y) = M(\pi_X) \circ h\big\}.$$

By ?? the characteristic polynomial of $M(\pi_X)$ equals f_X, and similarly for Y. Hence by Lemma (16.22) we have $\dim_K(H) = r(f_Y, f_X) = \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\mathrm{Hom}(X, Y)\big)$.

Let $\#k = q = p^m$. We know that $\pi_X = F^m_{X/k}$, and by definition the endomorphism of $M(X)$ induced by $F_{X/k}$ is $F_{M(X)}$; similarly for Y. Hence $\mathrm{Hom}_{F\text{-}\mathsf{Isoc}}\big(M_\mathbb{Q}(Y), M_\mathbb{Q}(X)\big)$ is a $\mathbb{Q}_p$-subspace of H. We are done if we can show that the K-linear map

AVFF:KHomtoH
$$K \otimes_{\mathbb{Q}_p} \mathrm{Hom}_{F\text{-}\mathsf{Isoc}}\big(M_\mathbb{Q}(Y), M_\mathbb{Q}(X)\big) \to H \tag{5}$$

is injective, because then the $\mathbb{Q}_p$-dimension of $\mathrm{Hom}_{F\text{-}\mathsf{Isoc}}\big(M_\mathbb{Q}(Y), M_\mathbb{Q}(X)\big)$ is at most the K-dimension of H.

The extension $\mathbb{Q}_p \subset K$ is a cyclic Galois extension of order m, with $\mathrm{Gal}(K/\mathbb{Q}_p)$ generated by the automorphism σ_K. (Notation as in ??) Suppose we have elements $h_1, \ldots, h_r \in \mathrm{Hom}_{F\text{-}\mathsf{Isoc}}\big(M_{\mathbb{Q}}(Y), M_{\mathbb{Q}}(X)\big)$ that are linearly independent over $\mathbb{Q}_p$ and suppose we have a non-trivial relation $\sum_{j=1}^r a_j h_j = 0$ with coefficients $a_j \in K$. Without loss of generality we may assume that $a_1 = 1$. We have

$$\begin{aligned} 0 = F^i_{M(X)} \circ \sum_{j=1}^r a_j h_j &= \sum_{j=1}^r \sigma_K^i(a_j) \cdot (F^i_{M(X)} \circ h_i) \\ &= \sum_{j=1}^r \sigma_K^i(a_j) \cdot (h_i \circ F^i_{M(Y)}) = \Big(\sum_{j=1}^r \sigma_K^i(a_j) h_j\Big) \circ F^i_{M(Y)}\,, \end{aligned}$$

and because $F_{M(Y)}$ is injective it follows that $\sum_{j=1}^r \sigma_K^i(a_j) h_j = 0$. Summing this for $i = 0, \ldots, m-1$ we find that $\sum_{j=1}^r \mathrm{trace}_{K/\mathbb{Q}_p}(a_j) \cdot h_j = 0$, and because the elements h_j are linearly independent over $\mathbb{Q}_p$ we conclude that $\mathrm{trace}_{K/\mathbb{Q}_p}(a_j) = 0$ for all j. But $a_1 = 1$ so for $j = 1$ this is clearly false. This proves that the map (5) is indeed injective, and the surjectivity of the map Φ follows by looking at the dimensions of the spaces involved. □

Note how close Theorem (16.20) and its companion (16.24) come to the corresponding statement for complex abelian varieties. There one has an isomorphism

$$\mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathsf{HS}}\big(H_1(X, \mathbb{Z}), H_1(Y, \mathbb{Z})\big)\,;$$

see ??. The Tate module $T_\ell X$ with its Galois action is an analogue of the lattice $H_1(X, \mathbb{Z})$ with its natural Hodge structure.

Note that because we use contravariant Dieudonné theory, we have $\mathbb{Z}_p \otimes \mathrm{Hom}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\mathsf{DM}}\big(M(Y), M(X)\big)$. In particular, $\mathbb{Z}_p \otimes \mathrm{End}(X) \xrightarrow{\sim} \mathrm{End}_{\mathsf{DM}}\big(M(X)\big)^{\mathrm{opp}}$, the opposite ring of $\mathrm{End}_{\mathsf{DM}}\big(M(X)\big)$.

§4. *Corollaries of Tate's theorem, and the structure of the endomorphism algebra.*

TateCorIsog **(16.25) Corollary.** *Let X and Y be abelian varieties over a finite field k of characteristic p. Then the following are equivalent:*

(a) $X \sim Y$;
(b1) *for some $\ell \neq p$ we have $V_\ell X \cong V_\ell Y$ as representations of* $\mathrm{Gal}(\overline{k}/k)$;
(b2) *for all $\ell \neq p$ we have $V_\ell X \cong V_\ell Y$ as representations of* $\mathrm{Gal}(\overline{k}/k)$;
(c1) $X[p^\infty] \sim Y[p^\infty]$;
(c2) $M_{\mathbb{Q}}(X) \cong M_{\mathbb{Q}}(Y)$ *as F-isocrystals;*
(d) $f_X = f_Y$;
(e1) $Z(X; t) = Z(Y; t)$;
(e2) *for all finite field extensions $k \subset k'$ we have $\#X(k') = \#Y(k')$.*

Proof. The implications (a) ⇒ (b2) ⇒ (b1) are clear. Now assume that for some $\ell \neq p$ we have a Galois-equivariant isomorphism $h\colon V_\ell X \xrightarrow{\sim} V_\ell Y$. Possibly after replacing h by $\ell^n h$ for some $n > 0$ we may assume that $h(T_\ell X) \subseteq T_\ell Y$, so that

$$U := \big\{h \in \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y) \;\big|\; h \text{ is injective}\big\}\,.$$

is non-empty. Note that U is ℓ-adically open in $\mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(T_\ell X, T_\ell Y)$ as it is given by the condition that $\det(h) \neq 0$. But $\mathrm{Hom}(X,Y) \subset \mathbb{Z}_\ell \mathrm{Hom}(X,Y)$ is ℓ-adically dense, so by Tate's Theorem (16.20) we can find an element $f \in \mathrm{Hom}(X,Y)$ such that $T_\ell(f)$ is injective. The kernel of f has to be finite, for otherwise $Z := \mathrm{Ker}(f)^0_{\mathrm{red}}$ would be a non-zero abelian subvariety of X (note that we are over a perfect field) and since $T_\ell(f)$ is zero on $T_\ell Z \subseteq T_\ell X$ this gives a contradiction. As the existence of the isomorphism h implies that $\dim(X) = \dim(Y)$, it follows that f is an isogeny.

Similarly it is clear that (a) implies (c1) which by ?? is equivalent to (c2). If (c2) holds then $\mathrm{Hom}_{\mathsf{DM}}\big(M(Y), M(X)\big)$ again contains a non-empty open subset of injective maps. By Theorem (16.24), using that $\mathrm{Hom}(X,Y)$ is dense in $\mathbb{Z}_p\mathrm{Hom}(X,Y)$, there exists an $f \in \mathrm{Hom}(X,Y)$ such that $M(f)$ is injective, which is equivalent to $f[p^\infty]$ being an isogeny. Now the same argument as in the ℓ-adic case shows that f is an isogeny.

Because f_X is the characteristic polynomial of $V_\ell(\pi_X)$ for any $\ell \neq p$ we have (b1) $\Rightarrow$ (d). Conversely, because the representations ρ_ℓ are semisimple, (d) implies that $V_\ell X \cong V_\ell Y$ as Galois representations. (Cf. Remark (16.21).)

The equivalence of (d), (e1) and (e2) readily follows from the Weil Conjectures, Theorems (16.4) and (16.7); note that the complex zeroes of f_X are precisely the zeroes of $Z(X;t)$ that have absolute value $q^{1/2}$, with $q = \#k$. □

TateCorEnd0 **(16.26) Corollary.** *Let X be an abelian variety over a finite field.*

(i) *The center of $\mathrm{End}^0(X)$ is the subalgebra $\mathbb{Q}[\pi_X]$. In particular, X is elementary if and only if $\mathbb{Q}[\pi_X] = \mathbb{Q}(\pi_X)$ is a field, and this occurs if and only if f_X is a power of an irreducible polynomial in $\mathbb{Q}[t]$.*

(ii) *Suppose X is elementary, $\dim(X) = g$. Let $h = f_{\mathbb{Q}}^{\pi_X}$ be the minimum polynomial of π_X over $\mathbb{Q}$. Further let $d := [\mathrm{End}^0(X) : \mathbb{Q}(\pi_X)]^{1/2}$ and $e := \big[\mathbb{Q}(\pi_X) : \mathbb{Q}\big]$. Then $de = 2g$ and $f_X = h^d$.*

Proof. (i) It is clear that $\mathbb{Q}[\pi_X]$ is contained in the center of $\mathrm{End}^0(X)$. To prove that the two are equal, it suffices to show that $\mathbb{Q}_\ell[\pi_X]$ is the center of $\mathbb{Q}_\ell\mathrm{End}^0(X)$ for some $\ell \neq p$. (If Z is the center of $\mathrm{End}^0(X)$ then $\mathbb{Q}_\ell \otimes Z$ is the center of $\mathbb{Q}_\ell\mathrm{End}^0(X)$.) But if f lies in the center of $\mathbb{Q}_\ell\mathrm{End}^0(X)$ then f is an element of the commutant of $\mathbb{Q}_\ell\mathrm{End}^0(X)$, which is $\mathbb{Q}_\ell\big[\mathrm{Im}(\rho_\ell)\big]$; cf. the remark after Theorem (16.18). Now use that $\mathbb{Q}_\ell\big[\mathrm{Im}(\rho_\ell)\big] = \mathbb{Q}_\ell[\pi_X]$, see Exercise (16.4). The remaining assertions of (i) are clear; see also (ii) of Prop. (16.3).

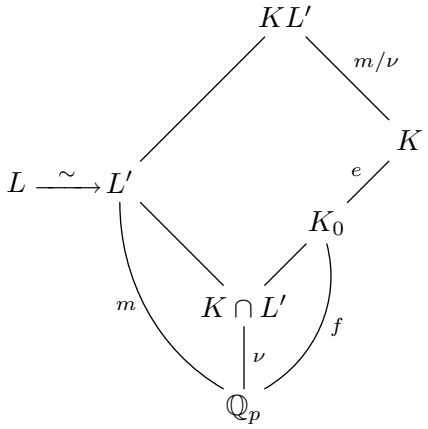
(ii) We know that $f_X = h^\delta$ for some δ, and comparison of the degrees gives $\delta = 2g/e$. On the other hand, by Corollary (16.23) the $\mathbb{Q}$-dimension of $\mathrm{End}^0(X)$ equals $e\delta^2$, so $\delta = d$. □

TateCor2End0 **(16.27) Corollary.** *Let X be an abelian variety of dimension g over a finite field. Then $2g \leqslant \dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) \leqslant (2g)^2$, and X is of CM-type.*

Proof. If X is elementary then by (ii) of the previous Corollary we have $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) = 2g \cdot d = (2g)^2/e$, so indeed $2g \leqslant \dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) \leqslant (2g)^2$. In this case $D := \mathrm{End}^0(X)$ is a central simple algebra of degree d^2 over $K := \mathbb{Q}[\pi_X]$, and any such algebra contains a subfield $L \subset D$ with $[L : K] = d$, so $[L : \mathbb{Q}] = de$. Hence the equality $de = 2g$ implies that X is of CM-type. For general X the assertions are readily obtained by considering the decomposition of X up to isogeny as a product of elementary factors. □

L[t]/h(tm)Prep **(16.28)** As a preparation for the next corollary of Tate's theorem we need a result about the structure of certain quotients of Dieudonné rings.

The situation that we shall be interested in is the following. We are working over a finite field $\mathbb{F}_q$, where $q = p^m$ is a power of a prime number p. Let L be the fraction field of $W(\mathbb{F}_q)$. Further we consider a finite field extension $\mathbb{Q}_p \subset K = \mathbb{Q}_p(\varpi)$ with $\varpi \neq 0$. Let $h = f^{\varpi}_{\mathbb{Q}_p} \in \mathbb{Q}_p[T]$ be the minimum polynomial of ϖ over $\mathbb{Q}_p$, so that $K \cong \mathbb{Q}_p[T]/(h)$. Choose an algebraic closure $K \subset \overline{K}$ and an embedding $i\colon L \hookrightarrow \overline{K}$. The subfield $L' := i(L) \subset \overline{K}$ is independent of the choice of i. Consider the ring $B := L[t;\sigma]/\big(h(t^m)\big)$, which we view as a K-algebra via the homomorphism $K = \mathbb{Q}_p(\varpi) \to B$ that sends ϖ to the class of t^m. If the residue field of O_K has cardinality p^f, let $\nu := \gcd(m,f) = [K \cap L' : \mathbb{Q}_p]$. Finally let KL' be the compositum of K and L'. To summarize, we have the following diagram of fields, where we denote by $K_0 \subset K$ the maximal unramified subfield, and where $e = [K : K_0]$ is the ramification index.



The field extension $K \subset KL'$ is cyclic of degree m/ν. A generator of the Galois group is the automorphism τ that via the isomorphism $L' \otimes_{K\cap L'} K \xrightarrow{\sim} KL'$ corresponds to the automorphism $\sigma^{\nu}_{L'} \otimes \mathrm{id}_K$, where $\sigma_{L'}$ is the unique automorphism of L' that induces the Frobenius automorphism $x \mapsto x^p$ on its residue field. Note that this automorphism is not, in general, the arithmetic Frobenius $\sigma_{KL'/K}$. (Recall that the latter is, by definition, the unique generator of $\mathrm{Gal}(KL'/K)$ that induces the automorphism $x \mapsto x^{p^f}$ on the residue field of KL'.) The relation between the two is that $\tau^{f/\nu} = \sigma_{KL'/K}$, as $\tau^{f/\nu}$ corresponds to $\sigma^f_{L'} \otimes \mathrm{id}_K$ on $L' \otimes_{K\cap L'} K$, which indeed induces $x \mapsto x^{p^f}$ on the residue field.

Let $\mathrm{ord}\colon \overline{K}^* \to \mathbb{Q}$ be the valuation with $\mathrm{ord}(p) = 1$.

L[t]/h(tm) **(16.29) Lemma.** *Situation and notation as in* (16.28). *Then $B = L[t;\sigma]/\big(h(t^m)\big)$ is isomorphic, as a K-algebra, to $M_\nu\big((KL'/K,\tau,\varpi)\big)$, the algebra of $\nu \times \nu$ matrices with coefficients in the cyclic algebra $(KL'/K,\tau,\varpi)$. In particular, B is a central simple K-algebra with Brauer invariant $\big(\mathrm{ord}(\varpi)/\mathrm{ord}(q)\big) \cdot [K : \mathbb{Q}_p]$.*

Proof. Write $(KL'/K,\tau,\varpi) = KL'[\varphi]$, where the element φ satisfies

$$\varphi^{m/\nu} = \varpi \qquad \text{and} \qquad \varphi \cdot a = \tau(a) \cdot a \quad \text{for all } a \in KL'.$$

We have $L' \otimes_{\mathbb{Q}_p} K \cong L[T]/\big(h(T)\big)$, and sending the class of T to the class of t^m in B we obtain an isomorphism

AVFF;BLK[t]
$$B \cong (L' \otimes_{\mathbb{Q}_p} K)\Big[t;\sigma_{L'} \otimes \mathrm{id}\Big] \Big/ \Big(t^m - (1 \otimes \varpi)\Big). \tag{6}$$

In particular, $\dim_K(B) = m^2$, which is equal to the K-dimension of $M_\nu\big((KL'/K,\tau,\varpi)\big)$.

Taking the isomorphism (6) as an identification, consider the homomorphism of K-algebras $j\colon B \to M_\nu\big(KL'[\varphi]\big)$ that sends an element $x \otimes y \in L' \otimes_{\mathbb{Q}_p} K$ to the diagonal matrix

$$\operatorname{diag}\big(xy, \sigma_{L'}(x)y, \ldots, \sigma_{L'}^{\nu-1}(x)y\big)\,,$$

and that sends the class of t to the matrix

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ \varphi & & & & 0 \end{pmatrix}$$

in which all omitted entries are 0. One checks directly that j gives a well-defined homomorphism of K-algebras. As the source and target have the same K-dimension, to prove that j is an isomorphism it suffices to show that it is surjective.

It is clear that the restriction of j to $L' \otimes_{\mathbb{Q}_p} K \subset B$ gives an isomorphism $L' \otimes_{\mathbb{Q}_p} K \xrightarrow{\sim} (KL')^\nu = KL' \times \cdots \times KL'$, where we place the ν factors KL' on the diagonal. Further, $j(t^\nu)$ is the diagonal matrix $\operatorname{diag}(\varphi, \ldots, \varphi)$. Together, these generate the full diagonal subalgebra $\Delta := KL'[\varphi] \times \cdots \times KL'[\varphi] \subset M_\nu\big(KL'[\varphi]\big)$. It follows that the image of j also contains

$$j(\bar{t}) \cdot \operatorname{diag}(\varphi^{(m/\nu)-1}\varpi^{-1}, 1, \ldots, 1) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ 1 & & & & 0 \end{pmatrix}.$$

Call this matrix A. By taking all expressions $\operatorname{diag}(0, \ldots, 0, 1, 0, \ldots, 0) \cdot A^i$ we get all elementary matrices, and together with Δ these generate the whole $M_\nu\big(KL'[\varphi]\big)$. So indeed j is an isomorphism.

For the last assertion we just note that

$$(KL'/K, \tau, \varpi) \cong (KL'/K, \tau^{f/\nu}, \varpi^{f/\nu}) = (KL'/K, \sigma_{KL'/K}, \varpi^{f/\nu})\,,$$

which has Brauer invariant

$$\frac{\operatorname{ord}\big(\varpi^{f/\nu}\big)}{(m/\nu)} = f \cdot \frac{\operatorname{ord}(\varpi)}{m} = ef \cdot \frac{\operatorname{ord}(\varpi)}{\operatorname{ord}(q)} = \frac{\operatorname{ord}(\varpi)}{\operatorname{ord}(q)} \cdot [K : \mathbb{Q}_p]\,.$$

(Cf. (A.5) and (A.6).) □

With the aid of this lemma we obtain a precise result about the structure of the endomorphism algebra of an elementary abelian variety X, viewed as a simple algebra over its centre $\mathbb{Q}[\pi_X]$.

End0LocInv **(16.30) Corollary.** *Let X be an elementary abelian variety over a field with $q = p^m$ elements. Let $K = \mathbb{Q}(\pi_X)$. If v is a place of K then the local invariant of $\operatorname{End}^0(X)$ in the Brauer group $\operatorname{Br}(K_v)$ is given by*

$$\operatorname{inv}_v\big(\operatorname{End}^0(X)\big) = \begin{cases} 0 & \text{if } v \text{ is a finite place not above } p; \\ \frac{\operatorname{ord}_v(\pi_X)}{\operatorname{ord}_v(q)} \cdot [K_v : \mathbb{Q}_p] & \text{if } v \text{ is a place above } p; \\ 1/2 & \text{if } v \text{ is a real place of } K; \\ 0 & \text{if } v \text{ is a complex place of } K. \end{cases}$$

Note that the line about the local invariant at complex places is included for completeness only, as the Brauer group of $\mathbb{C}$ is trivial.

Proof. Without loss of generality we may assume that X is simple, for if $X \sim Y^m$ then $\mathrm{End}^0(X) = M_m\big(\mathrm{End}^0(Y)\big)$ which has the same local invariants as $\mathrm{End}^0(Y)$. Then $D := \mathrm{End}^0(X)$ is a divison algebra with center $K := \mathbb{Q}(\pi_X)$. If K admits a real place then D is necessarily of Type III in the Albert classification (cf. Remark ??), in which case $\mathrm{inv}_v(D) = 1/2$ for all infinite places of K (which are then all real). See also (16.33) below for further discussion.

