Université de Rennes 1

Seminar report

An Introduction to Abelian Varieties

Pierrick Dartois

Abstract: The goal of this seminar is to understand abelian varieties and to see some generalizations of the results I have already studied on elliptic curves (regarding torsion subgroups and the $\mathbb{Z}$-module of homomorphisms $\mathrm{Hom}(A, B)$ in particular). The study of abelian varieties in plain generality requires a significant amount of knowledge in algebraic geometry, a field I started to study with the lectures of Florian Ivorra this year, during the course of this seminar. That is why a first chapter with geometric prerequisites was necessary. Of course, all the results used here are not proved (it would require an entire book), but we emphasized on some topics (invertible sheaves and divisors in particular). The emphasis might have been influenced by the subjectivity of the author.

In chapter 2, we introduce abelian varieties (and group schemes). We prove some basic properties of these objects (mainly that they are smooth and that their group structure is commutative) and present some deep consequences of the theorem of the cube: the projectiveness of abelian varieties and the structure their torsion subgroups. We mainly followed the lectures given by Milne [1] but unlike him, we preferred a scheme theoretic approach like Mumford [2] and the Stack Project [3, chapter 39].

Our objective is reached in chapter 3 presenting Tate modules and constructing an embedding $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(A, B) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$. Then, we present further refinements and applications of this result (without proof) in the case of finite fields, namely, the fact that this map becomes essentially an isomorphism[1] and a characterization of isogenous abelian varieties. Those theorems are due to John Tate [4] and presented in the conference proceeding of Waterhouse and Milne [5] initially set as a main reference document for this seminar.

[1] This is not exactly true because we need to take into account a Galois invariance property.

Contents

Chapter 1

Geometric preliminaries

Throughout the document, k is a field and $\overline{k}$ is an algebraic closure of k.

1.1 Preliminaries of general scheme theory

1.1.1 Separatedness, finiteness, varieties

Definition 1.1. Let X be a k-scheme. One says that X is *separated* if the structural morphism $\pi : X \longrightarrow \mathrm{Spec}(k)$ is separated, i.e. if the diagonal morphism $\Delta_{X/k} : X \longrightarrow X \times_k X$ induced by the universal property of the fiber product as follows:

$$\begin{tikzcd}
X \arrow[dr, dotted, "\Delta_{X/k}"] \arrow[drr, "\mathrm{id}_X"] \arrow[ddr, "\mathrm{id}_X"'] & & \\
& X \times_k X \arrow[r] \arrow[d] & X \arrow[d, "\pi"] \\
& X \arrow[r, "\pi"] & \mathrm{Spec}(k)
\end{tikzcd}$$

is a closed immersion.

Lemma 1.2. *Let $\varphi, \psi : X \longrightarrow Y$ two morphisms of k-schemes. Suppose that Y is separated. Then the set:*

$$\{x \in X \mid \varphi(x) = \psi(x)\}$$

is closed in X.

Proof. Consider the morphism $\theta : X \xrightarrow{\Delta_{X/k}} X \times_k X \xrightarrow{\varphi \times_k \psi} Y \times_k Y$, $x \longmapsto (\varphi(x), \psi(x))$. Then, we have:

$$\{x \in X \mid \varphi(x) = \psi(x)\} = \theta^{-1}(\Delta_{Y/k}(Y \times_k Y))$$

And Y is separated so $\Delta_{Y/k}$ is closed, which completes the proof. □

Definition 1.3. One says that a morphism $f : X \longrightarrow Y$ is of finitr type if it is:

(i) Locally of finite type: for all open affines $U \subseteq X$ and $V \subseteq Y$ such that $f(U) \subseteq V$, the morphism $\Gamma(V, \mathcal{O}_Y) \longrightarrow \Gamma(U, \mathcal{O}_X)$ is of finite type.

(ii) Quasi compact: for all quasi compact open subset $V \subseteq Y$, $f^{-1}(V)$ is quasi-compact.

Definition 1.4. One says that a k-scheme X is of finite type when the structural morphism $\pi : X \longrightarrow \mathrm{Spec}(k)$ is. Equivalently, X is of finite type when it is:

(i) Locally of finite type, i.e. $\Gamma(U, \mathcal{O}_X)$ is a finite-type k-algebra for all open subset $U \subseteq X$.

(ii) Quasi compact (as a topological space).

Definition 1.5. A k-variety is a separated k-scheme of finite type.

1.1.2 Geometric properties and extension of scalars

Definition 1.6. One says that a k-scheme X is geometrically reduced, irreducible or integral (i.e. both) if $X_{\overline{k}} = X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ is respectively reduced, irreducible or integral.

Proposition 1.7. *A k-scheme X is geometrically reduced, irreducible or integral if and only if X_K is respectively reduced, irreducible or integral for every field extension K/k. In that case, X is integral.*

Proof. See [6, propositions 5.49, 5.51 and corollary 5.54]. □

1.1.3 Completeness and properness

Definition 1.8. A morphism of schemes $f : X \longrightarrow Y$ is said to be *universally closed* if for every morphism of schemes $g : Z \longrightarrow Y$, the base change of f, $f' : X \times_Y Z \longrightarrow Z$ provided by the definition of the fiber product is closed:

$$\begin{tikzcd}
X \times_Y Z \arrow[r, "f'"] \arrow[d] & Z \arrow[d, "g"] \\
X \arrow[r, "f"] & Y
\end{tikzcd}$$

Such a morphism is *proper* if it is separated, of finite type and universally closed.

Definition 1.9. A k-scheme X is *complete* if the structural morphism $\pi : X \longrightarrow \mathrm{Spec}(k)$ is universally closed, or equivalently, if the right projection map $q : X \times_k Y \longrightarrow Y$ is closed for every k-scheme Y.

A k-scheme X is said to be *proper* if it is complete and a k-variety (i.e. separated and of finite type), or equivalently, if the structural morphism $\pi : X \longrightarrow \mathrm{Spec}(k)$ is proper.

Lemma 1.10. (i) *Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be morphisms of schemes. If $g \circ f$ is proper and g is separated, then f is proper.*

(ii) *Proper morphisms are stable under base change.*

Proof. See [7, corollary II.4.8, points c and e]. □

Lemma 1.11. *Let $f : X \longrightarrow Y$ be a morphism of k-schemes. Assume that X is proper and Y is separated. Then f is proper.*

Proof. Since $\pi_{Y/k} \circ f = \pi_{X/k}$, it is an immediate consequence of the point (i) of the preceding lemma. □

Lemma 1.12. *Let X be a proper and geometrically integral k-scheme. Then, every morphism from X to an affine k-variety is constant.*

Proof. See [6, corollary 12.67]. □

Theorem 1.13 (rigidity lemma)**.** *Let $\varphi : X \times_k Y \longrightarrow Z$ be a morphism of k-schemes. Assume that X is proper and geometrically integral, that $X \times_k Y$ is geometrically irreducible, that Z is separated and that there exist k-valued points $x_0 \in X(k)$, $y_0 \in Y(k)$ and $z_0 \in Z(k)$ such that:*

$$\varphi(X \times \{y_0\}) = \{z_0\} = \varphi(\{x_0\} \times Y)$$

Then, $\varphi(X \times Y) = \{z_0\}$.

Proof. One can easily see that the properties of the theorem are invariant under base change, so we can assume that k is algebraically closed. Let U_0 be an open affine neighborhood of z_0, $q : X \times_k Y \longrightarrow Y$ the right projection map and $F := q(\varphi^{-1}(Z \setminus U_0))$. Note that F is closed in Y because q is closed (since X is complete), so $U := Y \setminus F$ is open in Y. Moreover, we have:

$$U = \{y \in Y \mid \varphi(X \times \{y\}) \subseteq U_0\}$$

so in particular, $y_0 \in U$ and $U \neq \emptyset$. Since U_0 is affine and that X is proper and geometrically integral, for all $y \in U$, $\varphi_{|X \times \{y\}} : X \times \{y\} \simeq X \longrightarrow U_0$ is constant by lemma 1.12. Then, for all $y \in U$, $\varphi(X \times \{y\}) = \{\varphi(x_0, y)\} = \{z_0\}$. Then, φ is constant on $X \times U$.

Since $X \times Y$ is irreducible and $X \times U$ is a non-empty open subset, $X \times U$ is dense. Since Z is separated, the set on which φ agrees with the constant map is closed (by lemma 1.2), so it contains $\overline{X \times U} = X \times Y$, which completes the proof. □

1.1.4 Smooth, regular and normal schemes

Definition 1.14. Let $f : X \longrightarrow Y$ be a morphism of schemes.

(i) One says that f is smooth (of relative dimension d) at $x \in X$, if there exist affine open neighborhoods U of x and $V = \mathrm{Spec}(R)$ of $f(x)$ such that $f(U) \subseteq V$, and an open immersion

$$j : U \hookrightarrow \mathrm{Spec}(R[T_1, \cdots, T_n]/(f_1, \cdots, f_{n-d}))$$

of R-schemes where $n \geq d$ and $f_1, \cdots, f_{n-d} \in R[T_1, \cdots, T_n]$, such that the Jacobian matrix

$$\mathrm{Jac}(f_1, \cdots, f_{n-d})(x) := \left(\frac{\partial f_i}{\partial T_j}(x)\right)_{\substack{1 \leq i \leq n-d \\ 1 \leq j \leq n}} \in M_{n-d,n}(\kappa(x))$$

has rank $n - d$ (x being seen as a $\kappa(x)$-valued point).

(ii) One says that $f : X \longrightarrow Y$ is smooth (of relative dimension d), if it is smooth (of relative dimension d) at all points $x \in X$.

(iii) A k-variety X is smooth (respectively $x \in X$ is smooth) if its structural morphism $\pi_{X/k} : X \longrightarrow \mathrm{Spec}(k)$ is smooth (respectively smooth at x).

Lemma 1.15. *Let X be a geometrically reduced k-scheme. Then, the smooth locus (i.e. the set of smooth points of X) is open and dense in X.*

Proof. See [6, proposition 6.19 and remark 6.20]. □

Definition 1.16. A Noetherian local ring R is *regular* if its maximal ideal can be generated by $\dim(R)$ elements.

A scheme X is regular if for all $x \in X$, $\mathcal{O}_{X,x}$ is regular.

Theorem 1.17 (Auslander and Buchsbaum)**.** *A regular local ring is a unique factorization domain.*

Proof. See [8, theorem 20.3]. □

Definition 1.18. A ring R is *normal* if the localization $R_{\mathfrak{p}}$ is an integrally closed domain for every prime ideal $\mathfrak{p}$ of R.

A scheme X is normal if for all $x \in X$, $\mathcal{O}_{X,x}$ is normal.

Lemma 1.19. *Let X be a k-variety.*

(i) *If X is smooth, then X is regular.*

(ii) *If X is regular, then X is normal.*

Proof. See [6, Lemma 6.26] for (i) and [6, Lemma 6.39] for (ii). □

1.2 More results on morphisms of schemes

1.2.1 Finite locally free morphisms

Definition 1.20. **(i)** A morphism of schemes is *affine* when the preimage of every open affine is affine.

(ii) A morphism of schemes $f : X \longrightarrow Y$ is *finite* if it is affine and for every open affine $V \subseteq Y$, the induced morphism $f^b_U : \Gamma(V, \mathcal{O}_Y) \longrightarrow \Gamma(f^{-1}(V), \mathcal{O}_X)$ is of finite type (meaning that $\Gamma(f^{-1}(V), \mathcal{O}_X)$ is a finite type $\Gamma(V, \mathcal{O}_Y)$-module).

Let $f : X \longrightarrow Y$ be a morphism of schemes. In general, the topological fibers of f do not have a structure of scheme. That is why we consider the *scheme theoretic fibers* of f defined as follows. Let $y \in Y$. Then, we have a morphism $\hat{y} : \mathrm{Spec}(\kappa(y)) \longrightarrow Y$ mapping the point to y. The *scheme theoretic fiber* of f at y is the fiber product:

$$X_y := X \times_Y \mathrm{Spec}(\kappa(y))$$

induced by $f : X \longrightarrow Y$ and $\hat{y} : \mathrm{Spec}(\kappa(y)) \longrightarrow Y$.

Lemma 1.21. *Let $f : X \longrightarrow Y$. Assume that Y is locally Noetherian. Then f is finite if and only if it is proper with finite (scheme theoretic) fibers.*

Proof. See [3, lemma 30.21.1]. □

Definition 1.22. **(i)** Let R be a ring and M be a R-module. One says that M is *flat* if the functor $M \otimes_A \_$ is exact.

(ii) Let $(X, \mathcal{O}_X)$ be a ringed space. An $\mathcal{O}_X$-module $\mathcal{M}$ is *flat* if for all $x \in X$, $\mathcal{M}_x$ is a flat $\mathcal{O}_{X,x}$-module.

(iii) A morphism of schemes $f : X \longrightarrow Y$ is *flat* (respectively coherent) when $f_*\mathcal{O}_X$ is a flat (respectively coherent) $\mathcal{O}_Y$-module.

Definition 1.23. **(i)** Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{M}$ be an $\mathcal{O}_X$-module. One says that $\mathcal{M}$ is *locally free* if for all $x \in X$, there exists an open neighborhood U of x such that $\mathcal{M}_{|U} \simeq \mathcal{O}_X^{(I_x)}{}_{|U}$ for a given set I_x.

(ii) One says that $\mathcal{M}$ is *locally free of finite type* if I_x is additionally finite for all $x \in X$.

(iii) One says that $\mathcal{M}$ is *locally free of rank n* if $|I_x| = n$ for all $x \in X$.