If ℓ is a prime number with $\ell \neq \mathrm{char}(k)$ and $\lambda_1, \ldots, \lambda_t$ are the places of K above ℓ then $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} K = K_{\lambda_1} \times \cdots \times K_{\lambda_t}$ with each K_{λ_i} a finite extension of $\mathbb{Q}_\ell$. We have a corresponding decomposition $V_\ell X = V_{\lambda_1} X \oplus \cdots \oplus V_{\lambda_t} X$, with $V_{\lambda_i} X := K_{\lambda_i} \cdot V_\ell X$ a vector space of dimension $d = 2g/[K : \mathbb{Q}]$ over K_{λ_i}. Tate's theorem, taking into account what was explained in (16.21), gives that $\mathbb{Q}_\ell \mathrm{End}(X) = \mathrm{End}_{\mathbb{Q}_\ell \otimes K}(V_\ell X)$, so

$$\begin{aligned} \mathrm{End}^0(X) \otimes_K K_{\lambda_i} &= \mathbb{Q}_\ell \mathrm{End}(X) \otimes_{\mathbb{Q}_\ell \otimes K} K_{\lambda_i} \\ &= \mathrm{End}_{\mathbb{Q}_\ell \otimes K}(V_\ell X) \otimes_{\mathbb{Q}_\ell \otimes K} K_{\lambda_i} = \mathrm{End}_{K_{\lambda_i}}(V_{\lambda_i} X) \cong M_d(K_{\lambda_i})\,. \end{aligned}$$

Hence indeed the local invariants at the λ_i are trivial.

It remains to compute the local invariants at the places of K above p. Let $h = f_{\mathbb{Q}}^{\pi_X}$, and let $h = h_1 \cdots h_u$ be its factorization in $\mathbb{Q}_p[t]$. The factors h_i correspond to the places v_i of K above p, and we have a decomposition $\mathbb{Q}_p \otimes K = K_1 \times \cdots \times K_u$ with $K_i \cong \mathbb{Q}_p[t]/(h_i)$ the v_i-adic completion of K. As $\mathbb{Q}_p \otimes K$ acts on $M_{\mathbb{Q}}(X)$ this induces a decomposition of $\mathbb{Q}_p$-vector spaces $M_{\mathbb{Q}}(X) = M_1 \oplus \cdots \oplus M_u$.

Write L for the fraction field of $W(k)$. Let σ be the automorphism of L induced by the Frobenius automorphism of k, and consider the skew polynomial ring $L[F] = L[F;\sigma]$. The isocrystal $M_{\mathbb{Q}}(X)$ is a (left) $L[F]$-module. We know that π_X acts on $M_{\mathbb{Q}}(X)$ as F^m, which is L-linear. Because F^m is a central element in $L[F]$ the subspaces $M_i \subset M_{\mathbb{Q}}(X)$ are $L[F]$-submodules, so the decomposition $M_{\mathbb{Q}}(X) = M_1 \oplus \cdots \oplus M_u$ is a decomposition of isocrystals. The minimum polynomial of $\pi_X = F^m$ acting on M_i is just the polynomial h_i.

By Tate's Theorem (16.24) we have an isomorphism

$$\mathbb{Q}_p \otimes \mathrm{End}^0(X) \xrightarrow{\sim} \mathrm{End}_{L[F]}\big(M_{\mathbb{Q}}(X)\big)^{\mathrm{opp}}\,,$$

and this induces isomorphisms

$$\mathrm{End}^0(X) \otimes_K K_i = \big(\mathbb{Q}_p \otimes \mathrm{End}^0(X)\big) \otimes_{(\mathbb{Q}_p \otimes K)} K_i \xrightarrow{\sim} \mathrm{End}_{L[F]}(M_i)^{\mathrm{opp}}\,.$$

As $h_i(F^m) = 0$ on M_i we may view M_i as a module over $B_i := L[F]/\big(h_i(F^m)\big)$. But by Lemma (16.28), B_i is a central simple algebra over K_i. If N_i is the unique simple B_i-module (up to isomorphism) then $M_i \cong N_i^r$ for some $r \geqslant 1$, and we find

$$\mathrm{End}_{L[F]}(M_i)^{\mathrm{opp}} = \mathrm{End}_{B_i}(M_i)^{\mathrm{opp}} \cong M_r(B_i)\,,$$

which is Brauer-equivalent with B_i. Hence the local invariant of $\mathrm{End}^0(X)$ at the prime v_i equals that of B_i, which we have calculated to be $\big(\mathrm{ord}_{v_i}(\pi_X)/\mathrm{ord}_{v_i}(q)\big) \cdot [K_i : \mathbb{Q}_p]$. This finishes the proof. □

EndFFRem **(16.31) Remarks.** (i) To avoid any misunderstanding let us again stress that throughout, by $\mathrm{End}^0(X)$ we mean the endomorphism algebra of X over the given finite field. The structure of

the endomorphism algebra may change under an extension of the ground field; for some concrete examples see (16.33) below.

(ii) As in Corollary (16.30), suppose X is elementary and let $K := \mathbb{Q}(\pi_X)$. Let $q = \#k$, and define invariants i_v by $\|\pi_X\|_v = q^{-i_v}$, where $\| \ \|_v$ is the normalized absolute value corresponding to a prime v. (See 0.6.) Then we can also describe the local invariants of the endomorphism algebra by the rule

$$\mathrm{inv}_v\big(\mathrm{End}^0(X)\big) \equiv i_v \bmod \mathbb{Z} \qquad \text{for all primes } v \text{ of } K.$$

(For the infinite primes use Theorem (16.4); for the primes above p use that $q^{-i_v} = q_v^{-\mathrm{ord}_v(\pi_X)}$, so $i_v \cdot \mathrm{ord}_v(q) = \mathrm{ord}_v(\pi_X) \cdot \mathrm{ord}_v(q_v) = \mathrm{ord}_v(\pi_X) \cdot [K_v : \mathbb{Q}_p]$.) The product formula for normalized absolute values translates into the sum formula $\sum i_v \equiv 0 \bmod \mathbb{Z}$ in the Brauer group.

(iii) Still in the situation of Corollary (16.30), let $x \mapsto \bar{x}$ be the complex conjugation on $K = \mathbb{Q}[\pi_X]$, and let $K_0 = \mathbb{Q}[\pi_X + q/\pi_X] \subset K$ be the fixed field. Then K_0 is a totally real field, and either $K_0 = K$ or K is a totally imaginary quadratic extension of K_0; see also the discussion in (16.33) below. Let v be a place of K above p, and let v_0 be its restriction to K_0. We know that $\bar{\pi}_X = q/\pi_X$. It follows that $\mathrm{ord}_v(\pi_X) + \mathrm{ord}_{\bar{v}}(\pi_X) = \mathrm{ord}_v(q) = \mathrm{ord}_{\bar{v}}(q)$. Hence $\mathrm{inv}_v\big(\mathrm{End}^0(X)\big) = -\mathrm{inv}_{\bar{v}}\big(\mathrm{End}^0(X)\big)$. Further, if $v = \bar{v}$, which occurs if the place v_0 is either inert or ramified in the extension $K_0 \subset K$, then $[K_v : \mathbb{Q}_p]$ is necessarily even, and it follows that $\mathrm{inv}_v\big(\mathrm{End}^0(X)\big) = 0$.

d=lcm(iv) **(16.32) Corollary.** *Let X be a simple abelian variety over a finite field k. Let d be the index of the division algebra $D := \mathrm{End}^0(X)$ over its center $\mathbb{Q}[\pi_X]$ (so $d = [D : \mathbb{Q}(\pi_X)]^{1/2}$ and $f_X = (f_{\mathbb{Q}}^{\pi_X})^d$). Then d is the least common denominator of the local invariants $i_v = \mathrm{inv}_v(D)$.*

Proof. As discussed in (A.4) the index of D equals its period, i.e., the order of its class $[D]$ in the Brauer group $\mathrm{Br}(K)$. As $\mathrm{Br}(K) \hookrightarrow \prod_v \mathrm{Br}(K_v)$, this order is just the least common denominator of the local invariants i_v. □

QpiReal **(16.33)** Let X be a simple abelian variety over $k = \mathbb{F}_q$. Write $D := \mathrm{End}^0(X)$. Because X is of CM-type, D is either of Type III or of Type IV in the Albert classification; see Remark ??. We can see in which case we are by looking at the center $K := \mathbb{Q}(\pi_X)$. Indeed, as we have already seen in the proof of Theorem (16.4), either K is totally real (D of Type III) or K is a CM-field (D of Type IV).

The real case is very exceptional. Indeed, let $h := f_{\mathbb{Q}}^{\pi_X}$. As we have just seen, $f_X = h^d$ where d is the index of D. If K is totally real then all complex roots of f_X are real numbers of absolute value $\sqrt{q}$. We distinguish two cases:

(1) If q is a square then $h = t \pm \sqrt{q}$, so $K = \mathbb{Q}$ and we find that $d = 2g/e = 2g$. By Corollary (16.30) we have $\mathrm{inv}_p(D) = 1/2 = \mathrm{inv}_\infty(D)$ and $\mathrm{inv}_\ell(D) = 0$ at all other places. Corollary (16.32) then gives $d = 2$. Hence X is an elliptic curve and D is the unique quaternion algebra over $\mathbb{Q}$ that is non-split at p and ∞ and split at all other primes. This algebra is usually denoted by $D_{p,\infty}$. By Theorem (15.35) X is supersingular.

We shall prove in ?? that the isogeny classes corresponding to the characteristic polynomials $(t-\sqrt{q})^2$ and $(t+\sqrt{q})^2$ both occur. If we extend scalars from k to its quadratic extension $k' = \mathbb{F}_{q^2}$ then the two isogeny classes coincide, as in both cases the characteristic polynomial over k' is $(t-q)^2$. (But over k' there is also the isogeny class with characteristic polynomial $(t+q)^2$, which is not defined over k.) Concretely this means that if E is a supersingular curve over k with characteristic polynomial $(t-\sqrt{q})^2$, a suitable quadratic twist of E has characteristic polynomial $(t+\sqrt{q})^2$.

(2) If q is not a square then $h = t^2 - q$, so $K = \mathbb{Q}\big[\sqrt{q}\big] = \mathbb{Q}\big[\sqrt{p}\big]$ and we find that $d = g$. There is a unique prime $\mathfrak{p}$ of K above p and $\mathrm{inv}_{\mathfrak{p}}(D) = 0$. So D is the unique quaternion algebra over K that is non-split at the two infinite places of K and split at all finite primes. Using Corollary (16.32) we find that $d = 2$, so $g = 2$ and X is a simple abelian surface. If we extend scalars from k to its quadratic extension $k' = \mathbb{F}_{q^2}$ then $X' := X \otimes k'$ has characteristic polynomial $f_{X'} = (t-q)^4$. In this case we find that $\mathrm{End}^0(X') \cong M_2(D_{p,\infty})$ and X' is isogenous to Y^2, where Y is a supersingular elliptic curve over k' with characteristic polynomial $(t-q)^2$. (So Y realizes one of the two isogeny classes from case (1).) Again we shall see in ?? that the isogeny class over k with characteristic polynomials $t^2 - q$ does occur.

Except in these particular cases, the center $K = \mathbb{Q}(\pi_X)$ is always a CM-field. Note that in case (2) the structure of $\mathrm{End}^0(X)$ changes when we extend scalars from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$.

As we have seen in Corollary (16.27), the $\mathbb{Q}$-dimension of $\mathrm{End}^0(X)$, for X an abelian variety of dimension g over a finite field, lies between $2g$ and $(2g)^2$. Let us analyze the two extremal cases.

TateCorExtreme **(16.34) Corollary.** *Let X be an abelian variety of dimension g over a finite field k.*

(i) *The following are equivalent:*
- (a) $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) = 2g$;
- (b1) $\mathrm{End}^0(X) = \mathbb{Q}[\pi_X]$;
- (b2) $\mathrm{End}^0(X)$ *is commutative;*
- (c) f_X *has no multiple root.*

(ii) *The following are equivalent:*
- (a) $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) = (2g)^2$;
- (b) $\mathbb{Q}[\pi_X] = \mathbb{Q}$;
- (c) f_X *is a power of a linear polynomial;*
- (d) $\mathrm{End}^0(X) \cong M_g(D_{p,\infty})$, *where $D_{p,\infty}$ is the quaternion algebra with center $\mathbb{Q}$ that has local invariant $1/2$ at p and ∞ and local invariant 0 at all other places;*
- (e) X *is supersingular with* $\mathrm{End}(X) = \mathrm{End}(X_{\overline{k}})$;
- (f) X *is isogenous to E^g for a supersingular elliptic curve E over k with* $\mathrm{End}(E) = \mathrm{End}(E_{\overline{k}})$.

Proof. We start with two general remarks. Suppose f_X has r distinct complex roots, with multiplicities $\nu_1, \ldots, \nu_r$. On the one hand, $\nu_1 + \cdots + \nu_r = \deg(f_X) = 2g$. On the other hand, by Lemma (16.22) we may calculate $r(f_X, f_X)$ over $\mathbb{C}$, and this gives $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) = \nu_1^2 + \cdots + \nu_r^2$.

Next write $X \sim X_1 \times \cdots \times X_n$ where the factors X_i are elementary over k and satisfy $\mathrm{Hom}^0(X_i, X_j) = 0$ for $i \neq j$. (In the decomposition (1) in Corollary (12.5), take $X_i := Y_i^{m_i}$.) Write $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X_i)\big) = e_i d_i^2$ with e_i the degree of $\mathbb{Q}(\pi_{X_i})$ over $\mathbb{Q}$. Then $\dim_{\mathbb{Q}}\big(\mathrm{End}^0(X)\big) = \sum_{i=1}^n d_i^2 e_i$, whereas by (ii) of Corollary (16.26) we have $2g = \sum_{i=1}^n d_i e_i$.

We now prove (i). With the above notation, (ia) means that $\sum \nu_j = \sum \nu_j^2$, which occurs precisely if all ν_j are equal to 1. So (i)(a) $\Leftrightarrow$ (i)(c). Also (i)(a) means that $\sum_{i=1}^n d_i^2 e_i = \sum_{i=1}^n d_i e_i$; this occurs precisely if $d_i = 1$ for all i, which is equivalent to saying that $\mathrm{End}^0(X)$ is commutative. This shows that in (i) we have (a) $\Leftrightarrow$ (b2). Finally, the equivalence of (b1) and (b2) is immediate from part (i) of Corollary (16.26).

Next we prove (ii). Condition (a) means that $\sum_{j=1}^r \nu_j^2 = (\sum_{j=1}^r \nu_j)^2$, which occurs if and only if $r = 1$. So (a) $\Leftrightarrow$ (c). Further, (a) says that $\sum_{i=1}^n d_i^2 e_i = (\sum_{i=1}^n d_i e_i)^2$, and as for each index i we have $d_i^2 e_i \leqslant (d_i e_i)^2$ this only occurs if $n = 1$ and $e_1 = 1$. It follows that in (ii) we

have (a) $\Leftrightarrow$ (b). (Alternatively, (b) $\Leftrightarrow$ (c) readily follows from Corollary (16.26) together with (ii) of Proposition (16.3).)

The implication (d) $\Rightarrow$ (a) is clear. If (a)–(c) hold then (d) follows by application of Corollaries (16.26) and (16.30).

Next assume that (a)–(d) hold. By (d), $X \sim E^g$ for some elliptic curve, and by Theorem (15.35) it follows from (c) that E is supersingular. Further, by (a) and the estimates in (16.27) we have $\mathrm{End}_k^0(X) = \mathrm{End}_{\overline{k}}^0(X_{\overline{k}})$, so also $\mathrm{End}_k(X) = \mathrm{End}_{\overline{k}}(X_{\overline{k}})$. (See Exercise (12.2).) So (f) holds, and it is clear that this implies (e).

Finally assume that (e) holds. If $\alpha \in \overline{\mathbb{Q}}$ is a root of f_X then $\alpha/\sqrt{q}$ is a root of unity. Indeed, if K is a number field containing $\alpha/\sqrt{q}$ then the assumption that all slopes of the Newton polygon equal $1/2$ implies that $\mathrm{ord}_v(\alpha/\sqrt{q}) = 0$ for all primes v; see (16.9). Hence there is a finite extension $k \subset k'$, say of degree N, such that the roots α^N of $f_{(X \otimes k')}$ are all equal to $q^{N/2}$. So over k' we have (c), hence also (a). But by the assumption that $\mathrm{End}(X) = \mathrm{End}(X_{\overline{k}})$ it then follows that (a) also holds over k. $\square$

TateCorExtrRem **(16.35) Remark.** If X is a supersingular abelian variety over a finite field k then it follows from the proof that already over a finite extension of k the p-divisible group $X[p^\infty]$ becomes isogenous to $\mathscr{G}_{1/2}^g$. This behaviour is a-typical: if X has Newton polygon β and is not supersingular then in general we need to extend scalars to $\overline{k}$ to get an isogeny between $X[p^\infty]$ and $\mathscr{G}_\beta$. (Notation as in ??.)

To make this explicit, take a prime number p and an integer a with $p \nmid a$ and $a^2 < 4p$. Let $f := t^2 - at + p$. We shall prove in Theorem (16.41) below that there exists an elliptic curve E over $\mathbb{F}_p$ with $f_E = f$. By Theorem (15.35), E is ordinary. So over $\overline{\mathbb{F}}_p$ we have that $E[p^\infty]$ is isogenous to $\mathbb{Q}_p/\mathbb{Z}_p \times \widehat{\mathbb{G}}_m$, and we may ask if such an isogeny can be realised over a finite field. The answer is *no*. To see this, let α_1 and $\alpha_2 = \bar{\alpha}_1 = p/\alpha_1$ be the roots of f in $\overline{\mathbb{Q}}$. If $E_{\mathbb{F}_q}[p^\infty]$ is isogenous to $\mathbb{Q}_p/\mathbb{Z}_p \times \widehat{\mathbb{G}}_m$ over $\mathbb{F}_q$, for some $q = p^m$, then in particular the characteristic polynomial of π_E^m on the rational Dieudonné module $M_{\mathbb{Q}}(E_{\mathbb{F}_q})$ equals $t \cdot (t-p)$. Hence one of the α_i is a root of unity. But there is no root of unity that has minimum polynomial of the form $t^2 - at + p$, so indeed we need to extend scalars to $\overline{\mathbb{F}}_p$ in order to get an isogeny between $E[p^\infty]$ and $\mathbb{Q}_p/\mathbb{Z}_p \times \widehat{\mathbb{G}}_m$.

End0StructRem **(16.36) Remark.** The results that we have proven allow us to recover $\mathrm{End}^0(X)$, for an abelian variety X over $\mathbb{F}_q$, from the characteristic polynomial f_X. Before we describe a procedure for this, let us quickly recapitulate what we know.

If $X \sim Y_1^{m_1} \times \cdots \times Y_n^{m_n}$ is the decomposition of X up to isogeny as in (12.5), so with each Y_i simple over $\mathbb{F}_q$ and $Y_i \not\sim Y_j$ if $i \neq j$, then we have $f_X = f_{Y_1}^{m_1} \cdots f_{Y_n}^{m_n}$, and by (i) of Corollary (16.26), each f_{Y_i} is a power of an irreducible polynomial, say $f_{Y_i} = h_i^{a_i}$. Then $D_i := \mathrm{End}^0(Y_i)$ is the division algebra with center $\mathbb{Q}(\pi_{Y_i}) \cong \mathbb{Q}[t]/(h_i)$ that is uniquely determined by the local invariants given in Corollary (16.30). Further we have $a_i \cdot \deg(h_i) = 2\dim(Y_i) = \mathrm{index}(D_i) \cdot \deg(h_i)$, so $a_i = \mathrm{index}(D_i)$. Finally we have $\mathrm{End}^0(X) \cong \prod_{i=1}^n M_{m_i}(D_i)$ with $\pi_X \mapsto (\varpi_1, \ldots, \varpi_n)$.

These facts make it clear how to reconstruct $\mathrm{End}^0(X)$, up to isomorphism, from f_X. Start by writing $f_X = h_1^{\mu_1} \cdots h_n^{\mu_n}$ with $h_i \in \mathbb{Q}[t]$ monic irreducible and $h_i \neq h_j$ if $i \neq j$. Define $K_i := \mathbb{Q}[t]/(h_i)$, and let $\varpi_i \in K_i$ be the class of t. Next, let D_i be the division algebra with

center K_i, uniquely determined up to isomorphism, with local invariants $i_v(B_i)$ given by

$$\mathrm{inv}_v(B_i) = \begin{cases} \frac{\mathrm{ord}_v(\varpi_i)}{\mathrm{ord}_v(q)} \cdot \big[(K_i)_v : \mathbb{Q}_p\big] & \text{if } v \text{ is a place of } K_i \text{ above } p; \\ 1/2 & \text{if } v \text{ is a real place of } K_i; \\ 0 & \text{else.} \end{cases}$$

Then the index of D_i divides μ_i, and if we let $m_i := \mu_i/\mathrm{index}(D_i)$ we have $\mathrm{End}^0(X) \cong \prod_{i=1}^n M_{m_i}(D_i)$.

Note that if X is simple we in fact only need to know the minimum polynomial of π_X over $\mathbb{Q}$ in order to reconstruct $\mathrm{End}^0(X)$.

OrdCurveExa **(16.37) Example.** (i) Suppose $X/\mathbb{F}_q$ is a simple abelian variety of dimension g which is ordinary. By (16.33) we know that $\mathbb{Q}[\pi_X]$ has no real embeddings. Comparing Theorem (15.35) and Corollary (16.30) we find that all local invariants of $\mathrm{End}^0(X)$ are zero. It follows that $\mathrm{End}^0(X) = \mathbb{Q}[\pi_X]$ is a CM-field of degree $2g$ over $\mathbb{Q}$. This conclusion is in fact valid for simple ordinary abelian varieties over any field of characteristic p, as can be shown using the Serre-Tate theory of canonical liftings. See ??.

(ii) Let $X = \mathrm{Jac}(C)$ with C the nonsingular complete curve of genus 2 over $\mathbb{F}_3$ defined by the equation $y^3 - y = x + x^{-1} + 1$. Counting points over $\mathbb{F}_{3^i}$ for $i = 1, \ldots, 4$ we find that $f_X = t^4 + t^3 - 2\,t^2 + 3\,t + 9$, which is an irreducible polynomial in $\mathbb{Q}[t]$. Using Corollary (16.26) we find that $\mathrm{End}^0(X) = \mathbb{Q}[\pi_X]$, a CM-field of degree 4 over $\mathbb{Q}$. By Corollary (15.36), X is ordinary. After extensions of scalars to $\mathbb{F}_{27}$ we find $f_{X\otimes\mathbb{F}_{27}} = (t^2 + 8\,t + 27)^2$, and it follows from (i) together with (i) of Corollary (16.26) that $X_{\mathbb{F}_{27}}$ is isogenous to the square of an elliptic curve. This conflicts with Waterhouse [1], p. 553, Thm. 7.2 and with Milne and Waterhouse [1], p. 62, lines 15–16. See van der Geer and van der Vlugt [1] for further examples.

§5. *Abelian varieties up to isogeny and Weil numbers.*

qWeilDef **(16.38) Definition.** Let q be a power of a prime number. Then a *q-Weil number* is an algebraic integer π with the property that $|\iota(\pi)| = \sqrt{q}$ for all embeddings $\iota\colon \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$. Two q-Weil numbers π and π' are said to be *conjugate* if they have the same minimum polynomial over $\mathbb{Q}$, or, what amounts to the same, if there is an isomorphism $\mathbb{Q}[\pi] \xrightarrow{\sim} \mathbb{Q}[\pi']$ sending π to π'.

qWeilofAV **(16.39)** Let X be an elementary abelian variety over $\mathbb{F}_q$. By Theorem (16.4), the Frobenius endomorphism π_X is a q-Weil number. For every embedding $\iota\colon \mathbb{Q}[\pi_X] \to \overline{\mathbb{Q}}$ we get a q-Weil number $\iota(\pi_X)$ in $\overline{\mathbb{Q}}$, and up to conjugacy this number is independent of the choice of ι. So we may represent the conjugacy class of π_X by an actual number in $\overline{\mathbb{Q}}$. Note that we have assumed X to be elementary, since we want $\mathbb{Q}[\pi_X]$ to be a field.

It is an easy exercise to show that an algebraic integer $\pi \in \overline{\mathbb{Q}}$ is a q-Weil number if and only if $\pi = \pm\sqrt{q}$ or π is a root of $T^2 - aT + q$, where $a = \pi + q/\pi$ generates a totally real field $\mathbb{Q}(a)$ in which $a^2 - 4q$ is totally negative. (This is Exercise (16.6).) This gives a concrete method for constructing q-Weil numbers: Take an irreducible monic polynomial $g \in \mathbb{Z}[T]$ all whose complex roots are real and lie in the open interval $(-2\sqrt{q}, 2\sqrt{q})$. Let $a \in \overline{\mathbb{Q}}$ be a root of g. Then a root π of $T^2 - aT + q$ is a q-Weil number such that $F = \mathbb{Q}(\pi)$ has no real embeddings into $\mathbb{C}$. For example, let $g = T^6 - 4T^5 - T^4 + 17T^3 - 9T^2 - 16T + 11 \in \mathbb{Z}[T]$. All six roots are real and lie

in the interval $(-2\sqrt{2}, 2\sqrt{2})$. Therefore, a solution of $T^2 - aT + 2$ with a a root of g defines an algebraic integer of degree 12 over $\mathbb{Q}$ whose absolute value under any embedding is $\sqrt{2}$, so this gives a 2-Weil number.

In general, the characteristic polynomial f_X contains a little more information than the conjugacy class of the q-Weil number π_X. For instance, π_{X^n} gives the same conjugacy class as π_X for all $n \geqslant 1$, whereas $f_{X^n} = f_X^n$. But for a simple abelian variety X over $\mathbb{F}_q$ we can recover f_X from π_X, as we have $f_X = h^i$ with $h = f_{\mathbb{Q}}^{\pi_X}$ the minimum polynomial of π_X over $\mathbb{Q}$ and i the index of the division algebra $\mathrm{End}^0(X)$, which is determined by the conjugacy class of π_X via the method described in (16.36). Combined with the equivalence (a) $\Leftrightarrow$ (d) in Corollary (16.25) we obtain the following lemma.

qWeilConjug **(16.40) Lemma.** *Let X and Y be simple abelian varieties over a finite field $\mathbb{F}_q$. Then X and Y are isogenous if and only if the associated q-Weil numbers π_X and π_Y are conjugate.*

Miraculously, every q-Weil number occurs, up to conjugation, as the Frobenius of a simple abelian variety over $\mathbb{F}_q$, as a result of Honda asserts. Combination with the Theorem of Tate gives the following description of the isogeny classes of simple abelian varieties over $\mathbb{F}_q$.

HondaTate **(16.41) Theorem of Honda-Tate.** *Let q be a power of a prime number. For every q-Weil number π there exists a simple abelian variety X over $\mathbb{F}_q$ such that π_X is conjugate to π. Furthermore, we have a bijection*

$$\left\{\begin{matrix}\text{isogeny classes of simple}\\ \text{abelian varieties over } \mathbb{F}_q\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix}\text{conjugacy classes}\\ \text{of } q\text{-Weil numbers}\end{matrix}\right\}$$

given by $X \mapsto \pi_X$.

The inverse of the map $X \mapsto \pi_X$ associates to a q-Weil number π a simple abelian variety X such that f_X is a power of the minimum polynomial $f_{\mathbb{Q}}^{\pi}$ of π over $\mathbb{Q}$. In general there may be no abelian variety with characteristic polynomial $f_{\mathbb{Q}}^{\pi}$; see ?? below.

The injectivity of the map $X \mapsto \pi_X$ is a consequence of Tate's Theorem (16.20); see Lemma (16.40). The proof of surjectivity is based on an explicit knowledge of the reduction modulo primes of special abelian varieties—namely abelian varieties of CM-type—defined over a number field. It is done in three steps: (i) We show that π is a q-Weil number if and only if π^N is a q^N-Weil number for some N. (ii) We already know how to reconstruct the division algebra $D = \mathrm{End}^0(X)$ from π. Then we choose a CM-field L that splits D and construct a complex abelian variety of CM-type by L, show that it is defined over a number field, and calculate the Frobenius of its reduction modulo a prime. (iii) We show that by choosing the CM-type appropriately we get as Frobenius a power of π.

We now carry out the details.

Weilres **(16.42) Lemma.** *Let k' be a extension field of $k \cong \mathbb{F}_q$ of degree N, and let X' be a simple abelian variety over k'. If $X = \mathrm{Res}_{k'/k}(X')$ is the Weil restriction of X' to k then $f_X(T) = f_{X'}(T^N)$. In particular, the q^N-Weil numbers $\pi_{X'}$ and π_X^N are conjugate.*

Proof. The Tate module $T_\ell(X)$ is the induced module from $\mathrm{Gal}(\overline{k}/k')$ to $\mathrm{Gal}(\overline{k}/k)$ of $T_\ell(X')$ from which the formula results immediately. □

piN **(16.43) Corollary.** *If π is a q-Weil number such that π^N is conjugate to the Frobenius of a*

simple abelian variety over $\mathbb{F}_{q^N}$ then π is conjugate to the Frobenius of a simple abelian variety over $\mathbb{F}_q$.

Proof. If X' is a simple abelian variety over $\mathbb{F}_{q^N}$ whose Frobenius $\pi_{X'}$ is conjugate to π^N, let $X := \mathrm{Res}_{k'/k}(X')$, which is an abelian variety (not simple in general) over $\mathbb{F}_q$. By Lemma (16.42) π is a root of f_X and is therefore conjugate to the Frobenius of a k-simple factor of X. □

CMsplit **(16.44) Proposition.** *Let π be a Weil q-number, $F = \mathbb{Q}(\pi)$ and E the division algebra which is non-split at the real places of F, split at the complex places and the places not above p and with $q^{-\mathrm{inv_v}(E)} \equiv \|\pi\|_v \pmod 1$ for places above p. Then there exists a CM-field L containing F such that L splits E and $[L : F] = [E : F]^{1/2}$.*

Proof. We know that either F is totally real, and then $F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{p})$ and $[E : F]^{1/2} = 2$, or F is a CM-field with totally real subfield $F_0 = \mathbb{Q}(\pi + q/\pi)$.

i) Suppose that F is totally real. Then we take $L = F(\sqrt{-p})$. This is a CM-field and E splits over L as the invariant is multiplied by $2 = [L : F]$.

ii) Let $d = [E : F]^{1/2}$. We take for L_0 a totally real field which is an extension of degree d of F_0 and such that for every place v_0 of L_0 above p the local degree is d; see Exercise ?? for the construction. Then $L = FL_0$ is a CM-field and under the extension the invariant is multiplied by the local degree $[L_{v'} : F_v] = [L_0 : F_0]d$, thus killing it. Hence E is split at all places over p. □

Given a Weil q-number π with $F = \mathbb{Q}(\pi)$ and E a division algebra associated to π (unique up to isomorphism) we choose a CM-field L that splits E. Recall that an abelian variety X over a field K is called of CM-type L if we have an embedding $L \to \mathrm{End}^0_K(X)$ with $2\dim(X) = [L : \mathbb{Q}]$.

CMgivespi **(16.45) Proposition.** *There exists an abelian scheme $\mathcal{X}$ defined over the ring of integers of a finite extension K of $\mathbb{Q}_p$ whose generic fibre is of CM-type L and such that the Frobenius of the special fibre is conjugate to a power π^N of π.*

Proof. To construct X we have to specify the way L acts on the tangent space at the origin. If C is a field of characteristic 0 and ρ is complex conjugation on L then we choose a CM-type, i.e., a subset Φ of $\mathrm{Hom}_{\mathbb{Q}-\mathrm{alg}}(L, C)$ such that $\Phi \cup \Phi\rho = \mathrm{Hom}_{\mathbb{Q}-\mathrm{alg}}(L, C)$ and $\Phi \cap \Phi\rho = \emptyset$. An abelian scheme $\mathcal{X}$ defined over $\mathrm{Spec}(R)$ with $R \subset C$ is called of type (L, Φ) if the generic fibre X is of type L and the representation of L on the tangent space of X at the origin decomposes as the sum $\sum_{\varphi\in\Phi} \varphi$ of characters. By ?? (referentie voor CM AV) we know that there exists an abelian scheme of type (L, Φ) defined over the ring of integers of a number field in C.

We now take for C an algebraic closure of $\mathbb{Q}_p$. We decompose $\mathbb{Q}_p \otimes L = \prod_{w|p} L_w$, with L_w the completion of L at the place w. Let $\Sigma_w = \mathrm{Hom}_{\mathbb{Q}_p}(L_w, C)$ and we identify Σ_w with its image in $\mathrm{Hom}(L, C)$ and then have $\mathrm{Hom}(L, C) = \cup_{w|p}\Sigma_w$. It will now turn out that the reduction of an abelian scheme of type (L, Φ) up to isogeny is determined by the way the embeddings $\varphi \in \Phi$ are distributed over the Σ_w. We set $\Phi_w = \Phi \cap \Sigma_w$ and have $\Phi = \cup_{w|p}\Phi_w$. ¿From (referentie voor berekening p-deelbare groep) we derive:

Redmodp **(16.46) Lemma.** *Let $\mathcal{X}$ be an abelian scheme of type (L, Φ) defined over the ring of integers O_K of a finite extension field K of $\mathbb{Q}_p$. Let k_0 be the residue field of O_K with $q_0 = \#k_0$ and let $X_{/k_0} = \mathcal{X} \otimes k_0$. Then the Frobenius π_{X/k_0} can be identified with an element $\pi_0 \in L \subset \mathrm{End}^0_{k_0}(X_{/k_0})$ and*

$$\frac{w(\pi_0)}{w(q_0)} = \frac{\#\Phi_w}{\#\Sigma_w}$$

for every place w over p.

Now given π, and hence F and E and a CM-field L that splits E we are still free to choose the CM-type Φ. We claim that we can choose Φ in such a way that for every place $w|p$ of L we have

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#\Sigma_w}.$$

To see this, let us denote by v the place of F underlying w and put

$$n_w = \frac{w(\pi_0)}{w(q_0)}\#\Sigma_w = \frac{w(\pi_0)}{w(q_0)}[L_w : \mathbb{Q}_p] = \frac{w(\pi_0)}{w(q_0)}[L_w : F_v][F_v : \mathbb{Q}_p].$$

Then $n_w = \mathrm{inv}_w(E \otimes_F L)\ (\mathrm{mod}\ \mathbb{Z})$ is an integer since L splits E and obviously $n_w \geqslant 0$. Moreover from the identity $\pi\overline{\pi} = q$ we have $n_w + n_{\rho w} = \#\Sigma_w = \#\Sigma_{\rho w}$. We now define a CM-type Φ by choosing disjoint subsets Φ_w of cardinality n_w such that $\Phi = \cup_w \Phi_w$ satisfying $\Phi \cup \rho\Phi = \Sigma$ and $\Phi \cap \rho\Phi = \emptyset$. Then automatically we have $w(\pi)/w(q) = \#\Phi_w/\#\Sigma_w$. By Lemma 16.46 we obtain an abelian variety defined over a finite field k_0 whose Frobenius is conjugate to an element π_0 of L with $w(\pi_0)/w(q_0) = \#\Phi_w/\#\Sigma_w$. The following Lemma finishes the proof of the Honda-Tate Theorem.

Weilqnulq **(16.47) Lemma.** *Given a Weil q-number π and a Weil q_0-number π_0 in L with $w(\pi)/w(q) = w(\pi_0)/w(q_0)$ for all places $w|p$. Then there exists positive integers N and N_0 such that $\pi^N = \pi_0^{N_0}$.*

Proof. After replacing π and π_0 by suitable powers we may assume that $q = q_0$ and hence that $w(q) = w(q_0)$ for all $w|p$. At the other places π and π_0 are units since $\pi\overline{\pi} = \pi_0\overline{\pi}_0 = q$. And at the infinite place both π and π_0 have absolute value $q^{1/2}$. Therefore, π/π_0 has absolute value 1 at every place of L, so π/π_0 is a root of unity. □

ExaHT **(16.48) Example.** Let $q = p^m$ and suppose that n and n' are integers with $0 \leqslant n < n'$, g.c.d.$(n, n') = 1$ and $n + n' = m$. Then there exists a simple abelian variety X of dimension m defined over $\mathbb{F}_q$ such that π is a root of $\pi^2 + p^n\pi + p^m$, cf. Example ('ExaEndFF'), 3).

The results of the preceding sections give a complete description of the isogeny classes of simple abelian varieties over a given finite field k of cardinality q, via the Weil q-numbers, and a description of their endomorphism algebras. This leads to two questions: i) Which rings occur as the endomorphism rings of a simple abelian variety over k? ii) What are the isomorphism classes of (polarized) abelian varieties defined over k contained in a given isogeny class of abelian varieties over k? Unfortunately, we have only very partial answers to these questions. They connect with very interesting research on Shimura varieties. For elliptic curves and for ordinary varieties over the prime field we have a satisfactory description. We shall indicate these results.

We first need some notions from algebra. Let A be an algebra over $\mathbb{Q}$ with identity element 1. Then by a lattice we mean a free $\mathbb{Z}$-module in A whose rank is equal to $\dim_{\mathbb{Q}} A$. A subring $R \subset A$ is called an order if it contains 1 and a lattice. If $\Lambda \subset A$ is a lattice in A then we define the left (resp. right) order of Λ as $\{a \in A\colon a\,\Lambda \subset \Lambda\}$ (resp. $\{a \in A\colon \Lambda\, a \subset \Lambda\}$). These are examples of orders in A.

Note that every element of an order is integral over $\mathbb{Z}$, because....

If X is an abelian variety of dimension g over a finite field k then $R = \mathrm{End}_k(X)$ is an order in the algebra $E = \mathrm{End}_k^0(X)$. It has the following special property.

pi+q/pi **(16.49) Lemma.** *For an abelian variety X over a finite field $\mathbb{F}_q$ the endomorphism ring $\mathrm{End}_k(X)$ is an order containing π and q/π.*

Proof. Recall that $\pi \in \mathrm{End}_k(X)$ is the 'mth power' of relative Frobenius $F = F_X$. Similarly, the relation $FV = VF = p$ implies that similarly q/π is the m-th power of Verschiebung, see 5.20, hence is contained in $\mathrm{End}_k(X)$. □

If X is a simple abelian variety over k with Weil q-number π_X then its isogeny class is determined by the pair $(\mathrm{End}_k^0(X), \pi_X)$ and we may identify $\mathrm{End}_k^0(X)$ with a given division algebra E such that π_X corresponds to an element $\pi \in E$. Any two such identifications coincide on the center $\mathbb{Q}(\pi)$, hence by the Skolem-Noether theorem (see ??) they differ by an inner automorphism of E. In particular, the endomorphism ring of X is determined in E up to conjugation. But if we specify the action of E on the Tate module $V_\ell(X)$ then by 16.20 we can retrieve $\mathrm{End}_k(X)$ inside the algebra E by the conditions that

$$\mathrm{End}_k(X) \otimes \mathbb{Z}_l = \{a \in E\colon T_\ell(a)T_\ell(X) \subseteq T_\ell(X)\} \tag{1}$$

and

$$\mathrm{End}_k(X) \otimes \mathbb{Z}_p = \{a \in E\colon aX[p^\infty] \subseteq X[p^\infty]\} \tag{1'}$$

since a lattice is determined by its localizations.

The endomorphism ring with the element π determines the isogeny class in the following precise sense.

IsomEnd **(16.50) Lemma.** *Let X and Y be abelian varieties over k. If $\alpha\colon \mathrm{End}_k(Y) \cong \mathrm{End}_k(X)$ is an isomorphism sending π_Y to π_X then there is an isogeny $X \to Y$ inducing the isomorphism $\mathrm{End}_k(Y) \cong \mathrm{End}_k(X)$.*

Proof. Since the characteristic polynomials are equal it follows from Theorem '`TateCor2`' that X and Y are isogenous. Let $\varphi\colon X \to Y$ be an isogeny inducing an algebra isomorphism $\varphi^*\colon \mathrm{End}_k^0(Y) \cong \mathrm{End}_k^0(X)$. By Skolem-Noether this algebra isomorphism differs from the one induced by α by an inner automorphism of $\mathrm{End}_k^0(Y)$ of the form $x \mapsto \rho x \rho^{-1}$ with $\rho \in \mathrm{End}_k^0$

and by multiplying it with a sufficiently large integer we may assume that ρ is an isogeny of Y. Composing φ with this ρ gives the desired isomorphism. □

Homfunctor **(16.51)** Let G be a commutative group scheme defined over k with an action of the ring R. For any finitely generated left R-module M we can define a functor on k-algebras by $A \mapsto \mathrm{Hom}_R(M, G(A))$. This functor is representable, because a resolution $R^a \to R^b \to M \to 0$ gives rise to an exact sequence $0 \to \mathrm{Hom}_R(M, G(A)) \to G(A)^b \to G(A)^a$ by which we can identify this functor with the kernel of $G^b \to G^a$. Thus $\mathrm{Hom}_R(M, G)$ is a commutative group scheme. The functor $M \mapsto \mathrm{Hom}_R(M, G)$ is a left-exact additive functor from the category of finitely generated left R-modules to commutative group schemes.