Proposition 1.24. *Let $f : X \longrightarrow Y$ be a morphism of locally Noetherian schemes. Then, the following conditions are equivalent:*

(i) *f is affine and $f_*\mathcal{O}_X$ is a locally free of finite type $\mathcal{O}_Y$-module.*

(ii) *f is finite, flat and coherent.*

Proof. See [6, proposition 12.19] and [6, proposition 7.45], the latter ensuring that coherent modules and modules of finite presentation[1] are the same on locally Noetherian schemes. □

Definition 1.25. A morphism of locally Noetherian schemes is said to be *finite locally free* when it satisfies the equivalent conditions above.

Lemma 1.26. *Let $f : X \longrightarrow Y$ be an affine morphism of schemes over a base scheme S. Let $\mathcal{M}$ be a quasi-coherent $\mathcal{O}_X$-module. Then $\mathcal{M}$ is flat over S if and only if $f_*\mathcal{M}$ is flat over S.*

Proof. See [3, lemma 29.25.4]. □

[1] This notion is useless here, so we do not introduce it and we prefer the notion of coherence. There are already too many definitions in this document.

1.2.2 Degree of finite morphisms

Definition 1.27. A morphism of schemes $f : X \longrightarrow Y$ is *dominant* when $f(X)$ is dense in Y.

Lemma 1.28. *Let $f : X \longrightarrow Y$ be a dominant morphism of irreducible schemes, then f sends the generic point of f to the generic point of Y.*

Proof. Let η be the generic point of X. Then, $\overline{\{\eta\}} = X$, so $\overline{\{f(\eta)\}} = \overline{f(\overline{\{\eta\}})} = \overline{f(X)} = Y$ and $f(\eta)$ is the generic point of Y. □

Let $f : X \longrightarrow Y$ be a dominant morphism of integral schemes. Then f maps the generic point η of X to the generic point ξ of Y, so it yields a field homomorphism $k(X) = \mathcal{O}_{X,\eta} \longrightarrow k(Y) = \mathcal{O}_{Y,\xi}$. Then, $k(Y)/k(X)$ is a field extension. When f is finite, $f_*\mathcal{O}_X$ is a finite type $\mathcal{O}_Y$ module so this field extension is finite.

Definition 1.29. When f is finite the *degree* of f is:

$$\deg(f) := [k(Y) : k(X)]$$

Finite morphisms have finite (scheme theoretic) fibers. Actually, there is a formula relating $\deg(f)$ to is fibers when f is finite locally free. First, we need to study how the finite fibers look like.

Lemma 1.30. *Let X be a finite k-scheme of finite-type. Then:*

(i) *All points of X are closed (hence X is discrete and zero dimensional).*

(ii) *X is affine.*

(iii) $\Gamma(X, \mathcal{O}_X) = \prod_{x\in X} \mathcal{O}_{X,x}$.

(iv) $\Gamma(X, \mathcal{O}_X)$ *is a finite dimensional k-vector space and:*

$$dim_k\Gamma(X, \mathcal{O}_X) = \sum_{x\in X} e_x f_x$$

where for all $x \in X$:

$$e_x = e_x(X) := lg_{\mathcal{O}_{X,x}}(\mathcal{O}_{X,x}) \quad and \quad f_x = f_x(X) := [\kappa(x) : k]$$

are respectively ramification index *and the* inertia index *of X at x.*

Proof. Let U be the set of non-closed points of X. Then, $X \setminus U$ is a finite union of closed sets so it is closed and U is open. But closed points are (very) dense in X by [6, proposition 3.35] so U is either empty or contains a closed point which is a contradiction. We conclude that all points of X are closed. Then, every irreducible subset of X is a singleton and therefore $\dim(X) = 0$. Every singleton $\{x\} \subseteq X$ is a finite intersection of open subsets $\{x\} = \bigcap_{y\in X\setminus\{x\}} X \setminus \{y\}$ so $\{x\}$ is open and X is discrete. Hence (i).

Open affines form a basis of the topology of X so for all $x \in X$, $\{x\} = \mathrm{Spec}(R_x)$ for a certain k-algebra of finite type R_x. Obviously, $R_x = \lim\limits_{\{x\}\subseteq U} \Gamma(U, \mathcal{O}_X) = \mathcal{O}_{X,x}$ for all $x \in X$. We conclude that:

$$X = \bigsqcup_{x\in X} \mathrm{Spec}(\mathcal{O}_{X,x}) = \mathrm{Spec}\left(\prod_{x\in X} \mathcal{O}_{X,x}\right)$$

Hence (ii) and (iii).

Since $\dim(X) = 0$, $\Gamma(X, \mathcal{O}_X)$ is a k-algebra of finite type and Krull dimension zero so the Noether's normalization theorem ensures that $\Gamma(X, \mathcal{O}_X)$ is finite dimensional over k. By (iii), we have:

$$\dim_k\Gamma(X, \mathcal{O}_X) = \sum_{x\in X} \dim_k(\mathcal{O}_{X,x})$$

Let $x \in X$. Consider the chain of ideals $\cdots \subseteq \mathfrak{m}^{i+1} \subseteq \mathfrak{m}^i \subseteq \cdots \subseteq \mathfrak{m} \subseteq \mathcal{O}_{X,x}$, where $\mathfrak{m} := \mathfrak{m}_{X,x}$. $\mathcal{O}_{X,x}$ is finite dimensional so it is a Noetherian and Artin local ring and there exists $n \in \mathbb{N}^*$ such that $\mathfrak{m}^i = \{0\}$ for all $i \geq n$ (by [9, proposition 8.6]) and the chain is finite. Considering the exact sequence:

$$\{0\} \longrightarrow \mathfrak{m}^{i+1} \longrightarrow \mathfrak{m}^i \longrightarrow \mathfrak{m}^i/\mathfrak{m}^{i+1} \longrightarrow \{0\}$$

we get that $\dim_k(\mathfrak{m}^i) = \dim_k(\mathfrak{m}^{i+1}) + \dim(\mathfrak{m}^i/\mathfrak{m}^{i+1})$ and $\lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^i) = \lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^{i+1}) + \lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$, so that :

$$\dim_k(\mathcal{O}_{X,x}) = \sum_{i=0}^{n-1} \dim_k(\mathfrak{m}^i/\mathfrak{m}^{i+1}) \quad \text{and} \quad \lg_{\mathcal{O}_{X,x}}(\mathcal{O}_{X,x}) = \sum_{i=0}^{n-1} \lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$$

But for all $i \in \mathbb{N}$, $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a $\kappa(x) := \mathcal{O}_{X,x}/\mathfrak{m}$-vector space and $\lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = \dim_{\kappa(x)}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$, so that $\dim_k(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = [\kappa(x) : k]\lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = f_x \lg_{\mathcal{O}_{X,x}}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$ and $\dim_k(\mathcal{O}_{X,x}) = f_x e_x$. Hence (iv). □

Lemma 1.31. *Let $f : X \longrightarrow Y$ be a finite locally free morphism of integral schemes. Then:*

(i) *f is dominant (so deg(f) is well defined).*

(ii) *For all $y \in Y$, we have:*

$$deg(f) = dim_{\kappa(y)}\Gamma(X_y, \mathcal{O}_{X_y}) = \sum_{x \in X_y} e_{x/y} f_{x/y}$$

where $e_{x/y}$ and $f_{x/y}$ are respectively the ramification and inertia indices of X_y at x for all $x \in X_y$.

Proof. Since f is affine we may assume that X and Y are affine, write $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(S)$. Let $\theta : S \longrightarrow R$ be the ring homomorphism induced by f. Then, we have (by usual properties of the Zariski topology):

$$\begin{aligned}\overline{f(X)} &= V\left(\bigcap_{\mathfrak{q} \in f(X)} \mathfrak{q}\right) = V\left(\bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \theta^{-1}(\mathfrak{p})\right) = V\left(\theta^{-1}\left(\bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}\right)\right) \\ &= V(\theta^{-1}(\sqrt{\{0\}})) = V(\sqrt{\ker(\theta)}) = V(\ker(\theta))\end{aligned}$$

But f is locally free so θ induces a structure of free S-module over R and $\ker(\theta) = \{0\}$ and $f(X)$ is dense in Y. Hence (i).

(ii) The second equality was already proved in 1.30.(iv) (it makes sense because X_y is finite since f is finite), so we prove the first. R is a free S-module and by localizing at the generic point, we see that it is of rank $r := \deg(f)$. Let $y \in Y$. Then y corresponds to a prime ideal $\mathfrak{p} \subset S$ and we have:

$$X_y = X \times_Y \mathrm{Spec}(\kappa(y)) = \mathrm{Spec}(R \otimes_S S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}) = \mathrm{Spec}((R \otimes_S S/\mathfrak{p})_\mathfrak{p}) = \mathrm{Spec}((R/\mathfrak{p})_\mathfrak{p}) = \mathrm{Spec}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p})$$

Since R is a free S-module of rank $r = \deg(f)$, we get that $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ is a $\kappa(y) = S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$-vector space of dimension r, so that $\deg(f) = \dim_{\kappa(y)}\Gamma(X_y, \mathcal{O}_{X_y})$ and the proof is complete. □

1.2.3 Unramified and étale morphisms

Definition 1.32. Let R and S be Noetherian local rings. A local homomorphism $R \longrightarrow S$ is said to be *unramified* if:

(i) $\mathfrak{m}_R S = \mathfrak{m}_S$.

(ii) $\kappa(\mathfrak{m}_S)$ (residue field of S) is a finite separable extension of $\kappa(\mathfrak{m}_R)$ (residue field of R).

(iii) S is essentially of finite type over R (this means that S is the localization of a finite type R-algebra at a prime ideal).

Definition 1.33. Let Y be a locally Noetherian scheme and $f : X \longrightarrow Y$ be a morphism locally of finite type.

(i) One says that f is *unramified* at $x \in X$ if $f_x^{\#} : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$ is unramified.

(ii) On says that f is unramified if it is unramified at every point $x \in X$.

Remark 1.34. Actually, [3, definition 29.35.1] provides a more general equivalent definition of this notion involving differential modules but we will not use it. We follow [3, definition 41.3.5] here.

Lemma 1.35. *Let $f : X \longrightarrow Y$ be a morphism of k-schemes locally of finite type. Let $x \in X$ be a point. Set $y = f(x)$ and assume that $\kappa(y) = \kappa(x)$. Then the following are equivalent:*

(i) *The differential map $df_x : T_x(X) \longrightarrow T_y(Y)$ is injective.*

(ii) *f is unramified at x.*

Proof. See [3, lemma 33.16.8]. □

Definition 1.36. Let Y be a locally Noetherian scheme and $f : X \longrightarrow Y$ be a morphism locally of finite type. One says that f is *étale* if it is flat and unramified.

Proposition 1.37. *Assume k algebraically closed and let $f : X \longrightarrow Y$ be a finite locally free and unramified (i.e. étale) morphism of integral schemes. Then, for all k-valued point $y \in Y(k)$, we have $deg(f) = |X_y|$.*

Proof. Let $y \in Y(k)$. By lemma 1.31, we only have to prove that ramification and inertia indices are trivial $e_{x/y} = f_{x/y} = 1$ for all $x \in X_y$. For all $x \in X_y$, $\kappa(x)/\kappa(y) = k$ is finite because f is unramified so that $\kappa(x) = k$ because k is algebraically closed and $f_{x/y} = [\kappa(x) : k] = 1$.

As we saw in the proof of lemma 1.31, we may assume that $X = \text{Spec}(R)$, $Y = \text{Spec}(S)$ and that f is given by a ring homomorphism $\theta : S \longrightarrow R$ which is free and of finite type. $x \in X_y$ and y correspond to prime ideals $\mathfrak{p} \subseteq R$ and $\mathfrak{q} \subseteq S$ respectively and we have seen that $X_y = \text{Spec}(R_\mathfrak{q}/\mathfrak{q}R_\mathfrak{q})$. Then, $\mathcal{O}_{X_y,x} = (R_\mathfrak{q}/\mathfrak{q}R_\mathfrak{q})_\mathfrak{p} = (R_\mathfrak{q})_\mathfrak{p}/\mathfrak{q}(R_\mathfrak{q})_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$, but $S_\mathfrak{q} \longrightarrow R_\mathfrak{p}$ is unramified so $\mathfrak{q}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$ and finally $\mathcal{O}_{X_y,x} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \kappa(x)$ is a field so it is of length 1 and we have $e_{x/y} = 1$. This completes the proof. □

1.3 Invertible sheaves and divisors

1.3.1 Invertible sheaves

Throughout this paragraph, $(X, \mathcal{O}_X)$ will be a ringed space.

Definition 1.38. An *invertible $\mathcal{O}_X$-module* also called *invertible sheaf on X* is a locally free $\mathcal{O}_X$-module of rank 1.

Example 1.39. Let R be a graded ring. Take $X := \text{Proj}(R)$, and for $n \in \mathbb{N}$, $R(n) := \bigoplus_{d \geq n} R_d$ the ideal of R formed of elements of degree $\geq n$ and $\mathcal{O}_X(n) := \widetilde{R(n)}$, the sheaf associated to the R-module $R(n)$ as defined in [7, p. 116]. Then, $\mathcal{O}_X(n)$ is an invertible sheaf on X. $\mathcal{O}_X(1)$ is called the *twisted sheaf of Serre* on X.

Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{O}_X$-modules. We define $\text{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$ as the presheaf on X whose sections on a given open subset $U \subseteq X$ are morphisms of $\mathcal{O}_{X|U}$-modules $f : \mathcal{M}_{|U} \longrightarrow \mathcal{N}_{|U}$ i.e. morphisms of sheaves such that the induced morphisms $f_V : \mathcal{M}(V) \longrightarrow \mathcal{N}(V)$ are $\mathcal{O}_X(V)$-linear for all open subset $V \subseteq U$. Actually, $\text{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{N})$ is a sheaf.

The sheaf $\text{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{O}_X)$ is called the *dual* of $\mathcal{M}$ and denoted by $\mathcal{M}^\vee$.

Lemma 1.40. **(i)** *For all invertible $\mathcal{O}_X$-modules $\mathcal{L}$, $\mathcal{L}'$, $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}'$ is an invertible $\mathcal{O}_X$-module.*

(ii) *For all invertible $\mathcal{O}_X$-module $\mathcal{L}$, $\mathcal{L}^\vee$ is an invertible $\mathcal{O}_X$-module.*

(iii) *For all invertible $\mathcal{O}_X$-module $\mathcal{L}$, $\mathcal{L}^\vee \otimes_{\mathcal{O}_X} \mathcal{L} \simeq \mathcal{O}_X$.*

Proof. (i) For $x \in X$, there exist open neighborhoods $U, V \subseteq X$ of x such that $\mathcal{L}_{|U} \simeq \mathcal{O}_{X|U}$ and $\mathcal{L}'_{|V} \simeq \mathcal{O}_{X|V}$. Then, $W = U \cap V$ is an open neighborhood of x such that:

$$(\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}')_{|W} = \mathcal{L}_{|W} \otimes_{\mathcal{O}_{X|W}} \mathcal{L}'_{|W} \simeq \mathcal{O}_{X|W} \otimes_{\mathcal{O}_{X|W}} \mathcal{O}_{X|W} \simeq \mathcal{O}_{X|W}$$

by functoriality of the tensor product.

(ii) For $x \in X$, there exists an open neighborhood $U \subseteq X$ of x such that $\mathcal{L}_{|U} \simeq \mathcal{O}_{X|U}$. Then:

$$\mathcal{L}_{|U} = \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)_{|U} = \mathrm{Hom}_{\mathcal{O}_{X|U}}(\mathcal{L}_{|U}, \mathcal{O}_{X|U}) \simeq \mathrm{Hom}_{\mathcal{O}_{X|U}}(\mathcal{O}_{X|U}, \mathcal{O}_{X|U})$$

Then, we may assume that $X = U$ and we only have to prove that $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{O}_X) \simeq \mathcal{O}_X$. The morphism $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{O}_X) \longrightarrow \mathcal{O}_X$ given by:

$$f \in \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{O}_X)(U) \longmapsto f(1) \in \mathcal{O}_X(U)$$

for all open subset $U \subseteq X$ is an isomorphism whose inverse is given by:

$$a \in \mathcal{O}_X(U) \longmapsto (\lambda \longmapsto a\lambda) \in \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{O}_X)(U)$$

for all open subset $U \subseteq X$. This completes the proof of (ii).

(iii) We define an isomorphism on the presheaf $U \longmapsto \mathcal{L}^\vee(U) \otimes_{\mathcal{O}_X(U)} \mathcal{L}(U)$ to $\mathcal{O}_X$ by the formula:

$$f \otimes x \in \mathcal{L}^\vee(U) \otimes_{\mathcal{O}_X(U)} \mathcal{L}(U) \longmapsto f(x) \in \mathcal{O}_X(U)$$

for all open subset $U \subseteq X$. This morphism induces a morphism $\mathcal{L}^\vee \otimes_{\mathcal{O}_X} \mathcal{L} \longrightarrow \mathcal{O}_X$ by the universal property of the associated sheaf [6, proposition 2.24]. It suffices to prove that this morphism is isomorphic on the stalks (by [7, Proposition II.1.1]), but the induced morphism of the stalk at $x \in X$ is:

$$f_x \otimes \lambda_x \in \mathcal{L}_x^\vee \otimes_{\mathcal{O}_{X,x}} \mathcal{L}_x \longmapsto f_x(\lambda_x) \in \mathcal{O}_{X,x}$$

which is an isomorphism because $\mathcal{L}_x \simeq \mathcal{L}_x^\vee \simeq \mathcal{O}_{X,x}$. □

This lemma ensures that the tensor product defines a group law on the isomorphism classes of invertible sheaves on X and that the inverse of $[\mathcal{L}]$ is $[\mathcal{L}^\vee]$ for all invertible sheaf $\mathcal{L}$. That is why $\mathcal{L}^\vee$ will often be denoted by $\mathcal{L}^{-1}$ or $\mathcal{L}^{\otimes -1}$. In the same spirit, we will denote $\mathcal{L}^{\otimes n}$ the n-th exponentiation of $\mathcal{L}$ (given $n \in \mathbb{Z}$). The group of these isomorphism classes is called the *Picard group* of X and denoted by $\mathrm{Pic}(X)$. On says that an invertible sheaf $\mathcal{L}$ is *trivial* if it corresponds to the neutral element of $\mathrm{Pic}(X)$ i.e. if $\mathcal{L} \simeq \mathcal{O}_X$.

Lemma 1.41. *Let X, Y be two locally ringed spaces, $\mathcal{L}$ be an invertible sheaf on Y and $f : X \longrightarrow Y$ a morphism of locally ringed spaces. Then:*

(i) *$f^*\mathcal{L} = \mathcal{O}_X \otimes_{f^{-1}\mathcal{O}_Y} f^{-1}\mathcal{L}$ is an invertible sheaf on X.*

(ii) *If f is constant, then $f^*\mathcal{L}$ is trivial.*

Proof. (i) Let $x \in X$. Then, there exists an open neighborhood $V \subseteq Y$ of $f(x)$ such that $\mathcal{L}_{|V} \simeq \mathcal{O}_{Y|V}$. Let $U := f^{-1}(V)$. Then, the restriction to U of the presheaves $f^+\mathcal{L} : W \longmapsto \varinjlim_{f(W) \subseteq T \subseteq Y} \mathcal{L}(T)$ and

$f^+\mathcal{O}_Y : W \longmapsto \lim_{f(W)\subseteq T\subseteq Y} \mathcal{O}_Y(T)$ are isomorphic. It is the same for their associated sheaves $f^{-1}\mathcal{L}_{|U}$ and $f^{-1}\mathcal{O}_{Y|U}$ (by [6, proposition 2,24]) and we conclude immediately that:

$$f^*\mathcal{L}_{|U} = \mathcal{O}_{X|U} \otimes_{f^{-1}\mathcal{O}_{Y|U}} f^{-1}\mathcal{L}_{|U} \simeq \mathcal{O}_{X|U} \otimes_{f^{-1}\mathcal{O}_{Y|U}} f^{-1}\mathcal{O}_{Y|U} \simeq \mathcal{O}_{X|U}$$

Which completes the proof.

(ii) If f is constant equal to $y \in Y$, we may choose an open neighborhood $V \subseteq Y$ of y on which $\mathcal{L}$ is trivial. Then, $f^{-1}(V) = X$ and as we have seen in the proof of (i), $f^{-1}\mathcal{L} \simeq f^{-1}\mathcal{O}_Y$ on the whole of X and $f^*\mathcal{L} \simeq \mathcal{O}_X \otimes_{f^{-1}\mathcal{O}_Y} f^{-1}\mathcal{O}_Y \simeq \mathcal{O}_X$. □

Now, we state a theorem on invertible sheaves with deep consequences for the theory of abelian varieties. As its proof is long and not at the center of this seminar, we will not prove it here.

Theorem 1.42 (theorem of the cube). *Let X, Y, Z be three geometrically irreducible k-varieties. We assume that X and Y are complete. Let $\mathcal{L}$ be an invertible sheaf on $X \times Y \times Z$, $x_0 \in X(k)$, $y_0 \in Y(k)$ and $z_0 \in Z(k)$ such that $\mathcal{L}$ is trivial on $X \times Y \times \{z_0\}$, $X \times \{y_0\} \times Z$ and $\{x_0\} \times Y \times Z$. Then, $\mathcal{L}$ is trivial on $X \times Y \times Z$.*

Proof. See [2, p.55 or p.91]. □

1.3.2 Divisors on a normal variety

Throughout this paragraph, X is a fixed normal k-variety. The *group of divisors* on X, denoted by $\mathrm{Div}(X)$ is the free abelian group generated by irreducible closed subvarieties of codimension 1 in X. A *prime divisor* is a closed subvariety of codimension 1 in X. A *divisor* on X is an element $D \in \mathrm{Div}(X)$. It can be written as a finite sum of prime divisors:

$$D = \sum_{Z\in P(X)} n_Z[Z]$$

where $P(X)$ is the set of prime divisors of X and $(n_Z)_{Z\in I^1(X)} \in \mathbb{Z}^{(I^1(X))}$ is a family of integers with finitely many nonzero elements. The *support* of D denoted by $\mathrm{Supp}(D)$ is the reunion:

$$\mathrm{Supp}(D) := \bigcup_{\substack{Z\in P(X)\\ n_Z\neq 0}} Z$$

D is said *positive* and we denote $D \geq 0$ when $n_Z \geq 0$ for all $Z \in P(X)$. There is a (partial) order relation $\leq$ on $\mathrm{Div}(X)$ induced by comparison of the coefficients: if D and D' are divisors on X, then $D \leq D'$ if and only if the difference $D' - D$ is positive.

X being normal, it is integral, so it is irreducible. Then, we can consider the function field $k(X)$. We will now explain how to associate divisors to rational functions of $k(X)$. As a complex analysis analogue, irreducible closed subvarieties of codimension 1 will play the roles of zeros or poles and the coefficients will correspond the orders of these zeros and poles.

Then, for all $Z \in P(X)$, we need to define a discrete valuation $\mathrm{ord}_Z : k(X) \longrightarrow \mathbb{Z} \cup \{\infty\}$. Let us fix $Z \in P(X)$ and η the generic point of Z. Let U be an open affine $U = \mathrm{Spec}(R)$ of X intersecting Z, then $\eta \in U$. $Z \cap U$ is a maximal proper and closed subset of U and $\overline{\{\eta\}} = Z \cap U$ so η corresponds to a minimal nonzero prime ideal of R, so $\mathcal{O}_{X,\eta} = R_\eta$ is a normal ring of dimension 1, so [9, proposition 9.2] ensures that is a discrete valuation ring. This defines the valuation ord_Z we sought, which does not depend on the choice of U. If $D := \sum_{Z\in P(X)} n_Z[Z] \in \mathrm{Div}(X)$, we will sometimes denote $\mathrm{ord}_Z(D) := n_Z$ by abuse of notations.

For all $f \in k(X)^*$, we associate a divisor to f as follows:

$$\operatorname{div}(f) = \sum_{Z \in P(X)} \operatorname{ord}_Z(f)[Z]$$

It is well defined according to the following lemma.

Lemma 1.43. *For $f \in k(X)^*$, $ord_Z(f) \neq 0$ for finitely many prime divisors $Z \in P(X)$.*

Proof. X is a k-variety so it is quasi-compact, so it can be covered by finitely many open subsets, so we can suppose X affine $X = \operatorname{Spec}(R)$. Then, $f \in \operatorname{Frac}(R)$ and we can write $f = \frac{g}{h}$ with $g, h \in R \setminus \{0\}$, so that for all prime divisor Z, $\operatorname{ord}_Z(f) = \operatorname{ord}_Z(g) - \operatorname{ord}_Z(h)$ and we can therefore assume that $f \in R \setminus \{0\}$.

For any prime divisor Z, $\operatorname{ord}_Z(f) \neq 0$ if and only if f is in the maximal ideal ηR_η of the local ring $\mathcal{O}_{X,\eta} = R_\eta$, where η is the generic point of Z. Then:

$$\operatorname{ord}_Z(f) \neq 0 \Longleftrightarrow f \in \eta \Longleftrightarrow \eta \in V(f) \Longleftrightarrow Z = \overline{\{\eta\}} \subseteq V(f)$$

Since $f \in R \setminus \{0\}$ and R is an integral domain, $V(f)$ is either empty (when f is invertible) or of codimension 1 so every prime divisor $Z \subseteq V(f)$ is an irreducible component of $V(f)$. But there are finitely many because R is Noetherian (as a finite-type k-algebra), so $X = \operatorname{Spec}(R)$ is a Noetherian topological space and $V(f)$ as well (since it is closed). □

A divisor of the form $\operatorname{div}(f)$ for $f \in k(X)^*$ is called *principal.* Principal divisors form a subgroup of $\operatorname{Div}(X)$ denoted by $\operatorname{Princ}(X)$. When X is smooth, will see later that the quotient $\operatorname{Div}(X)/\operatorname{Princ}(X)$ is isomorphic to the Picard group of X. We say that two divisors D and D' are *linearly equivalent* and denote $D \sim D'$ when their difference $D - D'$ is principal.

If U is an open subset of X, then for every prime divisor $Z \in P(X)$ intersecting U ($U \cap Z \neq \emptyset$), $U \cap Z$ is of codimension 1 in U so $U \cap Z \in P(U)$. Therefore, if $D = \sum_{Z \in P(X)} n_Z[Z]$ is a divisor on X, we can define the *restriction* of D to U as follows:

$$D_{|U} := \sum_{\substack{Z \in P(X) \\ U \cap Z \neq \emptyset}} n_Z[Z \cap U]$$

We say that D is *locally principal* if every point $x \in X$ admits an open neighborhood $U \subseteq X$ such that $D_{|U}$ is principal. If $f \in k(X)^*$ is such that $D_{|U} = \operatorname{div}(f)$, f is called a *local equation* of D on U.

Proposition 1.44. *If X is regular, then every divisor on X is locally principal. It is in particular true when X is smooth.*

Proof. By linearity, we only have to prove this for principal divisors on X. Let Z be a principal divisor and $x \in X$. If $x \notin Z$, then $U = X \setminus Z$ is an open neighborhood of x and $[Z]_{|U} = 0 = \operatorname{div}(1)$, so we can assume that $x \in Z$.