If R is an order in an algebra E then by a left R-ideal in E we mean a left R-submodule of E which contains a lattice. The condition that a left R-module I in E contains a lattice is equivalent to the fact that I contains an isogeny and is automatically fulfilled if X is simple and $I \neq (0)$. Let X be an abelian variety with endomorphism ring $\mathrm{End}_k(X) = R$ and let I be a left R-ideal. By applying $\mathrm{Hom}_R(-, X)$ to the short exact sequence $0 \to I \to R \to R/I \to 0$ we find a long exact sequence that begins like this

$$0 \to \mathrm{Hom}_R(R/I, X) \to X \to \mathrm{Hom}_R(I, X) \to \mathrm{Ext}^1_R(R/I, X) \to 0, \tag{2}$$

where the last term is $\mathrm{Ext}^1_R(R, X) = (0)$ because R is projective, see Atiyah and Macdonald 1.

R-occur **(16.52) Definition.** Let X be an abelian variety with $R = \mathrm{End}_k(X)$ and let I be a left R-ideal in R. We define $H(X, I) := \mathrm{Hom}_R(R/I, X)$ and we view it via the exact sequence (2) as a finite subgroup scheme of X. Moreover, we put $X_I := X/H(X, I)$. This is an abelian variety defined over k and isogenous to X.

The following lemma provides alternative descriptions of X_I.

kernel **(16.53) Lemma.** *Let $\varphi\colon X \to X_I$ be the canonical map.*

i) We have $H(X, I) = \cap_{\alpha \in I} X[\alpha]$ with $X[\alpha] = \ker(\alpha)$.

ii) If $\alpha_1, \ldots, \alpha_r$ generate of I then X_I is isomorphic to the image of $(\alpha_1, \ldots, \alpha_r) : X \to X^r$.

iii) For $l \neq p$ we have

$$T_\ell(\varphi)^{-1} T_\ell(X_I) = \cap_{\alpha \in I} T_\ell(\alpha)^{-1} T_\ell(X)$$

iv) The dual of $T_\ell(\varphi)^{-1} T_\ell(X_I)$ in $T_\ell(X)^\vee$ is $I\, T_\ell(X)^\vee$.

v) For the Dieudonné modules we have

$$\varphi_p M(X_I[p^\infty]) = \sum_{\alpha \in I} \alpha_p M(X[p^\infty]).$$

Proof. If $R^n \to R \to R/I \to 0$ is a resolution and $r_1, \ldots, r_n$ are the corresponding generators of I then we get $\mathrm{Hom}_R(R/I, X) = \ker\{(r_1, \ldots, r_n) : X \to X^n\}$ and the statements i) and ii) become clear. The other statements are a direct consequence of this, use 10.6. □

The Lemma makes it possible to describe the lattice $\mathrm{End}_k(X_I)$ in E via these local conditions iii) and v) using the conditions (1) and (1').

Note that by assumption R/I is finite, and if N annihilates R/I then N also annihilates $\mathrm{Ext}^1_R(R/I, X)$. Thus by the exact sequence (2) the abelian variety X_I is the connected component of $\mathrm{Hom}_R(I, X)$. If I and J are isomorphic as left R-modules, then the isomorphism extends to an isomorphism of E which by Skolem-Noether is scalar multiplication, $I = J\lambda$, i.e., I and J

belong to the same ideal class of R. By the definition of X_I a R-isomorphism between I and J implies that X_I and X_J are isomorphic. But the converse need not hold. It holds if we impose an extra condition on the ideals.

kerideal **(16.54) Definition.** A left ideal I of $R = \mathrm{End}_k(X)$ is called a *kernel ideal* if I is the annihilator of the subgroup scheme $H(X, I)$, that is, if $I = \{\alpha \in R\colon \alpha H(X, I) = 0\}$. The ideal $J = \{\alpha \in R\colon \alpha H(X, I) = 0\}$ with $J = H(X, J)$ is called the kernel ideal associated to I.

ExaKerId **(16.55)** Examples of kernel ideals. i) A principal ideal $R\lambda$ is a kernel ideal. Any $\alpha \in R$ that vanishes on $H(X, I) = \ker(\lambda)$ factors as $\alpha = \beta\,\lambda$ for some $\beta \in R$. ii) If I is a kernel ideal then so is $I\lambda$ for any isogeny λ. To see this, consider an element α that annihilates $H(X, I\lambda)$. Then it annihilates $\ker(\lambda)$, in particular it annihilates $H(X, R\lambda)$ and since by i) the ideal $R\lambda$ is a kernel ideal it follows that $\alpha \in R\lambda$, say $\alpha = \beta\lambda$. Since α annihilates $H(X, I\lambda)$ we have that $H(X, I\lambda) \subset \ker \beta\lambda$. Since λ is an isogeny and thus surjective this implies that β annihilates $H(X, I)$ i.e., $\beta \in I$ and thus $\alpha \in I\lambda$. □

EndChange **(16.56) Lemma.** *Let X be a simple abelian variety over a finite field k with $R = \mathrm{End}_k(X)$ and let I be a left R-ideal. Then $\mathrm{End}_k(X_I)$ contains the right order of I and equals it if I is a kernel ideal.*

Proof. Let $\varphi\colon X \to X_I$ be the canonical map. An element ρ in the right order of I has the property that ρ preserves $T_\ell(\varphi)^{-1}T_\ell(X_I) = \cap_{\alpha\in I}\alpha^{-1}T_\ell(X)$and similarly $\sum_{\alpha\in I}\alpha M(X[p^\infty])$,hence belongs to $\mathrm{End}_k(X_I)$. Suppose that β is an elementpreserving these lattices. Then $J = I + I\beta$ is a left ideal of R and we have $H(X, I) = H(X, J)$. This shows that if I is a kernel ideal we have $I = H(X, J) = J$. □

action **(16.57) Proposition.** *Let I and J be kernel ideals of $\mathrm{End}_k(X)$. Then $X_I \cong X_J$ if and only if $I = J\lambda$ for some invertible $\lambda \in \mathrm{End}_k^0(X)$.*

Proof. We already remarked above that $X_I \cong X_J$ if $I = J\lambda$. It remains to show that an isomorphism $X_I \cong X_J$ implies that $I = J\lambda$ for an invertible element of E. By Exercise 16.15 there exists an isogeny $\rho \in R$ such that $\rho^{-1}(H(X, I)) = N_X^{-1}(H(X, J))$. Note that $\rho^{-1}(H(X, I)) = H(X, I\rho)$ and $N_X^{-1}(H(X, J)) = H(X, JN)$. By 16.55 both $I\rho$ and IN are kernel ideals, and as annihilator of the same subgroup scheme $H(X, I\rho) = H(X, JN)$ the ideals $I\rho$ and JN are equal. We find $I = JN\rho^{-1}$. □

maxRoccur **(16.58) Proposition.** *Let X be an abelian variety over a finite field k with endomorphism algebra E. Then every maximal order in E occurs as an endomorphism ring of an abelian variety in the isogeny class of X. Moreover, if $R = \mathrm{End}_k(X)$ is a maximal order then so is $\mathrm{End}_k(X_I)$ for any left R-ideal I.*

Proof. We claim that $\mathrm{End}_k(X_I)$ contains the right order of I. Indeed, if $\alpha \in I$ and j is in the right order of I then $\alpha j \in I$ and one checks that j maps $T_\ell(X_I)$ and $M(X_I[p^\infty])$ to itself.

Let S be a maximal order of E. Then a multiple $N \cdot S$ is contained in R for some $N \in \mathbb{Z}_{\geqslant 1}$. Let I be the left ideal generated by $N \cdot S$. Its right order contains S, therefore the endomorphism ring of X_I contains S and equals S since S is maximal.

By Deuring 2, p. 75 (???) or Reiner 1, (21.2) the right order of a left ideal of a maximal order is maximal. □

rkH(X,I) **(16.59) Proposition.** *Let X be a simple abelian variety over a finite field k whose endomorphism ring $R = \mathrm{End}_k(X)$ is a maximal order in $E = \mathrm{End}_k^0(X)$. Then $\mathrm{rank}H(X, I) = N(I)$, the reduced norm of I in E and every left ideal I of R is a kernel ideal.*

Proof. If $I = R\lambda$ is a principal ideal then $\mathrm{rank}H(X,I) = \mathrm{rank}X[\lambda] = \deg\lambda$ and we know by (ref naar End hfdstk) that $\deg\lambda = N(R\lambda)$. Given an arbitrary left ideal I we let R' be its right order. Then there exists a left R'-ideal J such that $IJ = R\lambda$, see (Deuring [2], p. 106 ???). Moreover, we may choose $N(J)$ prime to $\mathrm{rank}H(X,I)$. We then have $N(I)N(J) = N(R\lambda) = \deg\lambda$. The reader may check in Exercise 16.10 that $\mathrm{rank}H(X,IJ) = \mathrm{rank}H(X,I)\mathrm{rank}H(X_I,J)$. Thus we find that $\mathrm{rank}H(X,I)$ divides $N(I)$. Applying the same reasoning to J we find that $\mathrm{rank}H(X,J)$ divides $N(J)$. Together this shows that $\mathrm{rank}H(X,I) = N(I)$.

Finally, if I' is the kernel ideal associated to I then $I' \supseteq I$ and we have $\mathrm{rank}H(X,I) = N(I')$, thus $N(I') = N(I)$ and it follows that $I = I'$. □

notXI **(16.60) Remark.** Let X be an elliptic curve over $k = \mathbb{F}_q$ with $R = \mathrm{End}_k(X)$ the ring of integers of an imaginary quadratic field in which p is inert. Then X and $X^{(p)}$ are isogenous via F_X but $X^{(p)}$ is not of the form X_I for an ideal I of R. Every ideal is a kernel ideal, but there is no ideal I with $H(X,I) = \ker(F_X)$.

ordsimple **(16.61) Proposition.** *Let X be an ordinary simple abelian variety over a finite field k. Then $R = \mathrm{End}_k(X)$ is commutative. If moreover $\mathrm{End}_k(X)$ is a maximal order in the fraction field of R then the set of k-isomorphism classes of abelian varieties in the isogeny class of X with endomorphism ring R is a torsor over $\mathrm{Pic}(R)$.*

Proof. By '`ExaEndFF`' we know that $E = \mathrm{End}^0(X)$ has no real primes and by '`EndFF`' the invariant of E is 0 or $\mathrm{ord}_v(q)$ above p and zero for the other finite places, hence is an integer. It follows that $E = F$ is commutative. If R is a maximal order then by 16.57 the class group of R acts. We need to see that there is one orbit. By the theory of the canonical lift we have for each X a canonical lift and isogenies lift also. The lattice of a lift is a projective R-module of rank 1. This gives the bijection. □

§7. *Elliptic curves.*

We now illustrate the concepts from the earlier sections in the case of elliptic curves. Let X be an elliptic curve defined over a finite field k of characteristic p. Then multiplication by p factors as

$$X \xrightarrow{F_X} X^{(p)} \xrightarrow{V} X$$

We now have two possibilities: i) V is separable; ii) V is inseparable. In the first case X is called ordinary and in the second case supersingular. In the supersingular case we see that $V = F_{X^{(p)}}$ since both have the same kernel, the unique α_p in $X^{(p)}[p]$. We also see then that p_X gives a k-isomorphism $X \cong X^{(p^2)}$, i.e. the j-invariant satisfies $j^{p^2} = j$ and then $j \in \mathbb{F}_{p^2}$. For convenience we give a number of characterizations of ordinary elliptic curves.

ordchar **(16.62) Proposition.** *Let X be an elliptic curve over a finite field $k = \mathbb{F}_q$ with $R = \mathrm{End}_k(X)$ and $\#X(\mathbb{F}_q) = q + 1 - t$. Then the following are equivalent:*

i) X is ordinary;
ii) X has p-rank 1, i.e., $\#X[p](\overline{k}) = p$;
iii) $t \not\equiv 0 \pmod p$;
iv) $F = \mathbb{Q}(\pi)$ is an imaginary quadratic field and p splits in F.

Proof. i) ⇒ ii). Since V is étale the group scheme $\ker(V) \subset X[p]/\ker(F_X)$ is an étale group

scheme and by $VF_X = p_X$ it follows that it is of order p. ii) $\Rightarrow$ iii) We have $\#X(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \overline{\alpha}^n$ (with α and $\overline{\alpha}$ the roots of f_X) and for suitable n this is divisible by p. Since $\alpha\overline{\alpha} = q$ it follows that $\alpha^n + \overline{\alpha}^n \equiv \alpha + \overline{\alpha} \,(\mathrm{mod} p)$ and that $t = \alpha + \overline{\alpha}$ is prime to p. iii) $\Rightarrow$ iv). The discriminant $\Delta = t^2 - 4q$ of F is < 0 and a square mod p. iv) $\Rightarrow$ i) If $p = \wp\wp'$ in the ring of integers of F then $\pi = \wp^n \wp'^{n'}$ with $n + n' = m$. Then by Theorem '`EndFF`' the invariants of $\mathrm{End}_k^0(X)$ at $\wp$ and $\wp'$ are n/m and n'/m with $n + n' = m$ and by '`pidim`' we have either $n = 0$ or $n' = 0$. Suppose that $\pi = \wp^m$. Look at the isogeny $X \to X_{\wp'}$. This is a separable isogeny of degree p because its kernel is different from the connected kernel of $X \to X_\wp$, hence $\ker p_X$ is not connected. □

`IsogEC` We now consider isogeny classes of elliptic curves. Isogeny classes of elliptic curves are described by their Weil q-number π with $\pi^2 - t\,\pi + q = 0$, hence by the trace of Frobenius $t = q + 1 - \#X(\mathbb{F}_q)$. The following result of Deuring describes all t that occur.

`t-occur` **(16.64) Theorem.** *The integer t occurs as the trace of an elliptic curve defined over $\mathbb{F}_q$ with $q = p^m$ if and only if t is one of the following:*

i) t is prime to p and $t^2 \leqslant 4q$;

ii) If m is odd then a) $t = 0$; b) $t = \pm\sqrt{2q}$ and $p = 2$; c) $t = \pm\sqrt{3q}$ and $p = 3$;

iii) If m is even then a) $t = \pm 2\sqrt{q}$; b) $t = \pm\sqrt{q}$ and $p \not\equiv 1 (\mathrm{mod}\ 3)$; c) $t = 0$ and $p \not\equiv 1 (\mathrm{mod}\ 4)$.

Proof. We have to check which Weil q-numbers π with $\pi^2 - t\pi + q = 0$ give rise to elliptic curves. If $\pi \in \mathbb{Q}$, then in view of $t^2 - 4q \leqslant 0$ the discriminant vanishes and $f_X = (T \pm \sqrt{q})^2$ with and m necessarily even. We get $t = \pm 2\sqrt{q}$ and m even, the case iii a).

So assume now $F \neq \mathbb{Q}$. Then F is an imaginary quadratic field and $f_X = T^2 - tT + q$ with $t^2 < 4q$. We have to check when this gives an elliptic curve. The condition is (cf. '`pidim`') that $m = \mathrm{ord}(P_\nu(0))$ for the p-adic factors $P_\nu \in \mathbb{Q}_p[T]$.

If $p = \wp\wp'$ splits in F then $\pi = \wp^n \wp'^{n'}$ with $n + n' = m$ and the invariants at $\wp$ and $\wp'$ of E are n/m and n'/m. In order to get an elliptic curve we need $n = 0$ or $n' = 0$. This is equivalent to the condition that $t = \pi + \overline{\pi}$ is prime to p. This gives case i).

If p does not split in F then f_X remains irreducible in $\mathbb{Q}_p[T]$. Then there is a unique place $v|p$ and since $\pi\overline{\pi} = q$ we have $\mathrm{ord}_v(\pi) = (1/2)\mathrm{ord}(q)$. It follows that $\pi/\sqrt{q}$ has absolute value 1 at all embeddings, hence is a root of unity in an imaginary quadratic field, hence of order dividing 4 or 6. The reader may now check using Exercises 16.7, 16.8 that the cases listed give exactly all the possibilities. □

We illustrate this by a little table listing the isomorphism classes of elliptic curves defined over $k = \mathbb{F}_3$. The elliptic curve is given as $y^2 = f(x)$. We also give the j-invariant.

f	t	$1/\#\mathrm{Aut}_k(X)$	j	π
$x^3 + x^2 + 1$	-2	$1/2$	-1	$-1 \pm \sqrt{-2}$
$x^3 + x^2 - 1$	1	$1/2$	1	$(1 \pm \sqrt{-11})/2$
$x^3 - x^2 + 1$	-1	$1/2$	1	$(-1 \pm \sqrt{-11})/2$
$x^3 - x^2 - 1$	2	$1/2$	-1	$1 \pm \sqrt{-2}$
$x^3 + x$	0	$1/2$	0	$\pm\sqrt{-3}$
$x^3 - x$	0	$1/6$	0	$\pm\sqrt{-3}$
$x^3 - x + 1$	-3	$1/6$	0	$(-3 \pm \sqrt{-3})/2$
$x^3 - x - 1$	3	$1/6$	0	$(3 \pm \sqrt{-3})/2$

We also give a table for the field $k = \mathbb{F}_9$ listing the possible traces t and the frequencies

with which these occur, where we define the frequency as $\sum_{[X]} 1/\#\mathrm{Aut}_{\mathbb{F}_9}(X)$ with the sum over all the $\mathbb{F}_9$-isomorphism classes of elliptic curves defined over $\mathbb{F}_9$ with the given trace.

t	0	±1	±2	±3	±4	±5	±6
$\sum 1/\#\mathrm{Aut}_{\mathbb{F}_9}$	1/2	1	3/2	1/6	1	1/2	1/12

alg-occur Let E be the endomorphism algebra of an isogeny class of elliptic curves defined over $\mathbb{F}_q$ with corresponding Weil q-number π and field $F = \mathbb{Q}(\pi)$. If $F = \mathbb{Q}$ then $t = \pm 2\sqrt{q}$, the elliptic curve X is supersingular and by '`ExaEndFF`' we have $E = D_p$, the unique division quaternion algebra over $\mathbb{Q}$ ramified at p and at ∞. If $F \neq \mathbb{Q}$ then F is an imaginary quadratic field $\mathbb{Q}(\sqrt{t^2 - 4q})$ and by '`TateCor4`' and '`TateCor5`' we have $E = F$. The curve X can be ordinary or supersingular depending on whether $t \equiv 0 \pmod p$ or not. We now determine the possible endomorphism rings.

Orders in a quadratic number field K are special. They are completely determined by their disriminant $\Delta = Dc^2$, where c^2 is the largest square such that $D = \Delta/c^2 \equiv 0, 1 (\mathrm{mod} 4)$. Then D is the discriminant of K and the (positive) integer c, the conductor, is the index of the order in the ring of integers of the number field. To such an order R we can associate its class group $\mathrm{Pic}(R)$ of isomorphism classes of projective modules of rank 1 or invertible ideals in K. We write $h(R)$ for the class number $\#\mathrm{Pic}(R)$.

order-occur **(16.66) Theorem.** *Let X be an elliptic curve over a finite field k with $E = \mathrm{End}^0(X)$ and Weil number π. If $F = \mathbb{Q}(\pi)$ then the following orders occur as endomorphism ring of an elliptic curve defined over k in the isogeny class of X:*

(i) ordinary case $E = F$: every order containing π;

ii) supersingular case with $E = D_p$: every maximal order;

iii) supersingular case with $E = F$: every order containing π whose conductor is prime to p.

Proof. i) If X is ordinary with endomorphism algebra E then $\mathbb{Z}[\pi]$ is maximal at p since the derivative of f_X at π is $2\pi - b$ and this is prime to p. Let now R be an arbitrary order containing π. Then possibly $R \neq \mathrm{End}_k(X)$, but then there are only finitely many primes $l \neq p$, say $l_1, \ldots, l_r$ such that $R_l \neq \mathrm{End}_k(X)_l$. Choose a lattice L_1 in $V_{l_1}(X)$ that contains $T_{l_1}(X)$ and which has order R_{l_1}. Such a lattice exists since $V_\ell(X)$ is free of rank 1 over F_l. Since R contains π this lattice is Galois invariant. We take X_1 to be the quotient of X by the finite subgroup $L_1/T_{l_1}(X)$. Then we have $T_\ell(X) = T_l(X_1)$ for all $l \neq l_1$ and $\mathrm{End}_k(X_1) = R_{l_1}$.Repeating this procedure gives us an elliptic curve with endomorphism ring R.