Let $U = \operatorname{Spec}(R)$ be an open affine neighborhood of x. Then, $Z \cap U$ is a maximal proper irreducible closed subset of U, so there exists a minimal nonzero prime ideal $\mathfrak{q}$ of R such that $Z \cap U = V(\mathfrak{q})$. Let $\mathfrak{p}$ be the prime ideal corresponding to x. Then, $\mathfrak{p} \in V(\mathfrak{q})$ (because $x \in Z$) i.e. $\mathfrak{q} \subseteq \mathfrak{p}$ so $\mathfrak{q}R_\mathfrak{p}$ is a minimal nonzero prime ideal of the local ring $R_\mathfrak{p} = \mathcal{O}_{X,x}$.

By hypothesis, $R_\mathfrak{p}$ is regular so it is a unique factorization domain by theorem 1.17. Since $\mathfrak{q} \neq 0$, there exists $a \in \mathfrak{q}R_\mathfrak{p} \setminus \{0\}$. We can decompose it in irreducible factors and we get that one of these factors π is in $\mathfrak{q}R_\mathfrak{q}$ (as it is a prime ideal). Since $\pi R_\mathfrak{p}$ is prime and nonzero, we must have $\mathfrak{q}R_\mathfrak{p} = \pi R_\mathfrak{p}$ (by minimality of $\mathfrak{q}R_\mathfrak{p}$). π remains irreducible and a generator of $\mathfrak{q}$ when we multiply it by an element of $R \setminus \mathfrak{p}$, so we can assume $\pi \in R$. Hence, $\pi R = \pi R_\mathfrak{p} \cap R = \mathfrak{q}R_\mathfrak{p} \cap R = \mathfrak{q}$.

Since $\mathfrak{q}$ is the generic point of Z and π is a generator of $\mathfrak{q}$ (and therefore, a uniformizer in $R_\mathfrak{q} = \mathcal{O}_{X,\mathfrak{q}}$), we must have $\operatorname{ord}_Z(\pi) = 1$. If Z' is another prime divisor of X intersecting U, then we may write

$Z' \cap U = V(\mathfrak{r})$ where $\mathfrak{r}$ is a prime ideal of height 1 of R. If $\text{ord}_{Z'}(\pi) > 0$, then $\pi \in \mathfrak{r}$ so $\mathfrak{q} = \pi A \subseteq \mathfrak{r}$ and $\mathfrak{q} = \mathfrak{r}$ since $\text{ht}(\mathfrak{q}) = \text{ht}(\mathfrak{r}) = 1$ and finally $Z' = Z$. Then, $\text{div}(\pi) = [Z \cap U] = [Z]_{|U}$, which completes the proof. □

1.3.3 Correspondence between divisors and invertible sheaves

Let X be an integral smooth k-variety. Let D be a divisor on X. We define the *vector space associated to* D as follows:

$$L(D) := \{f \in k(X)^* \mid \text{div}(f) + D \geq 0\} \cup \{0\}$$

Generalizing this definition, we can furthermore associate to D a sheaf $\mathcal{L}(D)$ defined on X. For all open subset $U \subseteq X$:

$$\Gamma(U, \mathcal{L}(D)) := \{f \in k(X)^* \mid \text{div}(f)_{|U} + D_{|U} \geq 0\} \cup \{0\}$$

If $V \subseteq U$ is an open subset, then we have the trivial inclusion $\Gamma(V, \mathcal{L}(D)) \subset \Gamma(U, \mathcal{L}(D))$, so we have natural restriction maps and we have built a presheaf structure for $\mathcal{L}(D)$ (for now, in the category of k-vector spaces). Actually, $\mathcal{L}(D)$ is a sheaf. Furthermore, if $f \in \Gamma(U, \mathcal{L}(D))$, multiplying f by an element of $\Gamma(U, \mathcal{O}_X)$ only increases $\text{ord}_Z(f)$ for every prime divisor Z of U, so $\Gamma(U, \mathcal{L}(D))$ is stable by scalar multiplication by elements of $\Gamma(U, \mathcal{O}_X)$. As a consequence, $\mathcal{L}(D)$ is an $\mathcal{O}_X$-module.

Lemma 1.45. *$\mathcal{L}(D)$ is an invertible sheaf on X.*

Proof. Let $x \in X$. Since X is smooth, by proposition 1.44, there exists an open neighborhood U of x and a local equation $g \in k(X)^*$ for D on U: $D_{|U} = \text{div}(g)$. Then, for all open subset $V \subseteq U$:

$$\Gamma(V, \mathcal{L}(D)) = \{f \in k(X)^* \mid \text{div}(fg)_{|V} \geq 0\} \cup \{0\}$$

and we have an injective homomorphism:

$$\varphi_V : f \in \Gamma(V, \mathcal{L}(D)) \longmapsto fg \in k(X)$$

To conclude, we just have to prove that $\text{im}(\varphi_V) \subseteq \Gamma(V, \mathcal{O}_X)$, because it will ensure that the above map is an isomorphism $\Gamma(V, \mathcal{L}(D)) \simeq \Gamma(V, \mathcal{O}_X)$ and $\mathcal{L}(D)_{|U} \simeq \mathcal{O}_{X|U}$, as desired.

For $f \in k(X)^*$, it suffices to prove that $f \in \Gamma(V, \mathcal{O}_X)$ whenever $\text{div}(f)_{|V} \geq 0$. Let f be such a function. We only have to show that V is covered by open subsets U_i such that $f_{|U_i} \in \Gamma(U_i, \mathcal{O}_X)$. Let $y \in V$. Then, there exists an open affine neighborhood $W \subseteq V$ of y. y corresponds to a prime ideal $\mathfrak{p}$ of $R := \Gamma(W, \mathcal{O}_X)$. If $\mathfrak{p} = \{0\}$, then y is the generic point of X (an W) which intersects every open subset of X, so we can assume $\mathfrak{p} \neq \{0\}$. In that case, there exists a minimal nonzero prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$, so that $Z = V(\mathfrak{q})$ is a prime divisor of W and we have $\text{ord}_Z(f) \geq 0$ so $f \in R_{\mathfrak{q}}$ so we can write $f := \frac{a}{b}$ with $a \in R$ and $b \in R \setminus \mathfrak{q}$, so that $f \in R[1/b] = \Gamma(D(b), \mathcal{O}_X)$. But $b \notin \mathfrak{q} \subseteq \mathfrak{p}$ so $y = \mathfrak{p} \in D(b)$. This completes the proof. □

Remark 1.46. With the ideas of the preceding proof, we obtain that $\mathcal{L}(D)$ is trivial when D is principal.

Actually, the converse is true. More precisely, we will construct a group isomorphism between the quotient $\text{Div}(X)/\text{Princ}(X)$ and $\text{Pic}(X)$.

Lemma 1.47. *For $D, D' \in Div(X)$, $\mathcal{L}(D) \otimes \mathcal{L}(D') \simeq \mathcal{L}(D + D')$.*

Proof. For every open subset $U \subseteq X$, we have a $\Gamma(U, \mathcal{O}_X)$-bilinear map:

$$(f, g) \in \Gamma(U, \mathcal{L}(D)) \times \Gamma(U, \mathcal{L}(D')) \longmapsto fg \in \Gamma(U, \mathcal{L}(D + D'))$$

which factors into $\varphi_U : \Gamma(U, \mathcal{L}(D)) \otimes \Gamma(U, \mathcal{L}(D')) \longrightarrow \Gamma(U, \mathcal{L}(D + D'))$. This defines a morphism of $\mathcal{O}_X$-modules $\varphi : \mathcal{L}(D) \otimes \mathcal{L}(D') \longrightarrow \mathcal{L}(D + D')$.

If U is small enough, then there exist local equations $h, h' \in k(X)^*$ on U for D and D': $D_{|U} = \mathrm{div}(h)_{|U}$ and $D'_{|U} = \mathrm{div}(h')_{|U}$. Then, for all $k \in \Gamma(U, \mathcal{L}(D + D')) \setminus \{0\}$, we have:

$$0 \leq D_{|U} + D'_{|U} + \mathrm{div}(k)_{|U} = \mathrm{div}(kh') + D_{|U}$$

so $kh' \in \Gamma(U, \mathcal{L}(D))$ and $\mathrm{div}(1/h')_{|U} + D'_{|U} = \mathrm{div}(1/h' \cdot h') = \mathrm{div}(1) = 0$ so $1/h' \in \Gamma(U, \mathcal{L}(D'))$ and we have $\varphi_U(kh' \otimes 1/h') = k$. Whence, φ_U is surjective.

Moreover, as we saw in the proof of the lemma 1.45, $\Gamma(U, \mathcal{L}(D))$, $\Gamma(U, \mathcal{L}(D'))$ and $\Gamma(U, \mathcal{L}(D+D'))$ are $\Gamma(U, \mathcal{O}_X)$-modules of rank 1, so $\Gamma(U, \mathcal{L}(D)) \otimes \Gamma(U, \mathcal{L}(D')) \simeq \Gamma(U, \mathcal{O}_X)$ as modules. It follows that $\ker(\varphi_U)$ is of rank 0. Since $\Gamma(U, \mathcal{O}_X)$ is integral, it is torsion free so $\ker(\varphi_U) = \{0\}$ and φ_U is an isomorphism. Since D and D' are locally principal, those open subsets U's cover X and we conclude that φ is an isomorphism. □

By the preceding lemma, we have a group homomorphism $\mathrm{Div}(X) \longrightarrow \mathrm{Pic}(X)$ sending D to $[\mathcal{L}(D)]$. Actually, it induces a homomorphism $\mathrm{Div}(X)/\mathrm{Princ}(X) \longrightarrow \mathrm{Pic}(X)$.

Proposition 1.48. *The preceding homorphism $Div(X)/Princ(X) \longrightarrow Pic(X)$ is an isomorphism.*

Proof. **Injectivity:** Let $D \in \mathrm{Div}(X)$ such that $\mathcal{L}(D)$ is trivial and $\varphi : \mathcal{O}_X \longrightarrow \mathcal{L}(D)$ an isomorphism of sheaves. Let $g := \varphi_X(1)$. Then, $g \in \mathcal{L}(D)$ so $\mathrm{div}(g) + D \geq 0$. Moreover, if $U \subseteq X$ is an open subset on which D is principal, we write $D_{|U} = \mathrm{div}(f)_{|U}$, so that $1/f \in \Gamma(U, \mathcal{L}(D))$ because $\mathrm{div}(1/f)_{|U} + D_{|U} = 0$. Since φ_U is surjective, there exists $h \in \Gamma(U, \mathcal{O}_X)$ such that $1/f = \varphi_U(h) = h\varphi_U(1) = hg_{|U}$. We conclude that:

$$-D_{|U} = \mathrm{div}(1/f)_{|U} = \mathrm{div}(h)_{|U} + \mathrm{div}(g)_{|U} \geq \mathrm{div}(g)_{|U}$$

where we used the fact that $\mathrm{div}(h)_{|U}$ is positive because $h \in \Gamma(U, \mathcal{O}_X)$. Then, $D_{|U} + \mathrm{div}(g)_{|U} \leq 0$ and the open subsets U on which D is principal cover X (by proposition 1.44), so $D + \mathrm{div}(g) \leq 0$. Hence, $D + \mathrm{div}(g) = 0$ and D is principal.

Surjectivity: Let $\mathcal{L}$ be an invertible sheaf on X and $\mathcal{K}$ be the constant sheaf on X given by $\Gamma(U, \mathcal{K}) := k(X)$ for every nonempty open subset $U \subseteq X$. Let η be the generic point of X (it does exist because X is irreducible). Then, we have a natural morphism $\mathcal{L} \longrightarrow \mathcal{K}$ sending a section $s \in \mathcal{L}(U)$ (for a given non-empty open subset $U \subseteq X$) to the germ $s_\eta \in \mathcal{L}_\eta \simeq \mathcal{O}_{X,\eta} = k(X) = \mathcal{K}(U)$.

This map is injective. Indeed, let $s \in \mathcal{L}(U)$ such that $s_\eta = 0$. Then, we can cover U with a family of open affines $(U_i)_{i \in I}$ such that $\mathcal{L}_{|U_i} \simeq \mathcal{O}_{X|U_i}$ for all $i \in I$. Let $i \in I$ and $A_i := \Gamma(U_i, \mathcal{O}_X)$. Since X is integral, A_i is an integral domain, we have $\eta \in U_i = \mathrm{Spec}(A_i)$ and η corresponds to the zero prime ideal, so that $s_{|U_i}$ is zero in $\mathcal{O}_{X,\eta} = \mathrm{Frac}(A_i)$ so $s_{|U_i} = 0$. Since the U_i cover U, we have $s = 0$.

Then, we have an embedding $\mathcal{L} \hookrightarrow \mathcal{K}$ and we can suppose that $\mathcal{L}$ is a subsheaf of $\mathcal{K}$. But X is covered by open subsets $(V_i)_{i \in I}$ such that $\mathcal{L}_{|V_i} \simeq \mathcal{O}_{X|V_i}$ for all $i \in I$. Let $i \in I$ and $\varphi_i : \mathcal{O}_{X|V_i} \longrightarrow \mathcal{L}_{|V_i}$ be an isomorphism and let $g_i := \varphi_{i,V_i}(1)$. Then, $\mathcal{L}(V_i) = g_i\Gamma(V_i, \mathcal{O}_X)$, $g_i \in \mathcal{K}(V_i) = k(X)$ and $g_i \neq 0$. Furthermore, for all $i, j \in I$, $\mathcal{L}(V_i \cap V_j) = g_i\Gamma(V_i \cap V_j, \mathcal{O}_X) = g_j\Gamma(V_i \cap V_j, \mathcal{O}_X)$. It follows that $g_i = u_{i,j}g_j$ for a certain $u_{i,j} \in \Gamma(V_i \cap V_j, \mathcal{O}_X)^\times$ and that $\mathrm{ord}_{Z \cap V_i \cap V_j}(g_i) = \mathrm{ord}_{Z \cap V_i \cap V_j}(g_j)$ for every prime divisor Z of X, so there exists a divisor $D \in \mathrm{Div}(X)$ such that $D_{|V_i} := \mathrm{div}(g_i)_{|V_i}$ for all $i \in I$. We conclude that $\mathcal{L} = \mathcal{L}(D)$. □

1.3.4 Projective embeddings

Definition 1.49. Let X be a scheme and $\mathcal{M}$ be an $\mathcal{O}_X$-module. One says that a family of global sections $(s_i)_{i \in I} \in \Gamma(X, \mathcal{M})^I$ *generates* $\mathcal{M}$ if for all $x \in X$, $((s_i)_x)_{i \in I}$ generates $\mathcal{M}_x$ as an $\mathcal{O}_{X,x}$-module.