(ii) If R is an order in a finite dimensional $\mathbb{Q}$-algebra E then R is maximal if and only if $R \otimes \mathbb{Z}_p$ is maximal in $E \otimes \mathbb{Q}_p$ for all prime numbers p; see Reiner 1, (11.2). Now assume that X is supersingular and $E = D_p$ is non-commutative. For all $\ell \neq p$ we have $E \otimes \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$ and R is conjugate to $M_2(\mathbb{Z}_\ell)$, hence maximal at $l \neq p$. We now look at the case $l = p$. By 16.58 we know that the maximal order occurs for an elliptic curve defined over $\mathbb{F}_q$ contained in the isogeny class. Since we only look at $l = p$ we may restrict ourselves to p-order isogenies defined over k. These can be factored as a composition of Frobenii F. If we apply a k-isogeny $F^r : X \to X^{(p^r)}$ then F^r induces an isomorphism on the endomorphism rings via $\alpha \mapsto \alpha^{(p^r)}$. This implies the maximality at p.

iii) At $l \neq p$ the argument of i) shows that we can get any order in this isogeny class. Consider now the case $l = p$. After a quadratic extension of the base field we get $E = D_p$ and the order is maximal. At p the algebra D_p remains a division algebra and as such has a unique maximal order containing all integral elements. This order intersects any subfield in its maximal

order. Clearly this intersection is $\mathrm{End}_{\mathbb{F}_q}(X)$. □

We illustrate the theorem by listing representatives $y^2 = f(x)$ for the isomorphism classes of elliptic curves defined over $\mathbb{F}_7$ with the corresponding Weil 7-numbers and their endomorphism rings with the conductor c. Note that R need not be equal to $\mathbb{Z}[\pi]$.

f	t	$1/\#\mathrm{Aut}_k(X)$	j	π	c	$h(R)$
x^3+1	-4	$1/6$	0	$-2\pm\sqrt{-3}$	1	1
x^3+2	-1	$1/6$	0	$(-1\pm 3\sqrt{-3})/2$	1	1
x^3+3	-5	$1/6$	0	$(-5\pm\sqrt{-3})/2$	1	1
x^3+4	5	$1/6$	0	$(5\pm\sqrt{-3})/2$	1	1
x^3+5	1	$1/6$	0	$(1\pm 3\sqrt{-3})/2$	1	1
x^3+6	4	$1/6$	0	$2\pm\sqrt{-3}$	1	1
x^3+x	0	$1/2$	6	$\pm\sqrt{-7}$	2	1
x^3+x+1	3	$1/2$	1	$(3\pm\sqrt{-19})/2$	1	1
x^3+x+3	2	$1/2$	5	$1\pm\sqrt{-6}$	1	2
x^3+x+4	-2	$1/2$	5	$-1\pm\sqrt{-6}$	1	2
x^3+x+6	-3	$1/2$	1	$(-3\pm\sqrt{-19})/2$	1	1
x^3+3x	0	$1/2$	6	$\pm\sqrt{-7}$	1	1
x^3+3x+1	-4	$1/2$	2	$(-2\pm\sqrt{-3})$	2	1
x^3+3x+2	-1	$1/2$	3	$(-1\pm 3\sqrt{-3})/2$	3	1
x^3+3x+3	2	$1/2$	4	$1\pm\sqrt{-6}$	1	2
x^3+3x+4	-2	$1/2$	4	$-1\pm\sqrt{-6}$	1	2
x^3+3x+5	1	$1/2$	3	$(1\pm 3\sqrt{-3})/2$	3	1
x^3+3x+6	4	$1/2$	2	$-2\pm\sqrt{-3}$	2	1

classgr **(16.67) Proposition.** *Let X be an elliptic curve over a finite field k with $R = \mathrm{End}_k(X)$. Then every non-zero left R-ideal is a kernel ideal for every elliptic curve Y with $\mathrm{End}_k(Y) \cong R$.*

Proof. If R is non-commutative then R is a maximal order and by 16.59 every left R-ideal is a kernel ideal. So assume now that R is commutative. Then R is an order in an imaginary quadratic field and the ideals of R with order R are exactly the invertible ideals. Consider for a left ideal I the canonical map $\varphi\colon X \to X_I$. For $l \neq p$ the dual of $T_\ell(\varphi)^{-1}(T_\ell(X))$ is $I\,T_\ell(X)^\vee$ and the l-part of $H(X,I)$ is given by $T_\ell(X)^\vee / I\,T_\ell(X)^\vee$. But $T_\ell(X)^\vee$ is free of rank 1 over R_l and therefore at l the ideals I and the annihilator of $H(X,I)$ coincide. At p the order R is maximal, and the Dieudonné module is a sum of free modules.

EllEnd **(16.68) Theorem.** *Let X be an elliptic curve X defined over $k = \mathbb{F}_q$ with $R = \mathrm{End}_k(X)$ and $E = \mathrm{End}_k^0(X)$. Let $I(X,R)$ be the set of k-isomorphism classes of elliptic curves over k contained in the k-isogeny class of X with endomorphism ring R.*

i) If X is ordinary then $I(X,R)$ is a torsor over the ideal class of R.

ii) If X is supersingular and $E = F$ is commutative then the ideal class group of R acts freely on $I(X,R)$ with 2 orbits if p is inert in R and 1 orbit else.

iii) If X is supersingular and $E = D_p$ is non-commutative then $\#I(X,R)$ is 1 or 2. It equals 1 if and only if the prime ideal over p in R is principal.

Proof. i) Using the construction $X \mapsto X_I$ we see that the ideal class group of R acts freely. We need to see that there is one orbit. One way to see this is to use the canonical lift. The canonical lift of an elliptic curve Y in $I(X)$ is a complex elliptic curve with endomorphism ring R. By the theory of complex multiplication we know that these are in $1-1$ correspondence with the class

group of R; for each such curve the lattice is a projectice R-module of rank 1. Alternatively, if $X \to X/G$ is an isogeny of X and $X/G \to X$ the dual map then $T_\ell(X/G)$ corresponds to a sublattice of $T_\ell(X)$. One now checks that every lattice comes from an ideal.

ii) If X is supersingular with $E = F$ commutative then the class group acts freely on the set of elliptic curves in this isogeny class with endomorphism ring R. If $X \to Y$ is a separable isogeny then I claim that $Y = X_I$ for some invertible ideal I. Indeed, at $l \neq p$ the isogeny is given by an overlattice of $T_\ell(X)$, or dually by a sublattice of the dual $T_\ell(X)^\vee$. But sincethe dual is free of rank 1 over R_l the sublattice is of the form $I_l T_\ell(X)^\vee$ for some local ideal I_l. At p it suffices to consider inseparable isogenies and these are compositionsof Frobenii. Note that p ramifies or is inert. If $(p) = \wp^2$ then$X^{(p)} = X_\wp$ and we find just one orbit. If p is inert,then there is no I such $X^{(p)} = X_I$, hence there are exactly 2 orbits. iii) Finally, suppose that E is non-commutative. We must show that there is one orbit. Note that R is maximal. Let Y be an elliptic curve with $\mathrm{End}_k(Y) = R$. This induces by 16.50 an isogeny of X with Y given by the ideal $I = R\varphi$. By 16.56 this ideal is a two-sided ideal. Two-sided ideal in R are classified, see Deuring [1], p. 263 (???). They are of the form nR or $n\wp$ with $\wp^2 = (p)$. These represent one class if and only if $\wp$ is principal. □

counting **(16.69)** This theorem makes it possible to count the number $N(t)$ of isomorphism classes of elliptic curves defined over $k = \mathbb{F}_q$ contained in a fixed isogeny class given by t. For example, if $t \not\equiv 0(\mathrm{mod}p)$ and $t^2 < 4q$ then $N(t) = \sum_R h(R)$, where the sum is over the orders R with $\mathbb{Z}[\pi] \subseteq R \subseteq O_F$ with O_F the ring of integers of the imaginary quadratic field $F = \mathbb{Q}(\pi)$. See Exercise 16.11 for the precise formulas, and see also Schoof [1]. Actually, always in mathematics it is better to count the objects with their natural weight which is 1 over the order of the automorphism group of the object. In the case at hand, we have to count an elliptic curve X with a weight equal to $1/\#\mathrm{Aut}_k(X)$. Therefore, we introduce a modified class number, the Hurwitz-Kronecker class number.

Hurwitz-K **(16.70) Definition.** The Hurwitz-Kronecker class number $H(\Delta)$ is the number of $\mathrm{SL}(2,\mathbb{Z})$-equivalence classes of positive binary integral quadratic forms $\varphi = aX^2 + bXY + cY^2$ with discriminant $-\Delta$, each class $[\varphi]$ being counted with weight $2/\#\mathrm{Aut}(\varphi)$, with $\mathrm{Aut}(\varphi)$ the group of orientation preserving automorphisms of φ. Equivalently, we let $H(\Delta) = \sum_{c \in \mathbb{Z}_{geq1}} \hat{h}(-\Delta/c^2)$ with $\hat{h}(N)$ the class number of the order R with discriminant N divided by $2/\#\mathrm{Aut}(R)$. Furthermore, we set $H(0) = -1/12$.

We give a small table illustrating the Hurwitz-Kronecker class number.

n	0	3	4	7	8	11	12	15	16	19
$H(n)$	$-1/12$	$1/3$	$1/2$	1	1	1	$4/3$	2	$3/2$	1

ClassNumber **(16.71) Proposition.** *Let t be an integer with $t^2 < 4q$ and $t \not\equiv 0(\mathrm{mod}p)$. The number of isomorphism classes of elliptic curves X defined over $\mathbb{F}_q$ weighted with $1/\#\mathrm{Aut}_{\mathbb{F}_q}(X)$ with trace of Frobenius t equals $(1/2)\,H(4q - t^2)$, where $H(\Delta)$ is the Hurwitz-Kronecker class number of discriminant Δ.*

Proof. Let t be a number prime to p occurring as the trace of Frobenius of an elliptic curve X over $\mathbb{F}_q$. Then each elliptic curve over $\mathbb{F}_q$ in the isogeny class of X can be lifted canonically and after choosing an embedding $W(\mathbb{F}_q)$ into $\mathbb{C}$ we get a complex elliptic curve and an associated lattice with $\mathrm{End}_k(X)$ as endomorphism ring. In particular, each automorphism can be lifted too. We thus find a bijection between the isomorphism classes containedin the isogeny class and

isomorphism classes of End_k-lattices. □

The reader will notice that the weights of all elliptic curves with the same j-invariant add up to 1. This is an instance of the following phenomenon.

massofgerb **(16.72) Theorem.** *Let Y be a variety defined over the finite field k such that its absolute automorphism group $\mathrm{Aut}_{\overline{k}}(Y)$ is finite. Then we have the formula:*

$$\sum_{Y'} \frac{1}{\#\mathrm{Aut}_k(Y')} = 1,$$

where the sum is over representatives Y' of the k-isomorphism classes contained in the $\overline{k}$-isomorphism class of Y.

Proof. If $\alpha : Y \to Y'$ is an $\overline{k}$-isomorphism and $\gamma \in G = \mathrm{Gal}(\overline{k}/k)$ then $\alpha^{-1} \cdot \alpha^\gamma$ is an $\overline{k}$-automorphism of Y. The map which associates to $\gamma \in G$ the automorphism $a_\gamma = \alpha^{-1} \cdot \alpha^\gamma$ defines a cocycle on G with values in the (possibly non-abelian) group $A = \mathrm{Aut}_{\overline{k}}(Y)$, that is, we have the relation $a_{\gamma\delta} = a_\gamma \cdot a_\delta^\gamma$. It is well-known that this gives a bijection between the set of k-isomorphism classes contained in the $\overline{k}$-isomorphism class of Y and the cohomology set $H^1(G, A)$. Since G is essentially cyclic, in the sense that G is topologically generated by the Frobenius element we can use continuous cohomology. Therefore, a cocycle $\gamma \mapsto a_\gamma \in Z^1(G, A)$ is given by the image of F, i.e., it is determined by giving an (arbitrary) element of A.Two cohomologous cycles thus correspond to elements that differ by the actionof A on itself given by $a \mapsto \varepsilon^{-1} \cdot a \cdot \varepsilon^F$ for $\varepsilon \in A$. The orbits correspond to the cohomology classes in $H^1(G, A)$.The stabilizer of an element a_F is in $1-1$-correspondence with the set$\mathrm{Aut}_k(Y')$. Indeed, we have a bijection $\mathrm{Aut}_{\overline{k}}(Y) \longleftrightarrow \mathrm{Aut}_{\overline{k}}(Y')$ via $\rho \mapsto \sigma = \alpha \cdot \rho \cdot \alpha^{-1}$, where α: $Y \to Y'$ is a $\overline{k}$-isomorphism of Y with Y'. So we get

$$\rho^{-1} a_F \rho^F = \rho^{-1}\alpha^{-1}\alpha^F\rho^F = \alpha^{-1}\sigma^{-1}\sigma^F\alpha^F$$

and this equals $a_F = \alpha^{-1}\alpha^F$ if and only if $\sigma^F = \sigma$, i.e., $\sigma \in \mathrm{Aut}_{\overline{k}}(Y')$. Counting the orbits now gives

$$\#A = \sum_{Y'} \frac{\#A}{\#\mathrm{Aut}_k(Y')},$$

and by division by $\#A$ the desired formula $\sum_{Y'} 1/\#\mathrm{Aut}_k(Y') = 1$. □

Applic **(16.73)** Counting the number of abelian varieties over a finite field of cardinality q can be used to obtain information about automorphic forms. We give a simple example. For a pair of integers (t, n) we define $P_k(t, n)$ for positive even k as the coefficient of x^{k-2} in the power series development of $(1 - tx + nx^2)^{-1}$. Equivalently, if we factor this quadratic polynomial $(1 - tx + nx^2) = (1 - \rho x)(1 - \overline{\rho} x)$ then

$$P_k(t, n) = \frac{\rho^{k-1} - \overline{\rho}^{k-1}}{\rho - \overline{\rho}}.$$

and equals the trace of the $k-2$th symmetric power of $\mathrm{diag}(\rho, \overline{\rho})$.

One place where the class numbers that we met naturally occur is the trace formulafor the action of the Hecke operators on the space of modular forms on $\mathrm{SL}(2, \mathbb{Z})$. The following theorem and an elementary proof can be found in 2.

TraceHecke **(16.74) Theorem.** *Let $k \geqslant 4$ be an even integer and n a positive integer. Then the trace of the Hecke operator $T(n)$ on the space S_k of cusp forms of weight k on $\mathrm{SL}(2,\mathbb{Z})$ is given by*

$$\mathrm{Tr}T(n) = -\frac{1}{2}\sum_{t\in\mathbb{Z}} P_k(t,n)H(4n-t^2) - \frac{1}{2}\sum_{dd'=n}\min(d,d')^{k-1}.$$

Using 16.68 and 16.71 we can rewrite this now purely in terms of elliptic curves over finite fields.

LocalSystem **(16.75) Theorem.** *Let p be a prime. The trace of the Hecke operator $T(p)$ on the space of cusp forms of even weight $k \in 2\mathbb{Z}$ with $k \geqslant 4$ on $\mathrm{SL}(2,\mathbb{Z})$ is given by*

$$\mathrm{Tr}T(p) + 1 = \sum_{E/\mathbb{F}_p,\,\text{up to}\,\cong_{\mathbb{F}_p}} \frac{-\mathrm{TrSym}^{k-2}(T_\ell(\pi))}{\#\mathrm{Aut}_{\mathbb{F}_p}(E)},$$

where the sum is over the $\mathbb{F}_p$-isomorphism classes of elliptic curves defined over $\mathbb{F}_p$.

Example. We have $P_{12}(t,p) = -p^5 + 15\,p^4t^2 - 35\,p^3t^4 + 28\,p^2t^6 - 9\,pt^8 + t^{10}$. Noting that $P_{12}(t,p) = P_{12}(-t,p)$ and $P_{12}(2,3) = -263$, $P_{12}(1,3) = 253$ and $P_{12}(0,3) = P_{12}(3,3) = -243$ and using the table we get $\mathrm{Tr}T(3) = 252$ for $k = 12$. This fits since $\tau(3) = 252$ is the third Fourier coefficient of the generator $\Delta = \sum_{n=1}^{\infty}\tau(n)q^n$ of S_{12}.

One should see this formula as an instance of a Lefschetz trace formula. The trace on cohomology is calculated by counting fixed points of Frobenius. ...

§8. *Newton polygons of abelian varieties over finite fields.*

Given an abelian variety X over a finite field $\mathbb{F}_q$ with $q = p^m$ we can look at the Newton polygon of the characteristic polynomial $f_X = T^{2g} + \ldots + p^{mg} = \prod_{i=1}^{2g}(T - \alpha_i)$ of Frobenius. To interpret this geometrically we consider the Witt ring $W(\mathbb{F}_q) = \mathbb{Z}_p(\zeta_{q-1})$ (=unique complete discrete valuation ring which is absolutely unramified and has $\mathbb{F}_q$ as its residue field). Suppose the α_i lie in a ring $W(\mathbb{F}_q)[p^{1/e}]$ for some $e \geqslant 1$. We write

$$\mathrm{ord}(\alpha_i) = mc_i \quad \text{with } 0 \leqslant c_i \leqslant 1.$$

Moreover, we set

$$r_c = \#\{\alpha_i\colon \mathrm{ord}(\alpha_i) = c\} \qquad \text{and } n_c = cr_c, m_c = r_c - n_c.$$

The the following theorem of Manin (cf [Ma]) explain the geometric significance of the numbers c_i :

ManinThm **(16.76) Theorem.** *The formal group of the abelian variety A is of the form*

$$r_0G_{1,0} + \sum_{0<c<\frac{1}{2}}(G_{n_c,m_c} + G_{m_c,n_c}) + \tfrac{1}{2}r_{\frac{1}{2}}G_{1,1}.$$

Example. (cf [Ta]) Let $q = p^m$ and choose integers n and n' with $0 \leqslant n < n'$ and $m = n + n'$. Let π be a root of $\pi^2 + p^n\pi + p^m = 0$. Then π is a imaginary quadratic Weil number with respect to q and p splits as $p = \wp\wp'$ in $\mathbb{Q}(\pi)$. A corresponding abelian variety A (by (11.16) has dimension m and the invariants of E^0 are n/m and n'/m. One can show that A remains simple over $\overline{\mathbb{F}}_q$. We find that the formal group is $G_{n,n'} \times G_{n',n}$. The formal group $G_{1,1}$ can be obtained from the Weil number $\sqrt{-p}$. (So all these formal groups are *algebraic*.)

§9. *Ordinary abelian varieties over a finite field.*

Recall the definition of 'ordinary abelian variety'.

OrdAVFF **(16.77) Definition-Proposition.** *An abelian variety X of dimension g defined over a finite field k of characteristic p is called ordinary if one of the following equivalent conditions is fulfilled.*

i) The p-rank of X is g, i.e., $\#X[p](\overline{k}) = p^g$.
ii) Verschiebung V: $X^{(p)} \to X$ is an étale map.
iii) The induced action F^*: $H^1(X^{(p)}, O_{X^{(p)}}) \to H^1(X, O_X)$ is invertible.
iv) $\ker(F)$ is a multiplicative group scheme.
v) Half of the $2g$ roots of the characteristic polynomial f_X of Frobenius π are p-adic units.

If one looks at the Newton polygon of the characteristic polynomial f_X then on the one end of the spectre one finds the supersingular abelian varieties and at the other end the ordinary abelian varieties. These abelian varieties show the strongest resemblance to abelian varieties in characteristic zero. For example, the endomorphism rings of simple ordinary abelian varieties similar to those of complex abelian varieties.

EndOrdAV **(16.78) Proposition.** *Let X be a simple ordinary abelian variety over a finite field k with corresponding Weil number π. Then $F = \mathbb{Q}(\pi)$ has no real primes and $\mathrm{End}_k^0(X) = F$ is commutative. Moreover, f_X is irreducible.*

Proof. As we saw in '`ExaEndFF`' the occurrence of a real prime of F implies that X is a supersingular elliptic curve or an abelian surface that over a quadratic extension k' of k becomes a power of a supersingular elliptic curve over k'. Therefore F is a CM-field. By $\pi\overline{\pi} = q$ we see that in $\|\pi\|_v = q^{-i_v}$ the exponent i_v is an integer for all $v|p$. By Theorem '`EndFF`' it follows that $\mathrm{End}_k(X) = F$, hence is commutative. The irreducibility of f_X follows immediately. □

If X is an ordinary abelian variety of dimension g over the finite field k then the Tate module $T_p(X) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, X(\overline{k}))$ is non-canonically isomorphic to $\mathbb{Z}_p^g$. We shall denote it here by $T_p'(X)$ and we use the notation $T_p''(X)$ for the dual of $T_p'(X^t)$, i.e.,

$$T_p''(X) := \mathrm{Hom}_{\mathbb{Z}_p}(T_p'(X^t), T_p(\mathbb{G}_m)),$$

where we may write $\mathbb{Z}_p(1)$ for the Tate module of the multiplicative group $\mathbb{G}_m$. We thus obtain two free rank g lattices over $\mathbb{Z}_p$ associated to X. We put $V_p'(X) = T_p'(X) \otimes \mathbb{Q}_p$ and $V_p'' = T_p''(X) \otimes \mathbb{Q}_p$.

Ordinary abelian varieties can be lifted in a canonical way to characteristic zero. Indeed, recall there is a general Serre-Tate theorem which says the following.

Let R be any artinian local ring with algebraically closed residue field $\overline{k}$ of characteristic p. Then the functor

$$\{\text{abelian schemes over } R\} \longrightarrow$$

$$\longrightarrow \{ \text{ ab. schemes over } \overline{k} \text{ plus lifting of their } p-\text{divisible groups to } R\}$$

given by

$$X/R \mapsto (X \otimes_R \overline{k}, X[p^\infty])$$

is an equivalence of categories, see [ ]. So to lift an abelian variety $X/\overline{k}$ to R we must lift its p-divisible group. For an ordinary abelian variety the p-divisible group is canonically a product

$$X[p^\infty] = \hat{X} \times (T_p(X) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p)) \tag{14}$$

of its connected and étale part. We can lift both factors separately:

$$\hat{X} = (\mu_{p^\infty})^g, \quad T_p(X) = (\mathbb{Q}_p/\mathbb{Z}_p)^g$$

and take the product again. A general lift of (*) will combine both factors, more precisely, given a lift of (14) we find a pairing

$$\hat{X} \times T_p(X^t) \to \hat{\mathbb{G}}_m.$$

For an ordinary abelian variety X the canonical lift $\hat{X}$ is the unique lift to the Witt ring $W = W(\overline{k})$ such that each endomorphism of X lifts to an endomorphism of $\hat{X}$.

OrdAIsog **(16.79) Lemma.** *Let X be an ordinary abelian variety over $\overline{k}$. Then the finite subgroup schemes of X are in $1-1$ correspondence with the sublattices $R \subset \Lambda(X)$ such that*

$$R \otimes \mathbb{Z}_p = ((R \otimes \mathbb{Z}_p) \cap V_p' + ((R \otimes \mathbb{Z}_p) \cap V_p'').$$

In particular, $\ker(F)$ *corresponds to the sublattice $\Lambda^{(p)}$ of $\Lambda(X)$ which is p-isogenous to Λ and satisfies ..*

Using this Deligne has given a characterization of the category of ordinary abelian varieties over $\mathbb{F}_q$. Let φ: $W \to \mathbb{C}$ be a chosen embedding.

OrdinaryFF **(16.80) Theorem.** *The functor $X \mapsto (\Lambda(X), F)$, with $\Lambda(X) = H_1(\hat{A} \otimes_\varphi \mathbb{C}, \mathbb{Z})$ and F the endomorphism induced by Frobenius on $\Lambda(X)$, is an equivalence of categories between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category of free $\mathbb{Z}$-modules of finite type satisfying the following conditions*

i) F is semi-simple with eigen values of absolute value $q^{1/2}$,

ii) There is a decomposition $\Lambda(X) \otimes \mathbb{Z}_p = T_p' \oplus T_p''$ of $\mathbb{Z}_p[F]$-modules of the same dimension such that $F|T_p'$ is invertible, while $F|T_p''$ is divisible by q.

Proof. If X is an abelian variety over $k = \mathbb{F}_q$ then the operator F on $\Lambda(X)$ is semi-simple and has eigenvalues of absolute value $q^{1/2}$ by the Hasse-Weil Theorem '`Hasse-Weil`'.

We now first show that the functor is fully faithful, i.e., that for two abelian varieties X_1 and X_2 defined over k the natural map

$$\psi\colon \mathrm{Hom}_k(X_1, X_2) \to \mathrm{Hom}_F(\Lambda(X_1), \Lambda(X_2))$$

is an isomorphism. After tensoring with $\mathbb{Z}_l$ we obtain a map

$$\psi_l\colon \mathrm{Hom}_k(X_1, X_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}_F(\Lambda(X_1), \Lambda(X_2)) \otimes \mathbb{Z}_l,$$

and the latter RHS can be identified with $\mathrm{Hom}_F(T_\ell(X_1), T_\ell(X_2))$.By Tate's Theorem 16.20 it follows that $\psi_l \otimes \mathbb{Q}$is an isomorphism for $l \neq p$. Since $\mathrm{Hom}_k(X_1, X_2)$ is torsion-free we conclude that ψ is injective. We shall show that the co-kernel of ψ is torsion-free by showing that if φ: $X_1 \to X_2$ is a homomorphism such that the induced map Λ_φ: $\Lambda(X_1) \to \Lambda(X_2)$ is divisible by a natural number n then φ is also divisible by n in $\mathrm{End}_k(X_1, X_2)$. If Λ_φ is disible by n then the induced map on the canonical lifts $(X_{i\,/\overline{k}})_{\mathbb{C}}$ is also divisible by n, hence also the induced map $\tilde{\varphi}$ between the corresponding generic fibres of the p-divisible groups $X_i[p^\infty]$. But the kernel of multiplication by n is a flat group scheme over the Witt ring $W(\overline{k})$ it follows that $\tilde{\varphi}$ is also divisible by n, and so is φ. This proves that the functor is fully faithful.

The functor Λ induces a functor $\Lambda_{\mathbb{Q}}$ from the category of abelian varieties over k up to isogeny to the category $\mathcal{V}$ of $\mathbb{Q}$-vector spaces of finite dimension with a semi-simple operator F such that its eigenvalues are of absolute value $q^{1/2}$ and half of these are p-adic units. Now then Theorem of Honda and Tate 16.41 shows that $\Lambda_{\mathbb{Q}}$ is essentially surjective: if (V, F) is a simple object in the category $\mathcal{V}$ then there exists an abelian variety X over k such that the characteristic polynomial F_X of Frobenius is a power of that of F. Clearly, X is ordinary then and $(\Lambda(X) \otimes \mathbb{Q}, F)$ is a sum of copies of (V, F). The fact that our functor is fully faithful now implies X is up to isogeny a power of an abelian variety Y defined over k with $(\Lambda(Y) \otimes \mathbb{Q}, F) = (V, F)$.

Exercises.

Ex:ZetaCurve **(16.1)** Let C be a smooth irreducible projective curve defined over a finite field k. Prove the identity of formal series

$$\exp\left[\sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n})\frac{t^n}{n}\right] = \sum_{n=0}^{\infty} D_n t^n,$$

with D_n the number of effective divisors of degree n on C which are defined over k.

Ex:Ihara **(16.2)** Let C be a smooth irreducible projective curve defined over a finite field $\mathbb{F}_q$. Use $\#C(\mathbb{F}_q) \leqslant \#C(\mathbb{F}_{q^2})$ and Cauchy-Schwartz for the roots α_i of $f_{\mathrm{Jac}(C)}$ to prove that

$$\#C(\mathbb{F}_q) \leqslant q + 1 = \left[\left(\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g\right)/2\right].$$

Conclude that for $g > (q - \sqrt{q})/2$ this is a better bound than the Hasse-Weil bound.

Ex:EndSSEll **(16.3)** Let X be a supersingular elliptic curve defined over the prime field $\mathbb{F}_p$. Prove that $\mathrm{End}(X) \neq \mathrm{End}(X_{\overline{\mathbb{F}}_p})$.

Ex:QlImrho **(16.4)** Let X be an abelian variety over a finite field k. Let ℓ be a prime number, $\ell \neq \mathrm{char}(k)$, and consider the ℓ-adic representation ρ_ℓ: $\mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}(V_\ell X)$.

(i) Show that the map ρ_ℓ is continuous, where we give the Galois group the Krull topology and $\mathrm{GL}(V_\ell X)$ the ℓ-adic topology.

(ii) Show that $\mathrm{Im}(\rho_\ell)$ is the closure of the subgroup $\langle \pi_X \rangle \subset \mathrm{GL}(V_\ell X)$ generated by π_X.

(iii) Show that $\mathbb{Q}_\ell\big[\mathrm{Im}(\rho_\ell)\big]$, the $\mathbb{Q}_\ell$-subalgebra of $\mathrm{End}(V_\ell X)$ generated by the image of ρ_ℓ, equals $\mathbb{Q}_\ell[\pi_X]$, the subalgebra generated by $V_\ell(\pi_X)$.

Ex:IrrCrit **(16.5)** Let X be a simple abelian variety with characteristic polynomial f_X. Prove that the following are equivalent.

(i) f_X is irreducible.

(ii) F has no real primes and for all $v|p$ we have $\mathrm{inv}_v(E) = 0$ in $\mathbb{Q}/\mathbb{Z}$.
(iii) $\mathrm{End}_k^0(X)$ is commutative.

Ex:qWeilnr **(16.6)** Prove the assertion stated in ('qWeilnrs'): An algebraic integer $\pi \in \overline{\mathbb{Q}}$ is a q-Weil number if and only if either $q = \pm\sqrt{q}$ or π is a root of $T^2 - aT + q$ where a is an algebraic integer such that $\mathbb{Q}[a]$ is a totally real field in which $a^2 - 4q$ is totally negative.

Ex:QuadrFields1 **(16.7)** Let $q = p^m$ be an odd power of a prime, $b \in \mathbb{Z}$ with $b^2 - 4q < 0$ and $F = \mathbb{Q}(\sqrt{b^2 - 4q})$. Prove that p ramifies or splits in F. Prove moreover that p ramifies if and only if i) $b = 0$ or ii) $b = \pm p^{(m+1)/2}$ and $p = 2$ or 3.

Ex:QuadrFields2 **(16.8)** Let $q = p^m$ be an even power of a prime, $b \in \mathbb{Z}$ with $b^2 - 4q < 0$ and $F = \mathbb{Q}(\sqrt{b^2 - 4q})$.
1) Prove that p stays prime if and only if i) $b = 0$ and $p \equiv 3 \pmod 4$, or ii) $b = \pm\sqrt{q}$ and $p \equiv 2 \pmod 3$.
ii) Prove that p ramifies if and only if i) $b = 0$ and $p = 2$, or ii) $b = \sqrt{q}$ and $p = 3$.

Ex:pimacht=p **(16.9)** Let π be the Weil q-number of an elliptic curve X over $\mathbb{F}_q$. Show that some power of π is equal to a power of p if and only if X is supersingular.

Ex:IJ **(16.10)** Let X be an abelian variety over a finite field k, and let $R := \mathrm{End}(X)$. Let I be a left ideal of finite index of R and let J be a left ideal of finite index in $\mathrm{End}(X_I)$. Prove that we may view IJ as a left ideal of R and that $X_{IJ} \cong (X_I)_J$ canonically.

Ex:Schoof **(16.11)** Let $t \in \mathbb{Z}$ and let $N(q,t)$ be the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with trace of Frobenius t (equivalently with $\#X(\mathbb{F}_q) = q+1-t$). Define a class number by $H'(\Delta) = \sum_d h(\Delta/d^2)$, where the sum is over $d \in \mathbb{Z}_{>0}$ such that Δ/d^2 is integral and $\equiv 0$ or $1 \bmod 4$). Prove the following formulas for $N(q,t)$.
i) $N(q,t) = H'(t^2 - 4q)$ if $t \not\equiv 0 (\mathrm{mod} p)$.
ii) $N(q,0) = H'(-4p)$ if q is a not a square.
iii) $N(q,0) = 1 - (\frac{-4}{p})$ if q is a square.
iii) $N(q, \pm\sqrt{p\,q}) = 1$ if $p = 2$ or $p = 3$ and q is not a square.
iv) $N(q, \pm\sqrt{q}) = 1 - (\frac{-3}{p})$ if q is a square.
v) $N(q, \pm 2\sqrt{q}) = \frac{1}{12}\left(p + 6 - 4(\frac{-3}{p}) - 3(\frac{-4}{p})\right)$ if q is a square.
vi) $N(q,t) = 0$ otherwise.

Ex:q **(16.12)** 1) Show that $\sum_{[X]} 1/\#\mathrm{Aut}_{\mathbb{F}_q}(X) = q$, where the sum is over all $\mathbb{F}_q$-isomorphism classes of elliptic curves defined over $\mathbb{F}_q$. 2) Let p be a prime. Prove the Hurwitz class number relation $\sum_t H(4p - t^2) = 2p$, where the sum is over all $t \in \mathbb{Z}$ with $t^2 < 4p$ and $4p - t^2 \equiv 0 (\mathrm{mod} p)$.

Ex:Trace(Tp2) **(16.13)** Prove the following formula for the trace of the Hecke operator on the space of cusp forms of even weight $k \geqslant 4$ on $\mathrm{SL}(2,\mathbb{Z})$.

$$\mathrm{Tr}T(p^2) + p^{k-1} = \sum_{X/\mathbb{F}_{p^2}, \text{ up to } \cong_{\mathbb{F}_{p^2}}} \frac{-\mathrm{TrSym}^{k-2}(T_\ell(\pi))}{\#\mathrm{Aut}_{\mathbb{F}_{p^2}}(X)},$$

where the sum is over the $\mathbb{F}_{p^2}$-isomorphism classes of elliptic curves X defined over $\mathbb{F}_{p^2}$.

Ex:F49 **(16.14)** Check the following table of frequencies for elliptic curves over $\mathbb{F}_{49}$. Here the frequency $f(t)$ is defined as $f(t) = \sum_{[X]} 1/\#\mathrm{Aut}_{\mathbb{F}_{49}}(X)$ with the sum over all $[X]$ with $\#X(\mathbb{F}_{49}) = 50 - t$ for $k = \mathbb{F}_{49}$.

t	0	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10	±11	±12	±13
f	1/2	2	11/3	1	3	5/2	3	2	1	3	7/6	1	2/3	1/4

exercise for endo-chapter

Ex:G1G2 **(16.15)** Let X be an abelian variety defined over a field k and let G_1 and G_2 be two finite subgroup schemes of X defined over k. Suppose that $X/G_1 \cong X/G_2$. Prove that there exists an isogeny $\rho \in \mathrm{End}_k(X)$ of X and an integer $N \in \mathbb{Z}_{\geqslant 1}$ such that $\rho^{-1}(G_1) = N_X^{-1}(G_2)$.

Notes. Although Galois introduced finite fields in the 1830's it took a long time time before curves and abelian varieties over finite fields were seriously studied. Artin in his 1924 thesis considered the zeta function for hyperelliptic curves over a finite field $\mathbb{F}_q$, defined by an Euler product as an analogue of the Dedekind zeta function for number fields and proved that after the substitution $t = q^{-s}$ one obtains a rational function $Z_C(t)$ which satisfies a functional equation. Artin formulated an analogue of the Riemann hypothesis, namely that the zeros of $Z_C(t)$ have absolute value $q^{-1/2}$. In 1931 F.K. Schmidt reformulated $Z_C(t)$ as the generating series as in '`GenSer`' and deduced the functional equation from the Riemann-Roch theorem. Around 1932 Hasse observed the Riemann hypothesis proposed by Artin implies a bound on $\#C(\mathbb{F}_q)$. Two years later he proved that bound for elliptic curves making use of correspondences and endomorphisms. Deuring observed that in order to extend Hasse's proof to higher genus one needed a theory of correspondences in arbitrary characteristic. Weil developed such a theory and proved the Riemann hypothesis of Artin in 1940 by deducing it from an inequality on correspondences (the positivity of the trace) due to Castelnuovo and Severi. These results inspired Weil later to make his famous conjectures about the zeta function of a complete smooth variety over a finite field.

An elementary proof of the Hasse-Weil Theorem for curves bound using only Riemann-Roch was given much later by Stepanov, see Bombieri 1. Serre's improvement of the Hasse-Weil bound in Serre 5 stems from 1983. Improvements of the Hasse-Weil bound for curves in case g is large with respect to q are due to Ihara and Drinfeld and Vladuts, see Exercise 16.2 and Vladuts and Drinfeld [1].

The central theorem relating homomorphisms of abelian varieties to the Galois-equivariant homomorphisms between their Tate modules is due to Tate [1], who in his proof generalized an argument of Deuring following a suggestion by Lichtenbaum. The extension to the case $l = p$ was promised in an Inventiones paper, toujours a paraitre. A proof was given in Milne and Waterhouse [1]. They also wrote down Tate's proof for the invariants of the endomorphism ring in the Brauer group which Tate indicated in Tate [1]. Honda proved in Honda [1] that every Weil q-number occurs as the conjugate of Frobenius for a simple abelian variety over $\mathbb{F}_q$. Together with Tate's theorem it put the isogeny classes of abelian varieties over $\mathbb{F}_q$ in bijection with the Weil q-numbers.

Deuring classified the endomorphism rings of elliptic curves in Deuring 1 but he looked at $\mathrm{End}_{\overline{k}}(X)$. Waterhouse extended some of Deuring's results to higher dimension in 1. The construction of abelian varieties isogenous to a given one by using ideals of the endomorphism ring is due to Shimura and Taniyama 1. Serre gave a different interpretation of it in 3 and 4.

The description of the category of ordinary abelian varieties over a finite field given above is due to Deligne 2.

opp
irr
sim
sem
sim
sem

References are given at the end of the appendix.

RingsGeneral **(A.1)** All rings considered here are assumed to have an identity element, and homomorphisms $f\colon R_1 \to R_2$ are required to send $1 \in R_1$ to $1 \in R_2$.

As we shall consider noncommutative rings, we need to distinguish between left and right modules. We adopt the convention that "module" means "left module", unless we explicitely call it a right module. Note, however, that unless stated otherwise, by an ideal in a ring we shall mean a two-sided ideal.

If A is a ring then $A^{\rm opp}$ denotes the opposite ring and $Z(A)$ denotes the center of A. Further, for a nonnegative integer r we denote by $M_r(A)$ the ring of $r \times r$ matrices with coefficients in A.

Let A be a ring, M a left A-module. We say that M is an *irreducible* (or *simple*) A-module if $M \neq \{0\}$ and M has no A-submodules other than $\{0\}$ and M. We say that M is a semisimple A-module if every A-submodule of M is a direct summand. This is equivalent to the condition that M is a direct sum of a collection of simple A-modules. Note that the zero module is semisimple but not simple; by convention it is the direct sum of the empty collection of A-modules.

A nonzero ring A is called *simple* (as a ring) if $\{0\}$ and A are the only two-sided ideals in A. A ring A is called *semisimple* if every left A-module is semisimple. This is equivalent to the condition that A is semisimple as a left module over itself. A semisimple ring A has finitely many minimal nonzero ideals; call these $A_1, \ldots, A_r$. Each A_i, viewed as a ring, has an identity element making it a simple ring, and A is isomorphic to the product $A_1 \times \cdots \times A_r$. So every semisimple ring is a product of finitely many simple rings. Conversely, every finite product of simple rings is semisimple.

If A is a semisimple ring then every left ideal $I \subset A$ (resp. right ideal $J \subset A$) is generated by an idempotent, i.e., there is an idempotent $e \in A$ with $I = Ae$ (resp. $J = eA$). Indeed, because A is semisimple as a left (resp. right) module over itself there exists a left ideal I' (resp. right ideal J') such that $A = I \oplus I'$ as left A-modules (resp. $A = J \oplus J'$ as right A-modules); writing $1 = e + e'$ one easily finds that e is an idempotent and $I = Ae$ (resp. $J = eA$).

If A is a simple ring then up to isomorphism there is a unique simple A-module. It follows from the previous that over a semisimple ring there are finitely many simple modules, up to isomorphism; one corresponding to each simple factor A_i.