Example 1.50. Let R be a ring. On $X := \mathbb{P}^n_R = \mathrm{Proj}(R[T_0, \cdots, T_n])$, recall that we have the twisted sheaf of Serre $\mathcal{O}(1) := \widetilde{M}$, where $M := \sum_{i=0}^n T_iR[T_0, \cdots, T_n]$ (see example 1.39). Then, the global sections $T_0, \cdots, T_n \in \Gamma(X, \mathcal{O}(1))$ generate $\mathcal{O}(1)$.

We will now study the link between invertible sheaves and projective embeddings. Consider a morphism of R-schemes $\varphi : X \longrightarrow \mathbb{P}^n_R$ and the $\mathcal{O}_X$-module $\mathcal{L} := \varphi^*\mathcal{O}(1)$, which is an invertible sheaf (by lemma 1.41.(i)).

Let us explain how to pull-back sections. Let X_1 be a scheme and $\mathcal{M}$ an $\mathcal{O}_{X_1}$-module. One notices that every global section $s \in \Gamma(X_1, \mathcal{M})$ induces a morphism of sheaves $\hat{s} : \mathcal{O}_{X_1} \longrightarrow \mathcal{M}$ given by $\hat{s}_U(\lambda) := \lambda \cdot s_{|U}$ for all open subset $U \subseteq X_1$ and all section $\lambda \in \Gamma(U, \mathcal{O}_{X_1})$. Conversely, every morphism $\phi : \mathcal{O}_{X_1} \longrightarrow \mathcal{M}$ is of the form $\phi = \hat{s}$ where $s := \phi_X(1)$. If $f : X_2 \longrightarrow X_1$, we can apply the pull-back functor to obtain $f^*\hat{s} : f^*\mathcal{O}_{X_1} = \mathcal{O}_{X_2} \longrightarrow f^*\mathcal{M}$ and take $f^*(s) := f^*\hat{s}(1)$.

Taking $X_1 := \mathbb{P}^n_R$ and $X_2 := X$, we get a morphism of $\Gamma(\mathbb{P}^n_R, \mathcal{O}_{\mathbb{P}^n_R})$-modules between the global sections $\varphi^* : \Gamma(\mathbb{P}^n_R, \mathcal{O}(1)) \longrightarrow \Gamma(X, \mathcal{L})$. It is easy to see that the global sections $s_i := \varphi^*(T_i)$ ($i \in [\![0\ ;\ n]\!]$) generate $\mathcal{L}$. Conversely, one can reconstruct φ knowing $\mathcal{L}$ and the global sections s_i.

Theorem 1.51. *Let R be a ring and X be a R-scheme. Let $\mathcal{L}$ be an invertible sheaf on X generated by global sections $s_0, \cdots, s_n$. Then, there exists a unique morphism of R-schemes $\varphi : X \longrightarrow \mathbb{P}^n_R$ such that $\mathcal{L} \simeq \varphi^*\mathcal{O}(1)$ and $s_i = \varphi^*(T_i)$ for all $i \in [\![0\ ;\ n]\!]$.*

Proof. For each $i \in [\![0\ ;\ n]\!]$, let $X_i := \{x \in X \mid (s_i)_x \notin \mathfrak{m}_{X,x}\mathcal{L}_x\}$. Then, X_i is an open subset. Indeed, if $x \in X_i$, then x admits an open affine neighborhood $U := \operatorname{Spec}(R)$ in X such that $\mathcal{L}_{|U} \simeq \mathcal{O}_{X|U}$, so that for every point $\mathfrak{p} \in U$ (which corresponds to a prime ideal of R), $\mathcal{L}_\mathfrak{p} \simeq R_\mathfrak{p}$ (as R-modules) and $\mathfrak{m}_{X,\mathfrak{p}}\mathcal{L}_\mathfrak{p} \simeq \mathfrak{m}_{X,\mathfrak{p}} = \mathfrak{p}R_\mathfrak{p}$, so that $X_i \cap U = \{\mathfrak{p} \in U \mid (s_i)_{|U} \notin \mathfrak{p}\} = D((s_i)_{|U})$, which is an open neighborhood of x.

Furthermore, $X = \bigcup_{i=0}^n X_i$. Otherwise, since the s_i generate $\mathcal{L}$, we would have a point $x \in X$ such that $\mathfrak{m}_{X,x}\mathcal{L}_x = \mathcal{L}_x$ so that $\mathcal{L}_x = \{0\}$ by Nakayama's lemma [9, proposition 2.6], which is impossible because $\mathcal{L}_x \simeq \mathcal{O}_{X,x}$ and $\mathcal{O}_{X,x}$ is a local ring (so is not zero).

For all $i \in [\![0\ ;\ n]\!]$, let $U_i := D(T_i) = \{\mathfrak{p} \in \mathbb{P}^n_R \mid T_i \notin \mathfrak{p}\}$. Since $U_i = \operatorname{Spec}(R[T_0/T_i, \cdots, T_n/T_i])$, by [6, proposition 3.4] it suffices to define a homomorphism $\phi_i : R[T_0/T_i, \cdots, T_n/T_i] \longrightarrow \Gamma(X_i, \mathcal{O}_X)$ to define a morphism of scheme $\varphi_i : X_i \longrightarrow U_i$. The idea here is to set $\phi_i(T_j/T_i) := s_j/s_i$ for all $j \in [\![0\ ;\ n]\!]$ but the quotient needs to be properly defined in $\Gamma(X_i, \mathcal{O}_X)$.

Since $\mathcal{L}$ is an invertible sheaf, X_i admits an open covering $(V_e)_{e \in \mathcal{E}}$ such that for all $e \in \mathcal{E}$, there exists an isomorphism of $\mathcal{O}_{X|V_e}$-modules $\theta_e : \mathcal{L}_{|V_e} \longrightarrow \mathcal{O}_{X|V_e}$. For all $e \in \mathcal{E}$ and $x \in V_e$, $(s_i)_x \notin \mathfrak{m}_{X,x}\mathcal{L}_x$, so $\theta_{e,V_e}((s_i)_{|V_e})_x \notin \mathfrak{m}_{X,x}$ and this section is locally invertible and local inverses coincide (by unicity) so we can lift local inverses by the sheaf properties of $\mathcal{O}_X$ so that $\theta_{e,V_e}((s_i)_{|V_e})$ is invertible. Furthermore, for all $e, f \in \mathcal{E}$, we have $\theta_{e,V_e \cap V_f} = \theta_{e,V_e \cap V_f}(\theta^{-1}_{f,V_e \cap V_f}(1))\theta_{f,V_e \cap V_f}$, so that:

$$\forall j \in [\![0\ ;\ n]\!], \quad \left(\frac{\theta_{e,V_e}(s_j)}{\theta_{e,V_e}(s_i)}\right)_{|V_e \cap V_f} = \left(\frac{\theta_{f,V_f}(s_j)}{\theta_{f,V_f}(s_i)}\right)_{|V_e \cap V_f}$$

and there exists $t_{i,j} \in \Gamma(X_i, \mathcal{O}_X)$ such that $t_{i,j|V_e} = \theta_{e,V_e}(s_j)/\theta_{e,V_e}(s_i)$ for all $e \in \mathcal{E}$ and we can set $\phi_i(T_j/T_i) := t_{i,j}$. Later, we will denote s_j/s_i instead of $t_{i,j}$ by abuse of notations.

To define a morphism $\varphi : X \longrightarrow \mathbb{P}^n_R$ globally, we glue the φ_i. By [6, proposition 3.5] it suffices to verify that $(\varphi_i)_{X_i \cap X_j} = (\varphi_j)_{X_i \cap X_j}$ for all $i, j \in [\![0\ ;\ n]\!]$. Since:

$$U_i \cap U_j = D(T_iT_j) = \operatorname{Spec}(R[T_0/T_i, \cdots, T_n/T_i][T_i/T_j]) = \operatorname{Spec}(R[T_0/T_j, \cdots, T_n/T_j][T_j/T_i])$$

we only have to verify that the ring homomorphisms $R[T_0/T_i, \cdots, T_n/T_i][T_i/T_j] \longrightarrow \Gamma(X_i \cap X_j, \mathcal{O}_X)$ induced by φ_i and φ_j coincide, which is true by construction.

It remains to identify $\varphi^*\mathcal{O}(1)$ with $\mathcal{L}$. Let $\psi : \varphi^*\mathcal{O}(1) \longrightarrow \mathcal{L}$ mapping $\varphi^*(T_i)_{|U}$ to $(s_i)_{|U}$ for all $i \in [\![0\ ;\ n]\!]$ and for all open subset $U \subseteq X$. It suffices to prove that ϕ induces an isomorphism on the stalks. Let $x \in X$ and $i \in [\![0\ ;\ n]\!]$ such that $x \in X_i$. Then $\mathfrak{p} := \varphi(x)$ is a prime ideal of $S := R[T_0/T_i, \cdots, T_n/T_i]$ and we have:

$$\varphi^*\mathcal{O}(1)_x \simeq \mathcal{O}_{X,x} \otimes_{S_\mathfrak{p}} T_iS_\mathfrak{p}$$

Clearly ψ_x maps $\varphi^*(T_j)_x = 1 \oplus T_j$ to s_j for all $j \in [\![0 \; ; \; n]\!]$, so ϕ_x is surjective because the s_j generate $\mathcal{L}$. In addition, every element of $\varphi^*\mathcal{O}(1)$ is a sum of elements the form:

$$\lambda \otimes T_i f(T_0/T_i, \cdots, T_n/T_i) = \lambda f((s_0)_x/(s_i)_x, \cdots, (s_n)_x/(s_i)_x) \otimes T_i$$

where $\lambda \in \mathcal{O}_{X,x}$ and $f \in S_\mathfrak{p}$ is a rational fraction whose denominator is not in $\mathfrak{p}$, so every element of $\varphi^*\mathcal{O}(1)$ is of the form $\lambda \otimes T_i$ (where $\lambda \in \mathcal{O}_{X,x}$). Let $\lambda \in \mathcal{O}_{X,x}$ such that $\lambda \otimes T_i$ is sent to zero via ψ_x. Then $\lambda(s_i)_x = 0$. But the $(s_j)_x$ generate $\mathcal{L}_x$ and any linear combination of such elements can be factored by $(s_i)_x$, so that $\mathcal{L}_x = \mathcal{O}_{X,x}(s_i)_x$. Since $\mathcal{L}$ is invertible, there is an isomorphism $\theta_x : \mathcal{L}_x \longrightarrow \mathcal{O}_{X,x}$. Let $\mu \in \mathcal{O}_{X,x}$ such that $\theta_x^{-1}(1) = \mu(s_i)_x$. Then, $\theta_x^{-1}(\lambda) = \lambda\theta_x^{-1}(1) = \lambda\mu(s_i)_x = 0$, so that $\lambda = 0$. Hence the injectivity of ϕ_x. Then, $\varphi^*\mathcal{O}(1) \simeq \mathcal{L}$

The unicity of φ is a consequence of the relations $\varphi^*(T_i) = s_i$ for all $i \in [\![0 \; ; \; n]\!]$. This completes the proof. □

We would like to know when the morphism defined by the above theorem is in fact an embedding i.e. a closed immersion. We first need to make the link with divisors using the correspondence we have seen in 1.3.3. For that purpose, we need to introduce the notion of linear system. From now on and until the end of the paragraph, X will be a complete and regular k-variety.

Definition 1.52. A *complete linear system* on X is an equivalence class of positive divisors of X. In other words, a complete linear system $\mathfrak{d}$ is a subset of $\mathrm{Div}(X)$ of the form:

$$\mathfrak{d} = \{\mathrm{div}(f) + D_0 \mid f \in L(D_0) \setminus \{0\}\}$$

with $D_0 \in \mathrm{Div}(X)$ and $L(D_0) = \{f \in k(X)^* \mid \mathrm{div}(f) + D_0 \geq 0\} \cup \{0\}$. A *linear system* on X is of the form:

$$\mathfrak{d} = \{\mathrm{div}(f) + D_0 \mid f \in W \setminus \{0\}\}$$

where $W \subseteq L(D_0)$ is a k-vector subspace.

Definition 1.53. Let $\mathfrak{d}$ be a linear system on X. One says that $x \in X$ is a *base point* of $\mathfrak{d}$ if for all $D \in \mathfrak{d}$, $x \in \mathrm{Supp}(D)$.

Lemma 1.54. *Let $\mathfrak{d}$ be a linear system defined by $D_0 \in Div(X)$ and $V \subseteq L(D_0)$. We set $\mathcal{L} := \mathcal{L}(D_0)$. Then:*

(i) $x \in X$ is a base point of $\mathfrak{d}$ if and only if $s_x \in \mathfrak{m}_{X,x}\mathcal{L}_x$ for all $s \in V$.

(ii) $\mathfrak{d}$ is base point free if and only if $\mathcal{L}$ is generated by the global sections of V.

Proof. (ii) is an immediate consequence of (i). Indeed, if $\mathcal{L}$ is generated by the global sections of V, then for every $x \in X$, $\mathcal{L}_x$ is generated by the s_x for $s \in V$ and $\mathcal{L}_x \neq \mathfrak{m}_{X,x}\mathcal{L}_x$ (by Nakayama's lemma) so there exists $s \in V$ such that $s_x \notin \mathfrak{m}_{X,x}\mathcal{L}_x$. Conversely, if the global sections of V do not generate $\mathcal{L}$, then there exists $x \in X$ such that $V_x \neq \mathcal{L}_x$ but $\mathcal{L}_x \simeq \mathcal{O}_{X,x}$ so V_x corresponds to a proper ideal in $\mathcal{O}_{X,x}$ which is necessarily included in $\mathfrak{m}_{X,x}$, so that $V_x \subseteq \mathfrak{m}_{X,x}\mathcal{L}_x$.

Now we prove (i). It suffices to prove that for $x \in X$, $s \in V \setminus \{0\}$ and $D := \mathrm{div}(s) + D_0 \in \mathfrak{d}$, we have $x \in \mathrm{Supp}(D)$ if and only if $s_x \in \mathfrak{m}_{X,x}\mathcal{L}_x$.

$\Longleftarrow$ Suppose that $s_x \in \mathfrak{m}_{X,x}\mathcal{L}_x$. Then there exist an open affine neighborhood $U := \mathrm{Spec}(R)$ of x, $f \in \Gamma(U, \mathcal{O}_X) = R$ and $g \in \Gamma(U, \mathcal{L})$ such that $s_{|U} = fg$ and $f_x \in \mathfrak{m}_{X,x}$. Let $\mathfrak{p}$ be the prime ideal corresponding to x. Then $f \in \mathfrak{p}R_\mathfrak{p} = \mathfrak{m}_{X,x}$ so that $f = \frac{a}{b}$, with $a \in \mathfrak{p}$ and $b \in R \setminus \mathfrak{p}$. Let $\mathfrak{q} \subseteq \mathfrak{p}$ be the prime ideal minimal among the prime ideals containing a. Then, $\mathrm{ht}(\mathfrak{q}) = 1$ by the Hauptidealsatz [9, corollary 11.7] so that $V(\mathfrak{q}) = Z \cap U$ for a given prime divisor $Z \in P(X)$ and $x = \mathfrak{p} \in V(\mathfrak{q}) \subseteq Z$. And $f \in \mathfrak{q}R_\mathfrak{q}$ so that $\mathrm{ord}_Z(f) > 0$ and :

$$\mathrm{ord}_Z(D) = \mathrm{ord}_Z(s) + \mathrm{ord}_Z(D_0) = \mathrm{ord}_Z(f) + \mathrm{ord}_Z(g) + \mathrm{ord}_Z(D_0) > 0$$

Since $\mathrm{ord}_Z(g) + \mathrm{ord}_Z(D_0) \geq 0$ because $g \in \Gamma(U, \mathcal{L})$. Then, $x \in Z \subseteq \mathrm{Supp}(D)$.

$\Longrightarrow$ Suppose that $x \in \mathrm{Supp}(D)$. Then there exists a prime divisor Z of X such that $x \in Z$ and $\mathrm{ord}_Z(D) > 0$. Let $U := \mathrm{Spec}(R)$ be an open affine neighborhood of X on which D_0 is principal. We may write $D_{0|U} = \mathrm{div}(g)_{|U}$ for a certain $g \in k(X)^*$. Then, $\mathrm{ord}_Z(D) = \mathrm{ord}_Z(s_{|U}g) > 0$ so that $s_{|U}g \in \mathfrak{q}R_\mathfrak{q}$, where $\mathfrak{q} \in \mathrm{Spec}(R)$ is the generic point of $Z \cap U$ ($Z \cap U = V(\mathfrak{q})$). But $D_{|U} = \mathrm{div}(s_{|U}g) \geq 0$ so $\mathrm{ord}_{Z'}(s_{|U}g) \geq 0$ for all prime divisor $Z' \in P(X)$ intersecting U and $s_{|U}g \in R_\mathfrak{r}$ for all prime ideal $\mathfrak{r}$ of height 1. But X is regular so it is normal (by lemma 1.19), then R is normal by [6, lemma 6.38.(1)] and R is a finite type k-algebra so it is Noetherian and we have :

$$R = \bigcap_{\substack{\mathfrak{r} \in \mathrm{Spec}(R) \\ \mathrm{ht}(\mathfrak{r})=1}} R_\mathfrak{r}$$

by [8, theorem 12.3]. We conclude that $s_{|U}g \in \mathfrak{q}R_\mathfrak{q} \cap R = \mathfrak{q} \subseteq \mathfrak{p}$. But $1/g \in \Gamma(U, \mathcal{L})$ because $\mathrm{div}(1/g) + \mathrm{div}(g) = 0$, so that $s_x \in \mathfrak{m}_{X,x}\mathcal{L}_x$. This completes the proof. □

Let $D \in \mathrm{Div}(X)$ be a positive divisor. Since X is regular, D is locally principal by proposition 1.44. Thus, there exists an open covering $(U_i)_{i \in I}$ of X and sections $g_i \in K(U_i)^* = K(X)^*$ such that $D_{|U_i} = \mathrm{div}(g_i)$ for all $i \in I$. Since $D \geq 0$, the g_i are sections of $\Gamma(U_i, \mathcal{O}_X)$ (as we saw in the proof of lemma 1.45). For all $i, j \in I$, $\mathrm{div}(g_i g_j^{-1})_{|U_i \cap U_j} = \mathrm{div}(g_j g_i^{-1})_{|U_i \cap U_j} = 0$ so $g_i g_j^{-1}, g_j g_i^{-1} \in \Gamma(U_i \cap U_j, \mathcal{O}_X)$ and $g_i g_j^{-1} \in \Gamma(U_i \cap U_j, \mathcal{O}_X)^\times$, so g_i and g_j generate the same ideal in $\Gamma(U_i \cap U_j, \mathcal{O}_X)$. Then, the g_i define a sheaf of ideals on U_i for all $i \in I$ an we can glue these sheaves to define a sheaf of ideals $\mathcal{I}_D$ on X. $\mathcal{I}_D$ is coherent so it defines a closed subscheme $X_D := (S_D, (\mathcal{O}_X/\mathcal{I}_D)_{|S_D})$ of X, where $S_D := \mathrm{Supp}(\mathcal{O}_X/\mathcal{I}_D)$ (by [6, proposition 7.32]).

Then, for all $x \in S_D$, the *tangent space* of D at x: $T_x(D) := T_x(X_D)$ is naturally a subspace of the tangent space $T_x(X)$. Indeed, the maximal ideal of X_D at $x \in S_D$ is $\mathfrak{m}_{D,x} := \mathfrak{m}_{X,x}/(\mathcal{I}_D)_x$ so a any tangent vector $t : \mathfrak{m}_{D,x}/\mathfrak{m}_{D,x}^2 \longrightarrow k$ can be seen as a tangent vector $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2 \longrightarrow k$ vanishing on $\mathcal{I}_x$.

Definition 1.55. **(i)** A linear system $\mathfrak{d}$ is said to *separate points* when for all distinct closed points $x, y \in X$, there exists $D \in \mathfrak{d}$ such that $x \in \mathrm{Supp}(D)$ and $y \notin \mathrm{Supp}(D)$.

(ii) A linear system $\mathfrak{d}$ is said to *separate tangent directions* when for all closed point $x \in X$ and for all tangent vector $t \in T_x(X) \setminus \{0\}$, there exists $D \in \mathfrak{d}$ such that $t \notin T_x(D)$.

Given a divisor $D_0 \in \mathrm{Div}(X)$, we consider the invertible sheaf $\mathcal{L} := \mathcal{L}(D_0)$. $\mathcal{L}$ remains unchanged (up to isomorphism) when D_0 is translated by a principal divisor (by proposition 1.48). Then, $\mathcal{L}$ only depends on the complete linear system $\mathfrak{d}$ defined by D_0.

Assume that $\mathfrak{d}$ is base point free. Then, by lemma 1.54, $\mathcal{L}$ is generated by the global sections $\Gamma(X, \mathcal{L})$. Since X is complete, $\Gamma(\mathcal{O}_X, \mathcal{L})$ is a finite k-vector space by [6, proposition 12.65]. Then, by theorem 1.51, a basis $s_0, \cdots, s_n$ of $\Gamma(X, \mathcal{L})$ defines a morphism $\varphi : X \longrightarrow \mathbb{P}_k^n$.

Theorem 1.56. *Assume that k is algebraically closed. Let X be a complete regular k-variety. Let $\mathfrak{d}$ be a base point free complete linear system on X, $\mathcal{L}$ an invertible sheaf on X and $\varphi : X \longrightarrow \mathbb{P}_k^n$ the morphism determined by $s_0, \cdots, s_n$ generating $\Gamma(X, \mathcal{L})$, as above. Then φ is a closed immersion if and only if $\mathfrak{d}$ separates points and tangent directions.*

Proof. See [7, proposition II.7.3 and remark II.7.87.2]. Hartshorne assumes that X is projective (what we actually want to prove for abelian varieties) but the hypothesis made here (X complete and regular) are in fact sufficient. □

Definition 1.57. An invertible sheaf $\mathcal{L}$ on X is *very ample* if there exists a closed immersion $\varphi : X \hookrightarrow \mathbb{P}_k^n$ such that $\mathcal{L} \simeq \varphi^*\mathcal{O}(1)$ (as defined in theorem 1.51). $\mathcal{L}$ is *ample* if there exists $n \in \mathbb{N}^*$ such that $\mathcal{L}^{\otimes n}$ is very ample.

Similarly, a divisor $D \in \operatorname{Div}(X)$ is *very ample* (respectively ample) if $\mathcal{L}(D)$ is very ample (respectively ample). In other words, D is ample when there exists $n \in \mathbb{N}^*$ such that nD is very ample.

Theorem 1.58. *Let $\mathcal{L}$ be an invertible sheaf on X. Then $\mathcal{L}$ is ample if and only if for all coherent $\mathcal{O}_X$-module $\mathcal{M}$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $\mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{L}^{\otimes n}$ is generated by global sections.*

Proof. This theorem is actually quite difficult. See [7, theorem II.7.6]. □

The theorem 1.56 gives conditions of ampleness for divisors (or invertible sheaves) when k is algebraically closed. Now we explain why this hypothesis is unnecessary. Let K/k be a field extension and $X_K := X \times_k K$ the K/k-extension of scalars. We assume that X_K remains regular. Then, we can still consider divisors on X_K and get the usual results of paragraphs 2.8 and 1.3.3.

Furthermore, we have a natural embedding $k(X) \hookrightarrow K(X_K) = K \otimes_k k(X)$ so every function $f \in k(X)$ may be seen as an element of $K(X_K)$. Then, we can associate to a divisor D on X a divisor D_K on X_K by embedding its local equations in $K(X_K)$. Conversely, if k'/k is a subextension of K/k ($k \subseteq k' \subseteq K$), and if $D \in \operatorname{Div}(X_K)$, we say that D is *defined over* k' if its local equations are elements of $k'(X_{k'}) = k' \otimes k(X) \subseteq K(X_K)$. In that case, D can indeed be seen as an element of $\operatorname{Div}(X_{k'})$.

Since the group $G_{K/k} := \operatorname{Aut}(K/k)$ acts naturally on any K-algebra, it acts on the local equations on any divisor and respects the compatibility of these local equations so $G_{K/k}$ acts on $\operatorname{Div}(X_K)$.

Proposition 1.59. **(i)** *If D and D' are ample divisors on X, then $D + D'$ is ample.*

(ii) *If Y is a subscheme of X, and D is an ample divisor, then $D_{|Y}$ is ample.*

(iii) *If D is a divisor on X such that D_K is ample on X_K, then D is ample on X.*

(iv) *Suppose that K/k is algebraic and that there exists an ample divisor on X_K. Then, there exists an ample divisor on X.*

Proof. (*i*) and (*ii*) are immediate consequence of theorem 1.58.

(*iii*) Suppose that D_K is ample and let $n \in \mathbb{N}^*$ such that nD_K is very ample. By the construction of theorem 1.51 if $\varphi : X \longrightarrow \mathbb{P}^n_k$ is defined by nD, then the base change $\varphi_K : X_K \longrightarrow \mathbb{P}^n_K$ is defined by nD_K. So φ_K is a closed immersion and φ is a closed immersion as well by [10, Exercise 1.7.10], so that nD is very ample and D is ample.

(*iv*) Let D be an ample divisor over K. Since K/k is an algebraic extension and X_K is quasi-compact, D admits local equations on a finite open covering of X and they are all defined over a finite normal extension k'/k, so D is defined over k'. Let $G := \operatorname{Aut}(k'/k) \subseteq G_{K/k}$ and:

$$D' := \sum_{\sigma \in G} \sigma \cdot D$$

where for all $\sigma \in G$, $\sigma \cdot D$ is given by the group action described above. D' is invariant under the action of G, and consequently, D' admits G-invariant local equations, so D' is defined over k'^G. Assume that k is perfect, then $k'^G = k$ and D' is defined over k.

Moreover, if $\phi : X_K \longrightarrow \mathbb{P}^n_K$ is defined by D, then for all $\sigma \in G$, the morphism defined by $\sigma \cdot D$ is still a closed immersion, as the composite of ϕ with the isomorphism $\operatorname{id}_X \times \operatorname{Spec}(\sigma) : X \times_k K \longrightarrow X \times_k K$, where $\operatorname{Spec}(\sigma) : \operatorname{Spec}(K) \longrightarrow \operatorname{Spec}(K)$ is induced by $\sigma : K \longrightarrow K$. It follows that D' is ample by (*i*). We conclude by (*ii*) that D' is in fact an ample divisor on X.