Let A be a simple ring, M a simple A-module. Then A, viewed as a left module over itself, is of finite length r; hence it is isomorphic to M^r. The ring $D := \mathrm{End}_A(M)^{\rm opp}$ is a division algebra and M has dimension r as a right module over D. For $a \in A$ write $a_M \in \mathrm{End}_D(M)$ for the map $m \mapsto am$. By the Bicommutant Theorem, see (A.2) below, the homomorphism $a \mapsto a_M$ gives an isomorphism of the ring A with the ring $\mathrm{End}_D(M)$, and the latter ring is isomorphic to the ring $M_r(D)$ of $r \times r$ matrices over D. So the conclusion is that every simple ring A is isomorphic to a matrix ring over a division algebra. In particular, $Z(A) = Z(D)$ is a field.

Conversely, if D is a division algebra and r is a positive integer, $M_r(D)$ is a simple ring. The unique simple module over this ring is given by D^r with its natural structure of a left $M_r(D)$-module.

It follows from the previous results that if A is a simple ring, so is A^{opp}.

BicommThm **(A.2) Bicommutant Theorem.** *Let A be a semisimple ring, and let M be an A-module of finite type. Let $C := \mathrm{End}_A(M)$, and consider M as a left module over C by the rule $c \cdot m = c(m)$ for $c \in C$ and $m \in M$. Then the map $A \to \mathrm{End}_C(M)$ that sends $a \in A$ to the map $a_M \in \mathrm{End}_C(M)$ given by $m \mapsto am$ is an isomorphism.*

SkolNoeth **(A.3) Skolem-Noether Theorem.** *Let A be a simple algebra with center K. Let B and B' be simple K-subalgebras of A of finite dimension over K. Then for every isomorphism $\varphi\colon B \xrightarrow{\sim} B'$ of K-algebras there is an inner automorphism ψ of A with $\varphi = \psi_{|B}$.*

In particular, if A is a simple algebra of finite dimension over its centre K then all automorphisms of A over K are inner, so $\mathrm{Aut}_K(A) = \mathrm{Inn}(A) \cong A^*/K^*$.

BrauerGr **(A.4)** Let K be a field. By a K-algebra we mean a ring A together with a homomorphism $K \to Z(A)$, called the structural homomorphism. A K-algebra A is called a *central simple algebra over K* if A is a simple ring and the structure homomorphism $K \to Z(A)$ is an isomorphism. As we have seen, any such A is of the form $M_r(D)$ for some division algebra D with center K.

Let D be a division algebra with center K such that $\dim_K(D) < \infty$. If $K \subset \overline{K}$ is an algebraic closure of K then $\overline{K} \otimes_K D \cong M_n(\overline{K})$ for some $n \in \mathbb{N}$. It follows that any central simple K-algebra A of finite K-dimension is a K-form of a matrix algebra; by this we mean that $\overline{K} \otimes_K A$ is isomorphic to a matrix algebra $M_m(\overline{K})$ over $\overline{K}$. In particular, $\dim_K(A) = m^2$ is a square. The integer m is called the *degree* of A. Conversely, any K-form of a matrix algebra is central simple over K.

Let A and A' be two central simple K-algebras of finite K-dimension. We call A and A' *Brauer equivalent* if there exist a central simple K-algebra D and two natural numbers r and s such that $A \cong M_r(D)$ and $A' \cong M_s(D)$ as K-algebras. This is equivalent to the condition that there exist positive integers t and u such that $M_t(A) \cong M_u(A')$ as K-algebras. The *Brauer group of K*, denoted $\mathrm{Br}(K)$, is defined as the set of equivalence classes of central simple K-algebras of finite K-dimension. It has the structure of a commutative group, with group law defined by $[A] \cdot [A'] := [A \otimes_K A']$.

If A is a central simple K-algebra of finite K-dimension then the same is true for A^{opp}, and the class of A^{opp} is the inverse of the class of A. This corresponds to the fact that $A \otimes_K A^{\mathrm{opp}} \cong M_{n^2}(K)$ if $\dim_K(A) = n^2$.

Let D be a division algebra with center K with $\dim_K(D) < \infty$. By definition, the *index* of D is its degree. If A is a central simple K-algebra with $A \cong M_r(D)$ for some r then by definition $\mathrm{index}(A) := \mathrm{index}(D)$, and so $\deg(A) = r \cdot \mathrm{index}(A)$. The order of $[A]$ in $\mathrm{Br}(K)$ is called its *period*. It is always true that the period divides the index, but in general the two need not be equal. However, if K is a number field or a local field then the period of a central simple K-algebra equals its index.

Let $K \subset L$ be a field extension. If A is a central simple K-algebra then $A_L := L \otimes_K A$ is a central simple algebra over L. Sending $[A]$ to $[A_L]$ gives a well-defined homomorphism $h_{K,L}\colon \mathrm{Br}(K) \to \mathrm{Br}(L)$. We say that L *splits* A, or that L is a *splitting field* for A, if A_L is isomorphic, as an L-algebra, to a matrix algebra $M_n(L)$, or, equivalently, if the class $[A]$ is in the kernel of the homomorphism $h_{K,L}$. If $A \cong M_n(D)$ for some division algebra D then A and D have the same splitting fields. Further, if $L \subset D$ is any maximal subfield containing K then L is a splitting field for D, and $[L : K] = \mathrm{index}(D)$. Conversely, if $K \subset L$ is a finite field extension

then L splits the central simple algebra A if and only if there is an A' that is Brauer-equivalent with A such that L is isomorphic to a maximal subfield of A'. If this holds then $[L:K]$ is a multiple of index(A), and in fact A' can be chosen such that $[L:K]$ equals the degree of A'.

The Brauer group of a field can also be studied via Galois cohomology. In fact, if $K \subset K_s$ is a separable algebraic closure then $\mathrm{Br}(K) \xrightarrow{\sim} H^2\big(\mathrm{Gal}(K_s/K), K_s^*\big)$. If $K \subset L$ is a Galois extension with $L \subset K_s$ then the image of $H^2\big(\mathrm{Gal}(L/K), L^*\big)$ in $\mathrm{Br}(K)$ equals $\mathrm{Br}(L/K) := \mathrm{Ker}\big(h_{K,L}\colon \mathrm{Br}(K) \to \mathrm{Br}(L)\big)$, the subgroup of classes that are split by L.

CyclAlg **(A.5)** Let $K \subset L$ be a Galois extension of finite degree m such that $\mathrm{Gal}(L/K)$ is cyclic. Let $\sigma \in \mathrm{Gal}(L/K)$ and let y be an element of K^*. Consider the ring $L[t;\sigma]$ of polynomials in the variable t with coefficients in L and with ring multiplication satisfying $t \cdot a = \sigma(a) \cdot t$ for all $a \in L$. (Cf. ??) The polynomial $t^m - y$ lies in the centre of this ring, so it generates a 2-sided ideal. The *cyclic algebra* associated to chosen data, notation $(L/K, \sigma, y)$, is defined to be the K-algebra $L[t;\sigma]/(t^m - y)$. So, more informally, $(L/K, \sigma, y)$ can be described as the ring that is obtained by adjoining to L an element t subject to the relations $t \cdot a = \sigma(a) \cdot t$ and $t^m = y$.

It can be shown that $(L/K, \sigma, y)$ is a central simple K-algebra of degree m, and that L is a maximal subfield of A. In particular L is a splitting field. Conversely, if A is any central simple K-algebra of degree m that contains a subfield isomorphic to L (as a K-algebra), then A is isomorphic to $(L/K, \sigma, y)$ for some $y \in K^*$.

We have $(L/K, \sigma, y) \cong (L/K, \sigma, y')$ if and only if $y'/y \in \mathrm{Norm}_{L/K}(L^*)$. Further, if $\nu \in \mathbb{Z}$ is relatively prime with m then $(L/K, \sigma, y) \cong (L/K, \sigma^\nu, y^\nu)$. Fixing a generator σ for $\mathrm{Gal}(L/K)$ it follows that $\mathrm{Br}(L/K) \cong K^*/\mathrm{Norm}(L^*)$.

BrNumbField **(A.6)** If K is a finite field extension of $\mathbb{Q}_p$ for some p then we have $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$. To avoid confusion (especially about signs), let us make the isomorphism that we use explicit. Given a natural number n, let $K \subset L$ be the unramified extension of degree n, which is unique up to isomorphism. Let $q = p^m$ be the cardinality of the residue field of K. The Galois group $\mathrm{Gal}(L/K)$ is cyclic of order n and there is a unique generator $\sigma_{L/K}$ that induces the automorphism $x \mapsto x^q$ on the residue field of L. We refer to $\sigma_{L/K}$ as the *arithmetic Frobenius* of the extension $K \subset L$. Concretely, if $K_0 \subset K$ is the maximal absolutely unramified subfield then K_0 is isomorphic to the fraction field of $W(\mathbb{F}_q)$ and $L \cong W(\mathbb{F}_{q^n}) \otimes_{W(\mathbb{F}_q)} K$. Under such an isomorphism $\sigma_{L/K}$ corresponds to $\sigma^m \otimes \mathrm{id}_K$, where now σ is the automorphism of $W(\mathbb{F}_q)$ that is induced by the Frobenius automorphism $x \mapsto x^p$ of $\mathbb{F}_q$.

Now we take the automorphism $\mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ such that the Brauer class of a cyclic algebra $(L/K, \sigma_{L/K}, y)$ is mapped to the class of $\mathrm{ord}(y)/n$ in $\mathbb{Q}/\mathbb{Z}$. Note that the isomorphism we use is *minus* the isomorphism found in some literature; cf. Serre [2], Chap. X, § 5, Exerc. 1 for instance.

Next we consider a number field K. The determination of its Brauer group also involves the Brauer groups of all completions of K. If v is a non-archimedean place of K with completion K_v (a p-adic field) then as just discussed we have $\mathrm{Br}(K_v) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. If v is an infinite place then the completion K_v is either $\mathbb{R}$ or $\mathbb{C}$. We have $\mathrm{Br}(\mathbb{C}) = 0$ and $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. So all local Brauer groups can be identified with subgroups of $\mathbb{Q}/\mathbb{Z}$. (This is the reason for writing $\mathrm{Br}(\mathbb{R})$ as $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$.) If A is a central simple K-algebra of finite K-dimension then $K_v \otimes_K A$ is a central simple K_v-algebra, and we write $\mathrm{inv}_v(A) \in \mathbb{Q}/\mathbb{Z}$ for the corresponding class. Here it is of course understood that $\mathrm{inv}_v(A) = 0$ if $K_v = \mathbb{C}$ and $\mathrm{inv}_v(A) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ if $K_v = \mathbb{R}$. Then the map $A \mapsto \big(\mathrm{inv}_v(A)\big)$

gives an isomorphism

$$\mathrm{Br}(K) \xrightarrow{\sim} \Big\{ (i_v) \in \bigoplus_v \mathrm{Br}(K_v) \;\Big|\; \sum_v i_v = 0 \Big\}, \tag{1}$$

AppAlg:Br(K)

where the sum runs over all places v of K.

RedCharPol **(A.7)** Let A be a central simple algebra over a field K. Choose a splitting field $K \subset L$ for A and choose an isomorphism of L-algebras $\varphi\colon L \otimes_K A \xrightarrow{\sim} M_n(L)$. If $a \in A$ then the characteristic polynomial $\det\big(T - \varphi(1 \otimes a)\big) \in L[T]$ of the matrix $\varphi(1 \otimes a)$ has coefficients in K and is independent of the choices of the splitting field and the isomorphism φ. We call this polynomial the reduced characteristic polynomial of a over K and denote it by $\mathrm{Prd}_{A/K,a} \in K[T]$. Write

$$\mathrm{Prd}_{A/K,a} = T^n - s_1 T^{n-1} + s_2 T^{n-2} + \cdots + (-1)^n s_n$$

with $s_i \in K$. Then $\mathrm{Trd}_{A/K}(a) := s_1$ is called the reduced trace of a over K and $\mathrm{Nrd}_{A/K}(a) := s_n$ is called the reduced norm of a over K.

Let $\lambda_a\colon A \to A$ be the left multiplication by a, i.e., the map given $\lambda_a(b) = ab$. Then λ_a is a K-linear endomorphism of A. Its characteristic polynomial $P(\lambda_a) := \det(T - \lambda_a) \in K[T]$ is related to the reduced characteristic polynomial by

$$P(\lambda_a) = (\mathrm{Prd}_{A/K,a})^n .$$

In particular, $\det(\lambda_a) = \big(\mathrm{Nrd}_{A/K}(a)\big)^n$ and $\mathrm{trace}_K(\lambda_a) = n \cdot \mathrm{Trd}_{A/K}(a)$.

If $F \subset K$ is a subfield with $[K : F] < \infty$ then we define the reduced trace and norm of a over F by

$$\mathrm{Trd}_{A/F}(a) := \mathrm{trace}_{K/F}\big(\mathrm{Trd}_{A/K}(a)\big) \qquad \text{and} \qquad \mathrm{Nrd}_{A/F}(a) := \mathrm{Norm}_{K/F}\big(\mathrm{Nrd}_{A/K}(a)\big) .$$

For a_1, $a_2 \in A$ we have $\mathrm{Trd}_{A/F}(a_1 a_2) = \mathrm{Trd}_{A/F}(a_2 a_1)$ and $\mathrm{Nrd}_{A/F}(a_1 a_2) = \mathrm{Nrd}_{A/F}(a_1) \cdot \mathrm{Nrd}_{A/F}(a_2)$.

Invol **(A.8)** By an *involution* of a ring A we mean an anti-homomorphism $\sigma\colon A \to A$ such that $\sigma \circ \sigma = \mathrm{id}_A$. Note that σ can also be viewed as a homomorphism $A \to A^{\mathrm{opp}}$. We also note that in some literature this is called an anti-involution. We shall usually denote an involution as a map $a \mapsto a^*$ or $a \mapsto a^\dagger$.

Let A be a central simple algebra over a field K. Let $\sigma\colon a \mapsto a^*$ be an involution on A. We say that the involution σ is *of the first kind* if it is the identity on the center, i.e., $x^* = x$ for all $x \in K$, and that σ is *of the second kind* otherwise. In the latter case, σ gives an automorphism of order 2 of K and we write $K_0 := \{x \in K \mid x^* = x\}$ for its fixed field.

As an example, suppose that A is a quaternion algebra over K, i.e., a division algebra with center K and $\dim_K(A) = 4$. Then the map $a \mapsto a^* := \mathrm{Trd}_{A/K}(a) - a$ is an involution of the first kind on A, called the canonical involution.

Consider a central simple algebra A over a number field K. A necessary and sufficient condition for an involution of the first kind to exist, is that $A \cong A^{\mathrm{opp}}$ as K-algebras. This is equivalent to the condition that $\mathrm{inv}_v(A) \in \{0, 1/2\}$ for all places v of K. If $\mathrm{inv}_v(A) = 0$ for all v then A is a matrix algebra over K and transposition of matrices gives an example of an involution of the first kind. Assume now that $\mathrm{inv}_v(A) \in \{0, 1/2\}$ for all v and that there is at least one v with $\mathrm{inv}_v(A) = 1/2$. (In fact, it follows from (1) that there are then at least two

places v with $\mathrm{inv}_v(A) = 1/2$.) Then A is isomorphic to a matrix algebra over a quaternion algebra, say $A \cong M_r(D)$.

HermForms **(A.9)** Let K be a field. Let A be a central simple K-algebra of finite K-dimension. Let $a \mapsto a^*$ be an involution on A. Finally, let $\varepsilon \in \{-1, 1\}$.

Let V be a finitely generated A-module. By an *ε-hermitian form* on V with respect to the involution $*$, we mean a bi-additive map

$$h\colon V \times V \to A$$

such that

(1) $h(av, bw) = a \cdot h(x, w) \cdot b^*$ for all a, $b \in A$ and v, $w \in V$;
(2) $h(w, v) = \varepsilon \cdot h(v, w)^*$ for all v, $w \in V$.

A 1-hermitian form is often simply called hermitian; a -1-hermitian form is also called a skew-hermitian form.

If V is a finitely generated A-module then $V^\vee := \mathrm{Hom}_A(V, A)$ has the same K-dimension as V. To see this we can easily reduce to the case where V is simple, i.e., $V \cong A/I$ for some left ideal $I \subset A$. As discussed in (A.1) there are idempotents e and e' with $1 = e+e'$ and $I = Ae$; this gives $V^\vee \cong \{a \in A \mid ea = 0\} = e'A \cong eA\backslash A$. Now consider the subfield $K_0 = \{x \in K \mid x^* = x\}$ of K, and note that we have a K_0-linear bijection $A/Ae \xrightarrow{\sim} eA\backslash A$ by $a \bmod Ae \mapsto a^* \bmod eA$. Hence $\dim_K(V) = \dim_K(V^\vee)$.

We give $V^\vee$ the structure of a left A-module structure by the rule $(a \cdot \varphi)\big(v\big) = \varphi(v) \cdot a^*$, for $\varphi \in V^\vee$ and $a \in A$. There is a natural homomorphism of A-modules $\kappa\colon V \to (V^\vee)^\vee$, sending $v \in V$ to the evaluation map $\mathrm{ev}_v\colon V^\vee \to A$. The map κ is readily seen to be injective, so for dimension reasons it is in fact an isomorphism.

An ε-hermitian form h on V gives rise to a homomorphism of A-modules $\hat{h}\colon V \to V^\vee$ by $v \mapsto h(v, -)$. The form h is called *nondegenerate* if $\hat{h}$ is injective, i.e, if for every $v \in V$ there exists an element $w \in V$ such that $h(v, w) \neq 0$. If h is nondegenerate then, again by a dimension count, $\hat{h}$ is an isomorphism. Hence we can define an involution $f \mapsto f^\dagger$ on $\mathrm{End}_A(V)$ by the rule $f^\dagger = \hat{h}^{-1} \circ f^\vee \circ \hat{h}$, where we write $f^\vee\colon V^\vee \leftarrow V^\vee$ for the dual of the map $f\colon V \to V$. By construction we have the relations

$$h(f^\dagger v, w) = h(v, fw) \qquad \text{and} \qquad h(fv, w) = h(v, f^\dagger w)$$

for all v, $w \in V$.

FormsInvolCorr **(A.10) Proposition.** *Let A be a central simple algebra of finite dimension over a field K. Let $a \mapsto a^*$ be an involution on K. Let V be a finitely generated A-module.*

(i) *Suppose $*$ is of the first kind. Then the map that associates to an ε-hermitian form h on V the involution $f \mapsto f^\dagger = \hat{h}^{-1} \circ f^\vee \circ \hat{h}$ on $\mathrm{End}_A(V)$ gives a bijection*

$$\left\{ \begin{array}{c} \textit{nondegenerate} \\ \textit{$\pm$-hermitian forms on } V \\ \textit{up to homothety} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \textit{involutions of the first kind} \\ \textit{on } \mathrm{End}_A(V) \end{array} \right\}.$$

(ii) *Suppose $*$ is of the second kind. Then the map that associates to an ε-hermitian form h on V the involution $f \mapsto f^\dagger = \hat{h}^{-1} \circ f^\vee \circ \hat{h}$ on $\mathrm{End}_A(V)$ gives a bijection*

$$\left\{ \begin{array}{c} \textit{nondegenerate} \\ \textit{hermitian forms on } V \\ \textit{up to homotheties in } K_0^* \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \textit{involutions } \dagger \textit{ of the second kind} \\ \textit{on } \mathrm{End}_A(V) \\ \textit{with } f^\dagger = f^* \textit{ for all } f \in K \end{array} \right\}.$$

The hermitian forms on V that we consider here are of course understood to be hermitian with respect to the given involution $*$ on A. Note that in (ii) we only consider $+1$-hermitian forms. This is no restriction of generality, since by choosing an element $\alpha \in K$ with $\alpha^* = -\alpha$ we obtain a bijective correspondence $h \mapsto \alpha \cdot h$ between hermitian and skew-hermitian forms.

PosInvol **(A.11)** Let $(K, \geqslant)$ be an ordered field. (The most relevant examples for us are $K = \mathbb{Q}$ and $K = \mathbb{R}$.) Let A be a finite dimensional semisimple K-algebra. An involution $a \mapsto a^*$ on A is called a positive involution if $\mathrm{Trd}_{A/K}(aa^*) > 0$ for all nonzero $a \in A$.

Let V be an A-module, and consider a hermitian form $h\colon V \times V \to A$ with respect to the involution $*$. Then the form h is said to be positive definite (over the ordered field K) if $\mathrm{Trd}_{A/K} h(v, v) > 0$ for all nonzero $v \in V$.