If k is not perfect, then k'^G/k is radical by [11, proposition 5.6.11], so there exists $m \in \mathbb{N}^*$ such that $k'^{p^m} = k$ (where p is the characteristic of k), and we conclude that $p^m D'$ is defined over k. But $p^m D'$ is still ample (by (*i*)) so we conclude as previously. □

1.4 Intersection theory

In this section, we present useful and advanced tools of intersection theory which are crucial to study the multiplication by n map of abelian varieties. Since some invoked results may be long and difficult to prove and intersection theory is not at the center of this seminar, the following results are presented without proofs. The reader may refer to [3, chapters I.12, I.13, II.33.43 and II.33.44] and [7, III.1 and III.2] for further details.

1.4.1 Cohomology of sheaves

Let $\mathcal{A}$ be an abelian category (for instance the category of abelian groups, R-modules over a given ring R or sheaves of R-modules). One says that an object I of $\mathcal{A}$ is *injective* if $\mathrm{Hom}(\cdot, I)$ is an exact functor. One says that $\mathcal{A}$ has *enough injectives* if every object of $\mathcal{A}$ is isomorphic to a subobject of an injective object. An *injective resolution* of an object $A \in \mathrm{Obj}(\mathcal{A})$ is a complex of injectives $I^\bullet$ defined in nonnegative degrees only together with a map $A \longrightarrow I^0$ such that the following sequence is exact:

$$0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots$$

If $\mathcal{A}$ has enough injectives, it is easy to prove by induction that every object of $\mathcal{A}$ admits an injective resolution [3, lemma 13.18.3]. Two injective resolutions of the same object are homotopic [3, lemma 13.18.4].

Let $F : \mathcal{A} \longrightarrow \mathcal{B}$ be a covariant left exact functor. Let $\mathcal{B}^\bullet$ denote the category of complex of $\mathcal{B}$. Then, we define the *right derived functor* of F, $RF : \mathcal{A} \longrightarrow \mathcal{B}^\bullet$ as follows: given $A \in \mathrm{Obj}(\mathcal{A})$ and $I^\bullet$ an injective resolution of A, $R^iF(A) := H^i(F(I^\bullet))$ (cohomology group of the complex $F(I^\bullet)$). This is well defined because $I^\bullet$ is defined up to homotopy. Defining the derived functor on morphisms is much more complex (see [3, lemma 13.14.3]). We get easily that R^0F is naturally isomorphic to F, that R^iF is additive for all $i \in \mathbb{N}$ and that $R^iF(I) = 0$ for all $i \in \mathbb{N}^*$ if I is injective [7, theorem 1.1A].

Let $(X, \mathcal{O}_X)$ be a ringed space. Then, the category $\mathrm{Mod}(\mathcal{O}_X)$ of $\mathcal{O}_X$-modules has enough injectives [7, proposition III.2.2] and the functor $\Gamma(X, \cdot)$ is left exact so we can define its right derived functor $H^\bullet(X, \cdot)$. If $\mathcal{M}$ is an $\mathcal{O}_X$-module, for all $i \in \mathbb{N}$, we call $H^i(X, \mathcal{M})$ the i-th *cohomology group* of $\mathcal{M}$.

If X is Noetherian of dimension n, then a theorem due to Grothendieck ensures that $H^i(X, \mathcal{M}) = 0$ for all $i > n$ and all $\mathcal{O}_X$-module $\mathcal{M}$ [7, theorem III.2.7]. Now, if X is a complete k-variety and $\mathcal{M}$ is a coherent $\mathcal{O}_X$-module, then the homology groups of $\mathcal{M}$ are finite dimensional k-vector spaces [3, lemma 30.19.3] (in the case $i = 0$, we have $H^0(X, \mathcal{M}) = \Gamma(X, \mathcal{M})$ and we already have seen this result [6, proposition 12.65]). In that case, we can define the Euler characteristic of $\mathcal{M}$ as follows:

$$\chi(X, \mathcal{M}) := \sum_{i \in \mathbb{N}} (-1)^i \mathrm{dim}_k H^i(X, \mathcal{M})$$

1.4.2 Intersection numbers

Throughout this paragraph, we fix X a complete k-variety.

Lemma 1.60. *Let $\mathcal{M}$ be a coherent $\mathcal{O}_X$-module and $\mathcal{L}_1, \cdots, \mathcal{L}_r$ be invertible sheaves on X. Then, the function:*

$$(n_1, \cdots, n_r) \in \mathbb{Z}^r \longmapsto \chi(X, \mathcal{M} \otimes \mathcal{L}_1^{\otimes n_1} \otimes \cdots \otimes \mathcal{L}_r^{\otimes n_r}) \in \mathbb{Z}$$

is a numerical polynomial function (polynomial function with rational coefficients mapping $\mathbb{Z}$ to $\mathbb{Z}$) of total degree $\leq$ dim(Supp($\mathcal{M}$)).

Proof. See [3, lemma 33.44.1]. □

Definition 1.61. Let $i : Z \hookrightarrow X$ be a closed immersion, $d := \dim(Z)$ and $\mathcal{L}_1, \cdots, \mathcal{L}_d$ be invertible $\mathcal{O}_X$-modules. Then, we define the *intersection number* $(\mathcal{L}_1 \cdots \mathcal{L}_d \cdot Z)$ as the coefficient of $n_1 \cdots n_d$ of the polynomial function:

$$(n_1, \cdots, n_d) \in \mathbb{Z}^d \longmapsto \chi(X, i_*\mathcal{O}_Z \otimes \mathcal{L}_1^{\otimes n_1} \otimes \cdots \otimes \mathcal{L}_d^{\otimes n_d}) = \chi(Z, \mathcal{O}_Z \otimes \mathcal{L}_{1|Z}^{\otimes n_1} \otimes \cdots \otimes \mathcal{L}_{d|Z}^{\otimes n_d}) \in \mathbb{Z}$$

Lemma 1.62. *Let $i : Z \hookrightarrow X$ be a closed immersion, $d :=$ dim(Z) and $\mathcal{L}_1, \cdots, \mathcal{L}_d$ be invertible $\mathcal{O}_X$-modules. Then:*

(i) $(\mathcal{L}_1 \cdots \mathcal{L}_d \cdot Z) \in \mathbb{Z}$.

(ii) *If $\mathcal{L}_1, \cdots, \mathcal{L}_d$ are ample, then $(\mathcal{L}_1 \cdots \mathcal{L}_d \cdot Z) > 0$.*

(iii) *Intersection numbers are additive: for $i \in [\![1 ; d]\!]$, and $\mathcal{L}_i'$ is an invertible sheaf on X, then:*

$$(\mathcal{L}_1 \cdots \mathcal{L}_i \otimes \mathcal{L}_i' \cdots \mathcal{L}_d \cdot Z) = (\mathcal{L}_1 \cdots \mathcal{L}_i \cdots \mathcal{L}_d \cdot Z) + (\mathcal{L}_1 \cdots \mathcal{L}_i' \cdots \mathcal{L}_d \cdot Z)$$

Proof. See [3, lemma 33.44.4] for (i), [3, lemma 33.44.9] for (ii) and [3, lemma 33.44.5] for (iii). □

Lemma 1.63. *Let $f : X \longrightarrow Y$ be a finite dominant morphism of complete and integral k-varieties. Let $d :=$ dim(Y) and $\mathcal{L}_1, \cdots, \mathcal{L}_d$ be invertible sheaves on Y. Then, we have:*

$$(f^*\mathcal{L}_1 \cdots f^*\mathcal{L}_d \cdot X) = deg(f)(\mathcal{L}_1 \cdots \mathcal{L}_d \cdot Y)$$

Proof. Since $k(Y)/k(X)$ is finite $k(X)$ and $k(Y)$ have the same transcendence degree so $\dim(X) = \dim(Y)$ by [7, Exercise II.3.20.b] so the formula makes sense. For the proof see [3, lemma 33.44.7]. □

Chapter 2

Abelian varieties

2.1 Group schemes and abelian varieties

Definition 2.1. Let S be a scheme. A *group scheme G over S* is a quadruple (G, m, i, e) where G is a S-scheme, $m : G \times_S G \longrightarrow G$, $i : G \longrightarrow G$ two morphisms of S-schemes and $e \in G(S)$ a S-valued point such that for all S-scheme T, $G(T)$ has a group structure given by m as the multiplication map, i as the inversion map and e as the neutral element. Namely, for all $g_1, g_2, g_3 \in G(T)$:

(i) $m \circ (g_1 \times_S e \circ \pi_{T/S}) = m \circ (e \circ \pi_{T/S} \times_S g_1) = g_1$ (neutral element).

(ii) $m \circ (g_1 \times_S m \circ (g_2 \times_S g_3)) = m(m \circ (g_1 \times_S g_2) \times_S g_3)$ (associativity).

(iii) $m \circ (g_1 \times_S i \circ g_1) = m \circ (i \circ g_1 \times_S g_1) = e \circ \pi_{T/S}$ (inversion).

Where $\pi_{T/S} : T \longrightarrow S$ is the structural morphism of T.

To simplify the notations, we will often denote (G, m) or even G instead of (G, m, i, e) for a group scheme and $m(g, h)$ or simply gh instead of $m \circ (g \times_S h)$ for the multiplication of two elements.

Definition 2.2. A morphism of group shemes over S, $\varphi : (G, m) \longrightarrow (G', m')$ is a morphism of S-schemes which induces a group homomorphism $G(T) \longrightarrow G'(T)$ for all S-scheme T. Namely, for all $g, h \in G(T)$:

$$\varphi(m(g, h)) = m'(\varphi(g), \varphi(h))$$

Lemma 2.3. *Let (G, m) be a group scheme over S and S' be a S-scheme. Then, the pullback $(G_{S'}, m_{S'})$ is a group scheme over S'.*

Proof. First of all, we remark that:

$$\begin{aligned}(G \times_S G) \times_S S' &\simeq G \times_S (G \times_S S') = G \times_S G_{S'} \simeq G \times_S (S' \times_{S'} G_{S'}) \simeq (G \times_S S') \times_{S'} G_{S'} \\ &= G_{S'} \times_{S'} G_{S'}\end{aligned}$$

And we set $m_{S'} := m \times_S \mathrm{id}_{S'} : (G \times_S G) \times_S S' \simeq G_{S'} \times_{S'} G_{S'} \longrightarrow G_{S'}$, $i_{S'} := i \times_S \mathrm{id}_{S'}$ and $e_{S'} := e \times_S \mathrm{id}_{S'}$. With this definition, we have the following commutative diagrams for m and $m_{S'}$:

$$\begin{tikzcd}
(G \times_S G) \times_S S' \arrow[r, "m_{S'}"'] \arrow[d, "q_1"] & G_{S'} \arrow[d, "p_1"] \\
G \times_S G \arrow[r, "m"] & G
\end{tikzcd} \tag{1}$$

$$\begin{tikzcd}
(G \times_S G) \times_S S' \arrow[rr, "q_2"'] \arrow[drr, dotted, "m_{S'}"'] & & S' \\
 & & G_{S'} = G \times_S S' \arrow[u, "p_2"']
\end{tikzcd} \tag{2}$$

where the maps p_i, q_i of index 1 (resp. 2) are left (resp. right) projections (we will keep using this convention later). We also have similar diagrams for $i_{S'}$ and $e_{S'}$.

Let T be an S'-scheme and $g' \in G_{S'}(T)$. Then, we have:

$$\begin{aligned}
p_1 \circ m_{S'} \circ (g' \times_{S'} e') &= m \circ q_1 \circ (g' \times_{S'} e') \quad \text{(see diagram (1))} \\
&= m \circ q_1 \circ ((p_1 \circ g' \times_S p_1 \circ e') \times_S \mathrm{id}_{S'}) \\
&\text{(with the identification } (G \times_S G) \times_S S' \simeq G_{S'} \times_{S'} G_{S'} \\
&\ \text{and the unicity in the universal property of the fiber product)} \\
&= m \circ (p_1 \circ g' \times_S p_1 \circ e') \\
&= p_1 \circ g' \quad \text{(by the axiom (i) of group schemes)}
\end{aligned}$$

One proves as well that $p_2 \circ m_{S'} \circ (g' \times_{S'} e') = p_2 \circ g$ using (2), so we get that $m_{S'} \circ (g' \times_{S'} e') = g'$ and we can obtain that $m_{S'} \circ (e' \times_{S'} g') = g'$ with the same arguments. Axioms *(ii)* and *(iii)* can be proved with similar techniques so we will omit them. □

Definition 2.4. An *abelian variety* A over k is a group scheme over $\mathrm{Spec}(k)$ which is proper (i.e. complete, separated, of finite type) and geometrically integral. In particular, an abelian variety over k is a k-variety.

A morphism of abelian varieties is a morphism of group schemes between abelian varieties.

Proposition 2.5. *Let A be an abelian variety over k. For every field extension K/k, A_K is an abelian variety.*

Proof. A_K is still a group variety by lemma 2.3 and is still geometrically integral by proposition 1.7. Moreover, A is proper so its structural morphism $\pi_{A/k} : A \longrightarrow \mathrm{Spec}(k)$ is proper and $\pi_{A_K/K} : A_K \longrightarrow \mathrm{Spec}(K)$ is only the base change of $\pi_{A/k}$ with $\mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(k)$ so it is proper by lemma 1.10.(ii) and A_K is proper.