PosInvolProp **(A.12) Proposition.** *Let A be a finite dimensional semisimple $\mathbb{R}$-algebra. Let $a \mapsto a^*$ be an involution on A. Then the following properties are equivalent.*

(1) *The involution $*$ is positive.*
(2) *There exists a finitely generated faithful A-module V and a positive definite hermitian form $h\colon V \times V \to A$ with respect to $*$.*
(3) *For every finitely generated A-module V there exists a positive definite hermitian form $h\colon V \times V \to A$ with respect to $*$.*

References for Appendix A.

(A.1)–(A.3): Bourbaki [1], Chap. 8, Lam ..., Lang ... ?? (NOG AANVULLEN)

(A.4)–(A.6): Serre [2], Pierce [1], ...

(A.7): Bourbaki [1], Chap. 8, § 12.

(A.8): Knus, Merkurjev, Rost and Tignol [1]

(A.11)–(A.12): Kottwitz [1], § 2.

References

Books referred to by abbreviation

BLR **S. Bosch, W. Lütkebohmert, M. Raynaud**, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Vol. **21**, Springer-Verlag, 1990.

EGA **A. Grothendieck, J. Dieudonné**, *Eléments de Géométrie Algébrique*, Publ. Math. de l'I.H.E.S. **4**, **8**, **11**, **17**, **20**, **24**, **28**, **32** (1960–67); Chap. 1 republished as Die Grundlehren der mathematischen Wissenschaften **166**, Springer-Verlag, Berlin, 1971.

FGA **A. Grothendieck**, *Fondements de Géométrie Algébrique*, Séminaire Bourbaki, Exp. 190, 195, 212, 221, 232, 236, ???

SGA1 **A. Grothendieck et al.**, *Revêtements étales et groupe fondamental*, Lecture Notes in Math. **224**, Springer-Verlag, Berlin, 1971.

SGA3 **M. Demazure et al.**, *Schémas en groupes*, Lecture Notes in Math. **151**, **152**, **153**, Springer-Verlag, Berlin, 1970.

HAG **R. Hartshorne**, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, NewYork, 1977.

MAV **D. Mumford**, *Abelian Varieties*, Oxford University Press, Oxford, 1970.

GIT **D. Mumford, J. Fogarty, F. Kirwan**, *Geometric Invariant Theory (3rd enlarged ed.)*, Ergebnisse der Mathematik und ihrer Grenzgebiete **34**, Springer-Verlag, Berlin, 1994.

Other references

A. Altman, S. Kleiman

1. *Introduction to Grothendieck duality*, Lecture Notes in Math. **146**, Springer-Verlag, Berlin, 1970.

S. Anantharaman

1. *Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension* 1 Bull. Soc. Math. France, Mémoire **33** (1973), 5–79.

A. Andreotti

1. *On a theorem of Torelli*, Amer. J. Math. **80** (1958), 801–828.

A. Andreotti, A.L. Mayer

1. *On period relations for abelian integrals on algebraic curves*, Ann. Scuola Norm. Pisa **21** (1967), 189–238.

M.F. Atiyah, I.G. Macdonald

1. *Introduction to commutative algebra*, Addison-Wesley, Reading MA, 1969.

F. Bardelli, C. Ciliberto, A. Verra

1. *Curves of minimal genus on a general abelian variety*, Compos. Math. **96** (1995), 115–147.

W. Barth

1. *??*

A. Beauville

1. *Quelques remarques sur la transformation de Fourier dans l'anneau de Chow d'une variété abélienne*, in: Algebraic Geometry (Tokyo/Kyoto 1982), Lecture Notes in Math. **1016**, Springer-Verlag, Berlin, 1983, pp. 238–260.
2. *Sur l'anneau de Chow d'une variété abélienne*, Math. Ann. **273** (1986), 647–651.
3. *Le problème de Torelli*, Séminaire Bourbaki, Exp. ??, ??; in: Astérisque **145–146** (1987), 7–20.

P. Berthelot

1. *Cohomologie cristalline des schémas de caractéristique $p > 0$*, Lecture Notes in Math. **407**, Springer-Verlag, Berlin, 1974.

P. Berthelot, A. Ogus
1. *Notes on crystalline cohomology*, Mathematical Notes **21**, Princeton University Press, Princeton, NJ, 1978.

S. Bloch
1. *Algebraic cycles and K-theory*, Adv. Math. **61** (1986), 267–304.
2. *Some elementary theorems about algebraic cycles on Abelian varieties*, Invent. Math. **37** (1976), 215–228.

E. Bombieri
1. *Counting points on curves over finite fields (d'après S.A. Stepanov)* Séminaire Bourbaki, Exp. **430** (1972/73), pp. 234–241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974.

A. Borel
1. *Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts*, Ann. of Math. **57** (1953), 115–207. (= Œuvres, ??)

A. Borel, J-P. Serre
1. *Le th'eorème de Riemann-Roch, d'après Grothendieck*, Bull. Soc. Math. France **86** (1958), 97–136.

N. Bourbaki
1. *Algèbre*, (data to be supplied)
2. *Algèbre Commutative*, (data to be supplied)

A. Collino
1. *A new proof of the Ran-Matsusaka criterion for Jacobians*, Proc. A.M.S. **92** (1984), 329–331.
2. *A simple proof of the theorem of Torelli based on Torelli's approach*, Proc. A.M.S. **100** (1987), 16–20.

B. Conrad
1. *Grothendieck duality and base change*, Lecture Notes in Math. **1750**, Springer, 2000.

C.W. Curtis, I. Reiner
1. *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics **11**, John Wiley & Sons, Inc., 1962.

P. Deligne
1. *Théorème de Lefschetz et critères de dégénérescence de suites spectrales*, Publ. Math. de l'I.H.E.S. **35** (1968), 107–126.
2. *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.
3. *La conjecture de Weil. I.* Publ. Math. de l'I.H.E.S. **43** (1974), 273–307.
4. *??* in: Galois groups over $\mathbb{Q}$. (NOG AANVULLEN)

P. Deligne, L. Illusie
1. *Relèvements modulo p^2 et décomposition du complexe de de Rham*, Invent. Math. **29** (1987), 247–270.

P. Deligne, J.S. Milne
1. *Tannakian categories*, In: Hodge cycles, motives and Shimura varieties, P. Deligne et al., eds., Lecture Notes in Math. **900** (1981), pp. 101–228.

M. Demazure, P. Gabriel
1. *Groupes Algébriques, Tome I*, Masson & Cie, Paris/North-Holland, Amsterdam, 1970.

C. Deninger, J. Murre
1. *Motivic decomposition of abelian schemes and the Fourier transform*, J. reine angew. Math. **422** (1991), 201–219.

M. Deuring
1. *Über die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg **14** (1941), 197–272.
2. *Algebren (Zweite korrigierte Auflage)*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 1. Folge (???), Vol. **41**, Springer-Verlag, 1968.

J. Dieudonné
1. *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. VII.*, Math. Ann. **134** (1957), 114–133.
2. *Course de géométrie algébrique* **??** (data to be supplied)

G. Faltings, C-L. Chai
1. *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Vol. **22**, Springer-Verlag, 1990.

W. Fulton
1. *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Vol. **2**, Springer-Verlag, 1984.

J. Giraud
1. *Cohomologie non abélienne*, Die Grundlehren der mathematischen Wissenschaften**179**, Springer-Verlag, Berlin-New York, 1971.

G. van der Geer, M. van der Vlugt
1. *Kloosterman Sums and the p-torsion of Certain Jacobians*,

G.H. Hardy, E.M. Wright
1. *An introduction to the theory of numbers (5th ed.)*, Oxford Science Publications, Clarendon Press, Oxford, 1979.

R. Hartshorne
1. *Residues and duality*, Lecture Notes in Math. **20**, Springer-Verlag, Berlin, 1966.

T. Honda
1. *Isogeny classes of abelian varieties over finite fields*, Journ. Math. Soc. Japan **20** (1968), 83–95.

E. Howe
1. *Principally polarized ordinary abelian varieties over finite fields*, Trans. A.M.S. **347** (1995), 2361–2401.
2. *Isogeny classes of ableina varieties with no principal polarisations*, in: Moduli of abelian varieties, Faber, van der Geer, Oort (eds.), Progress in Math. **195**, Birkhäuser Verlag, Basel, 2001.

Y. Ihara
1. *Some remarks on the number of points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo **28** (1982), 721–724.

L. Illusie
1. *Report on crystalline cohomology*. In: Algebraic geometry (Arcata 1974), Procedings of Symposia in Pure Mathematics 29, AMS, Providence, RI, 1975, pp. 459–478.
2. *Cohomologie cristalline (d'après P. Berthelot)*, Séminaire Bourbaki, Exp. 456, in: Lecture Notes in Math. **514**, Springer, Berlin, 1976, pp. 53–60.
3. *Cohomologie de de Rham et cohomologie étale p-adique (d'après G. Faltings, J.-M. Fontaine et al.)*, Séminaire Bourbaki, Exp. 726, in: Astérisque **189–190** (1990), pp. 325–374.
4. *Crystalline cohomology*. In: Motives (Seattle, WA, 1991), Procedings of Symposia in Pure Mathematics **55**(1), AMS, Providence, RI, 1994, pp. 43–70.

N. Jacobson
1. *The theory of rings*, Mathematical Surveys **2**, American Math. Soc., New York, 1943.

T. Katsura, K. Ueno
1. *On elliptic surfaces in characteristic p*, Math. Ann. **272** (1985), pp. 291–330.

N.M. Katz
1. *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields*. In: Mathematical developments arising from Hilbert problems (Northern Illinois Univ., De Kalb, Ill., 1974), Procedings of Symposia in Pure Mathematics **28**, AMS, Providence, R.I., 1976, pp. 275–305.
2. *Slope filtration of F-crystals*. In: Journeées de Géométrie Algébrique de Rennes (I), Astérisque **63** (1979), 113–164.

N.M. Katz, B. Mazur
1. *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies **108**, Princeton University Press, Princeton, 1985.

S. Keel, S. Mori
1. *Quotients by groupoids*, Ann. of Math. **145** (1997), pp. 193–213.

G. Kempf
1. *On the geometry of a theorem of Riemann*, Ann. of Math. **98** (1973), 178–185.

S. Kleiman
1. *Algebraic cycles and the Weil conjectures*. In: Dix exposés sur la cohomologie des schémas. Amsterdam 1968.

F. Klein
1. *Geschichte der Mathematik im 19. Jahrhundert*, (data to be supplied)

M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol
1. *The book of involutions*, AMS Colloquium Publications **44**. AMS, Providence, RI, 1998.

J. Kollár
1. *Quotient spaces modulo algebraic groups*, Ann. of Math. **145** (1997), pp. 33–79.

R.E. Kottwitz
1. *Points on some Shimura varieties over finite fields*, J.A.M.S. **5** (1992), pp. 373–444.

K. Künnemann
1. *On the Chow motive of an abelian scheme.* In: Motives (Seattle, WA, 1991), Procedings of Symposia in Pure Mathematics **55**(1), AMS, Providence, RI, 1994, pp. 189–205.

T.Y. Lam
1. *A first course in noncommutative rings*, Graduate Texts in Mathematics **131**, Springer-Verlag, New York, 2001.

S. Lang
1. *Abelian varieties*, Interscience tracts in pure and applied math. **7**, Interscience Publ., New York, 1959.
2. *Introduction to modular forms (corrected reprint)*, Die Grundlehren der mathematischen Wissenschaften**222**, Springer-Verlag, 1995.

H. Lange, Ch. Birkenhake
1. *Complex abelian varieties*, Die Grundlehren der mathematischen Wissenschaften **302**, Springer-Verlag, 1992.

G. Laumon, L. Moret-Bailly
1. *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Vol. **39**, Springer-Verlag, 2000.

Yu.I. Manin
1. *Correspondences, motives and monoidal transforms*, Mat. Sborn. **77** (1970), 475–507.

W.S. Massey
1. *Algebraic topology: an introduction*, Graduate Texts in Mathematics **56**, Springer-Verlag, 1967.

H. Matsumura
1. *Commutative ring theory*, Cambridge studies in advanced mathematics **8**, Cambridge University Press, Cambridge, 1986.

H. Matsumura, F. Oort
1. *Representability of group functors, and automorphisms of algebraic schemes*, Invent. Math. **4** (1967), 1–25.

T. Matsusaka
1. *On a theorem of Torelli*, Amer. J. Math. **80** (1958), 784–800.

A. Mattuck, A. Mayer
1. *The Riemann-Roch theorem for algebraic curves*, Ann. Scuola Norm. Pisa **17** (1963), 223–237.

W. Messing
1. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes* Lecture Notes in Math. **264**, Springer-Verlag, Berlin, 1972.
2. *Short sketch of Deligne's proof of the hard Lefschetz theorem.* In: Algebraic geometry (Arcata 1974), Procedings of Symposia in Pure Mathematics 29, AMS, Providence, RI, 1975, pp. 563–580.

N. Mestrano, S. Ramanan
1. *Poincaré bundles for families of curves*, J. reine angew. Math. **362** (1985), 169–178.

J.S. Milne
1. *Abelian varieties.* In: Artihmetic Geometry, G. Cornell and J.H. Silverman, eds., Springer-Verlag, New York, 1986, pp. 103–150.
2. *Jacobian varieties.* In: Artihmetic Geometry, G. Cornell and J.H. Silverman, eds., Springer-Verlag, New York, 1986, pp. 167–212.

J.W. Milnor, J.C. Moore
1. *On the structure of Hopf algebras*, Ann. of Math. **81** (1965), 211-264.

F. Morel, V. Voevodsky
1. $\mathbb{A}^1$*-homotopy theory of schemes* (NOG AANVULLEN)

L. Moret-Bailly
1. *Familles de courbes et de variétés abéliennes sur* $\mathbb{P}^1$*; I: Descente des polarisations, II: Exemples.* In: Séminaire sur les pinceaux de courbes de genre au moins deux, L. Szpiro, ed., Astérisque **86** (1981), 109–124 & 125–140.
2. *Pinceaux de variétés abéliennes*, Astérisque **129** (1985).

S. Mukai
1. *Duality between* $D(X)$ *and* $D(\hat{X})$ *with its applications to Picard sheaves*, Nagoya Math. J. **81** (1981), 153–175.

D. Mumford
1. *On the equations defining abelian varieties, I–III*, Invent. Math. **1** (1966), 287–354, **3** (1967), 75–135 & 215–244.
2. *Lectures on curves on an algebraic surface*, Annals of mathematics studies **59**, Princeton University Press, Princeton NJ, 1966.
3. *Curves and their Jacobians*, The university of Michigan press, Ann Arbvor MI, 1975.
4. (with several collaborators) *Tata lectures on theta, I–III*, Progress in Math. **28**, **43**, **97**, Birkhäuser, Boston MA, 1983, 1984, 1991.

J.P. Murre
1. *On contravariant functors from the category of preschemes over a field into the category of abelian groups*, Publ. Math. de l'I.H.E.S. **23** (1964), 5–43.

M. Nagata
1. *Some questions on rational actions of groups.* In: Algebraic Geometry, S.S. Abhyankar et al., eds., Oxford University Press, 1969, pp. 323–334.

J. Neukirch
1. *Algebraic Number Theory* (Translated from the 1992 German original), Die Grundlehren der mathematischen Wissenschaften **322**, Springer, 1999.

T. Oda
1. *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135.

J. Oesterlé
1. *Dégénérescence de la suite spectrale de Hodge vers de Rham*, Séminaire Bourbaki, Exp. 673 (data to be supplied)

F. Oort
1. *Sur le schéma de Picard*, Bull. Soc. Math. France **90** (1962), 1–14.
2. *Algebraic group schemes in characteristic zero are reduced*, Invent. Math. **2** (1966), 79–80.
3. *Commutative group schemes*, Lecture Notes in Math. **15**, Springer-Verlag, Berlin, 1966.
4. *Endomorphism algebras of abelian varieties.* In: Algebraic geometry and commutative algebra, Vol. II, H. Hijikata et al., eds., Kinokuniya, Tokyo, 1988, pp. 469–502.

R.S. Pierce
1. *Associative Algebras* Graduate Texts in Mathematics **88**, Springer-Verlag, New York, 1982.

??. Pontryagin
1. Akd. Nauk USSR 1 (1935), 433–437 (DATA TO BE SUPPLIED)
2. C.R. Paris 200 (1935), 1277–1280.) (DATA TO BE SUPPLIED)

M. Raynaud
1. *Sur le passage au quotient par un groupoïde plate* C. R. Acad. Sc. Paris (Série I, Math.) **265** (1967), 384–387.
2. *Passage au quotient par une relation d'équivalence plate.* In: Proceedings of a conference on local fields, T.A. Springer, ed., Springer-Verlag, Berlin, 1967, pp. 78–85.
3. *Faisceaux amples sur les schémas en groupes et les espaces homogènes*, Lecture Notes in Math. **119**, Springer-Verlag, Berlin-New York, 1970.

I. Reiner
1. *Maximal orders (Corrected reprint of the 1975 original)*, London Math. Soc. Monographs (New Series) **28**, The Clarendon Press, Oxford University Press, Oxford, 2003.

J.J. Rotman
1. *An introduction to algebraic topology*, Graduate Texts in Mathematics **119**, Springer-Verlag, 1988.

R. Schoof
1. *Nonsingular plane cubic curves over finite fields* J. Combin. Theory Ser. A **46** (1987), 183–211.

E. Selmer
1. *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$ Acta Math. **85** (1951), 203–362.

J-P. Serre
1. *Quelques propriétés des variétés abéliennes en caractéristique p*, Amer. J. Math. **80** (1958), 715–739.
2. *Corps Locaux* (data to be supplied)
3. *Resumé des Cours de 1964–65*, Annuaire du Collège de France. Oeuvres II, p. 272.
4. *Complex Multiplication*. In: Algebraic Number Theory, J.W.S. Cassels, A. Fröhlich, Eds. Academic Press London 1967.
5. *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sc. Paris (Série I, Math.) **296** (1983), no. 9, 397–402.

E. Selmer
1. *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

A.M. Shermenev
1. *The motive of an abelian variety*, Funct. Anal. **8** (1974), 55–61.

G. Shimura
1. *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. **78** (1963), 149–192.

G. Shimura, Y. Taniyama
1. *Complex multiplication of abelian varieties and its applications to number theory*, Publ. of the Math. Soc. of Japan **6**, The Math. Soc. of Japan, Tokyo, 1961.

A. Silverberg, Yu.G. Zarhin
1. *Polarizations on abelian varieties*, Math. Proc. Cambridge Philos. Soc. **133** (2002), 223–233.

J.H. Silverman
1. *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
2. *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

J. Tate
1. *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.
2. *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.
3. *Finite flat group schemes*. In: Modular forms and Fermat's last theorem, G. Cornell et al, eds., Springer-Verlag, New York, 1997, pp. 121–154.

J. Tate, F. Oort
1. *Group schemes of prime order*, Ann. Sci. École Norm. Sup. **3** (1970), 1–21.

D. Toledo
1. *Projective varieties with non-residually finite fundamental group*, Publ. Math. de l'I.H.E.S. **77** (1993), 103–119.

R. Torelli
1. *Sulle serie algebriche semplicemente infinite di gruppi di punti appartenenti a una curva algebrica*, Rend. Circ. Mat. Palermo **37** (1914), ??.

A. van de Ven
1. *On the embedding of abelian varieties in projective space*, Annali di Matematica pura ed applicata (4), **103** (1975), 127–129.

S.G. Vladuts, V.G. Drinfeld
1. *Number of points of an algebraic curve*, Funct. Analysis **17** (1983), 68–69.

W.C. Waterhouse
1. *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4), **2** (1969), 521–560.
2. *Introduction to affine group schemes*, Graduate Texts in Mathematics **66**, Springer-Verlag, New York, 1979.

W.C. Waterhouse, J.S. Milne

1. *Abelian varieties over finite fields*, In: Procedings of Symposia in Pure Mathematics **20**, ??? (eds.), Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64.

A. Weil

1. *Zum Beweis des Torellischen Satzes*, Nachrichten der Akademie der Wissenschaften in Göttingen, Math.-Phys. Klasse, 2 (1957), 33–53.
2. *Sur les courbes algébriques et les variétés qui s'en déduisent*, (data to be supplied)
3. *Variétés abéliennes et courbes algébriques*, (data to be supplied)
4. *Number of solutions of equations over finite fields*, Bull. A.M.S. **55** (1949), 497–508.
5. *On the projective embedding of abelian varieties*, (data to be supplied)

T. Zink

1. *Cartiertheorie kommutativer formaler Gruppen*, Teubner-Texte zur Mathematik **68**, Teubner, Leipzig, 1984.

Index