□

Lemma 2.6. *Le $\varphi : A \longrightarrow B$ be a morphism of abelian varieties. Then, $\varphi(A)$ is an abelian subvariety of B.*

Proof. A is proper and B is seperated so φ is proper (hence closed) by lemma 1.11 so $\varphi(A)$ is closed and may be seen as a closed subscheme of B with the reduced induced structure. $\varphi(A)$ is clearly a subgroup scheme of B (because the restricted multiplication map $m_{B|\varphi(A)\times\varphi(A)}$ factors through $\varphi(A)$). By [3, lemma 30.26.3], we get that $\varphi(A)$ is proper (as a closed subscheme of a proper scheme). It remains to prove that $\varphi(A)$ is geometrically integral. First, we notice that $\varphi(A)_{\overline{k}} = \varphi_{\overline{k}}(A_{\overline{k}})$ and that φ remains a morphism after extension of sclars (it would require a justification) so we may assume $k = \overline{k}$ and we simply have to prove that $\varphi(A)$ is integral, which is obviously true because A is integral (so $\varphi(A)$ is irreducible) and $\varphi(A)$ has reduced induced structure. □

Let A be an abelian variety over k. Any k-valued point $x \in A(k)$, is by definition a morphism of schemes $x : \mathrm{Spec}(k) \longrightarrow A$ so we can define the right translation by x on A as the composition:

$$t_x : A \overset{\Delta_{A/k}}{\longrightarrow} A \times_k A \overset{\mathrm{id}_A \times x \circ \pi_{A/k}}{\longrightarrow} A \times_k A \overset{m}{\longrightarrow} A$$

where $\pi_{A/k}$ is the structural morphism $A \longrightarrow \mathrm{Spec}(k)$. t_x defines an automorphism and its inverse is $t_{\iota(x)}$.

Proposition 2.7. *Let A be an abelian variety. Then A is smooth.*

Proof. It suffices to prove that $A_{\overline{k}}$ is smooth (by [6, remark 6.30]). By proposition 2.5 we may assume that k is algebraically closed.

The smooth locus A_{sm} of A is open and dense in A (by [6, theorem 6.19]). Moreover, A_{sm} is stable by translation. Indeed, if $x \in A_{sm}$, then there exists an open affine neighborhood U of x and an immersion $j : U \hookrightarrow \mathrm{Spec}(R)$ where R is a finite-type k-algebra $R = k[X_1, \cdots, X_n]/(f_1, \cdots, f_{n-d})$ such that rank $\mathrm{Jac}(f_1, \cdots, f_{n-d})(x) = n - d$. And for any k-valued point, $y \in A(k)$:

$$j \circ t_{\iota(y)} : t_{\iota(y)}^{-1}(U) = t_y(U) \longrightarrow \mathrm{Spec}(R)$$

is still an open immersion and $t_y(U)$ is an open neighborhood of $t_y(x)$ so $t_y(x)$ is smooth.

Besides, the set of k-valued points $A(k)$ can be identified to the set of closed points of A and is very dense (by [6, corollary 3.36]). Then, $A(k) \cap A_{sm} \neq \emptyset$ so there exists $x_0 \in A(k) \cap A_{sm}$ and for all $y \in A(k)$, $t_{\iota(x_0)y}(x_0) = y \in A_{sm}$ by the stability property of A_{sm}. Then, A_{sm} is as very dense as well.

Suppose by contradiction that there exists $x \in A \setminus A_{sm}$. Then, $\overline{\{x\}} \subseteq A \setminus A_{sm}$, as $A \setminus A_{sm}$ is closed. Then, $\overline{\{x\}} = \overline{A_{sm} \cap \overline{\{x\}}} = \overline{\emptyset} = \emptyset$ because A_{sm} is very dense. Contradiction. Then, A is smooth. □

Proposition 2.8. *Let A and B be two abelian varieties over k. Then every morphism of k-schemes $\varphi : A \longrightarrow B$ is the composition of a translation and a morphism of abelian varieties.*

Proof. Let e and e', m and m', i and i' be the respective neutral elements, multiplication maps and inversion maps of A and B. We have $t_{i(e)} \circ \varphi(e) = e'$, so after translating, we may assume that $\varphi(e) = e'$. We now consider the morphism of k-schemes:

$$\psi := m' \circ ([\varphi \circ m] \times_k [i \circ m' \circ (\varphi \times_k \varphi)]) : A \times_k A \longrightarrow B$$

which corresponds to $(x, y) \in A(T) \times A(T) \longmapsto \varphi(xy)\varphi(y)^{-1}\varphi(x)^{-1} \in B(T)$ on T-valued points for all k-scheme T. Since $\varphi(e) = e'$, we have $\psi(A \times \{e\}) = \{e'\} = \psi(\{e\} \times A)$. By the rigidity lemma (theorem 1.13), we have $\psi(A \times A) = \{e'\}$, which completes the proof. □

Corollary 2.9. *Let A be an abelian variety. Then $A(T)$ is an abelian group for all k-scheme T.*

Proof. We apply proposition 2.8 on the inversion morphism $i : A \longrightarrow A$. Since $i(e) = e$, we get that i is a morphism of abelian variety. Then, it induces a group endomorphism on $A(T)$, so $A(T)$ is abelian. □

As a consequence of this corollary, we may denote the the group law additively and denote 0 instead of e the neutral element of an abelian variety.

2.2 Morphisms and isogenies

Let $\phi : A \longrightarrow B$ be a morphism of abelian varieties over k. The *kernel* of ϕ, is the scheme theoretic fiber of 0_B :

$$\ker(\phi) := A_{0_B} = A \times_B \mathrm{Spec}(k)$$

Where the fiber product is given by ϕ and the map $0_B : \mathrm{Spec}(k) \longrightarrow B$. This is a closed subscheme of A and a group scheme (because of the group homomorphism structure of ϕ).

Definition 2.10. A morphism of abelian varieties is an *isogeny* if it is surjective of finite kernel.

Proposition 2.11. *Let $\phi : A \longrightarrow B$ be a morphism of abelian varieties. Then, ϕ is an isogeny if and only if one of the following conditions stands:*

(i) *$dim(A) = dim(B)$ and $ker(\phi)$ is finite.*

(ii) *$dim(A) = dim(B)$ and ϕ is surjective.*

(iii) *ϕ is finte locally free.*

Proof. A and B are both complete k-varieties so lemma 1.11 ensures that ϕ is proper. It follows that ϕ is closed and that $\phi(A)$ is an integral subscheme of A (with the reduced induced structure). Then, ϕ factors through the closed immersion $\phi(A) \hookrightarrow B$ and we may see ϕ as a surjective (hence dominant) morphism of integral schemes of finite type $A \longrightarrow \phi(A)$. By [7, Exercise II.3.22], there exists a non-empty open subset $U \subseteq A$ such that for all $b \in \phi(U)$:

$$\dim(A_b) = \dim(A) - \dim(\phi(A)) \quad (\star)$$

Besides, for all $b \in B$ (viewed as a $k(b)$-valued point), the translation $t_b : B \times_k k(b) \longrightarrow B \times_k k(b)$ induces an isomorphism between the fibers $\ker(\phi) \times_k k(b) = A_0 \times k(b) \longrightarrow A_b$ up to extension of scalars, and under the hypothesis we have made (integrality and finite-typeness), the dimension is unchanged after extension of scalars (by [7, Exercise II.3.20.f]) so all fibers have the same dimension and $(\star)$ holds for every $b \in B$. In particular:

$$\dim(\ker(\phi)) = \dim(A) - \dim(\phi(A)) \quad (\star\star)$$

If (i) holds, then $\ker(\phi)$ is finite so its dimension is zero and $\dim(\phi(A)) = \dim(A) = \dim(B)$ so that $B = \phi(A)$ because B is irreducible and $\phi(A)$ is closed so ϕ is an isogeny. If (ii) holds, then $\dim(\ker(\phi)) = 0$ and we conclude by the following lemma. Conversely, if ϕ is an isogeny, then $\dim(B) = \dim(\phi(A)) = \dim(A)$ by $(\star\star)$ so (i) and (ii) hold.

Lemma 2.12. *Let X be a finite type k-scheme. If Y is a closed subscheme of dimension zero, then Y is finite.*

Proof. Let $U := \operatorname{Spec}(R)$ be an open affine subset of X intersecting Y, and let $I \subseteq R$ a reduced ideal such that $Y \cap U = V(I)$. Then every prime ideal $\mathfrak{p} \in V(I)$ is maximal so $V(I)$ is finite because R is Noetherian. Since X is quasi-compact, it can be covered by finitely many open affines so Y is finite. □

Now we prove that ϕ is an isogeny if and only if it is finite locally free. If ϕ is finite locally free then its fibers are finte by lemma 1.21 so $ker(\phi)$ is finite and $\phi_*\mathcal{O}_A$ is a locally free of finite type $\mathcal{O}_B$-module. It follows that for a given non-empty open affine $V \subseteq B$, $\mathcal{O}_A(\phi^{-1}(V))$ is a finitely generated $\mathcal{O}_B(V)$-module so that both rings have the same dimension and $\dim(A) = \dim(\mathcal{O}_A(\phi^{-1}(V))) = \dim(\mathcal{O}_B(V)) = \dim(B)$ by [7, Exercise II.3.20.e]. So (ii) holds and ϕ is an isogeny.

Conversely, if ϕ is an isogeny then $\ker(\phi)$ is finite so all the fibers are finite (as we have seen with the isomorphism induced by the translations) and ϕ is proper by lemma 1.11 so ϕ is finite by lemma 1.21. Then, $\phi_*\mathcal{O}_A$ is a coherent $\mathcal{O}_B$-module as the direct image of a coherent module by a finite morphism [7, exercise 5.5]. Since $\mathcal{O}_{A,a}$ is a k-vector space for all $a \in A$, it is flat over k so $\mathcal{O}_A$ is flat and $\mathcal{O}_A$ is (quasi)-coherent so $\phi_*\mathcal{O}_A$ is flat by lemma 1.26. Consequently, ϕ is finite locally free. □

2.3 The theorem of the cube and its consequences

Let us recall the:

Theorem 2.13 (theorem of the cube)**.** *Let X, Y, Z be three geometrically irreducible k-varieties. We assume that X and Y are complete. Let $\mathcal{L}$ be an invertible sheaf on $X \times Y \times Z$, $x_0 \in X(k)$, $y_0 \in Y(k)$ and $z_0 \in Z(k)$ such that $\mathcal{L}$ is trivial on $X \times Y \times \{z_0\}$, $X \times \{y_0\} \times Z$ and $\{x_0\} \times Y \times Z$. Then, $\mathcal{L}$ is trivial on $X \times Y \times Z$.*

Proof. See [2, p.55 or p.91]. □

Let A be an abelian variety over k. For $i \in \{1, 2, 3\}$, let $p_i : A^3 \longrightarrow A$ be the projection of the i-th coordinate. For $i, j, k \in \{1, 2, 3\}$, we denote:

$$p_{i,j} := m \circ (p_i \times p_j) : A^3 \longrightarrow A$$

(the sum $p_i + p_j$) and

$$p_{i,j,k} := m \circ (p_{i,j} \times p_k) : A^3 \longrightarrow A$$

(the sum $p_i + p_j + p_k$).

Corollary 2.14. *For any invertible sheaf $\mathcal{L}$ on A, the invertible sheaf:*

$$p_{1,2,3}^*\mathcal{L} \otimes p_{1,2}^*\mathcal{L}^{-1} \otimes p_{1,3}^*\mathcal{L}^{-1} \otimes p_{2,3}^*\mathcal{L}^{-1} \otimes p_1^*\mathcal{L} \otimes p_2^*\mathcal{L} \otimes p_3^*\mathcal{L}$$

on A^3 is trivial.

Proof. Let $\mathcal{M}$ be the invertible sheaf of the corollary. Then, the restriction of $p_{1,2,3}, p_{1,2}, p_{1,3}, p_{2,3}, p_1, p_2, p_3$ on $A \times A \times \{0\} \simeq A \times A$ are respectively $m, p, m, q, p, q, 0$ where $p : A \times A \longrightarrow A$ is the left projection, $q : A \times A \longrightarrow A$ is the right projection and 0 is the constant map $0_A \times \pi_{A/k}$. Then:

$$\mathcal{M}_{A\times A\times\{0\}} \simeq m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1} \otimes m^*\mathcal{L}^{-1} \otimes q^*\mathcal{L}^{-1} \otimes p^*\mathcal{L} \otimes q^*\mathcal{L} \otimes \mathcal{O}_{A\times A} \simeq \mathcal{O}_{A\times A}$$

where we used lemma 1.41.(ii) to identify $0^*\mathcal{L}$ with $\mathcal{O}_{A\times A}$. By similar arguments, we obtain that the restriction of $\mathcal{M}$ to $A \times \{0\} \times A$ and $\{0\} \times A \times A$ are trivial. Then, $\mathcal{M}$ is trivial by the theorem of the cube 2.13. □

Corollary 2.15. *Let X be a k-scheme and $f_1, f_2, f_3 : X \longrightarrow A$ be three morphisms of k-schemes. For $i, j, k \in \{1, 2, 3\}$, let us denote by $f_i + f_j$ and $f_i + f_j + f_k$ respectively the composites $p_{i,j} \circ (f_1 \times f_2 \times f_3)$ and $p_{i,j,k} \circ (f_1 \times f_2 \times f_3)$. Then, for all inverible sheaf $\mathcal{L}$ on A, the invertible sheaf:*

$$(f_1 + f_2 + f_3)^*\mathcal{L} \otimes (f_1 + f_2)^*\mathcal{L}^{-1} \otimes (f_1 + f_3)^*\mathcal{L}^{-1} \otimes (f_2 + f_3)^*\mathcal{L}^{-1} \otimes f_1^*\mathcal{L} \otimes f_2^*\mathcal{L} \otimes f_3^*\mathcal{L}$$

is trivial.

Proof. We only have to apply the functor $(f_1 \times f_2 \times f_3)^*$ on the invertible sheaf of the preceding corollary. □

For $n \in \mathbb{Z}$, we define the *multiplication by n* map $[n] : A \longrightarrow A$ as follows: $[0] := 0_A \circ \pi_{A/k}$ is the zero map, for all $n \in \mathbb{N}^*$, $[n + 1] = m \circ ([n] \times \mathrm{id}_A) \circ \Delta_{A/k}$ (by induction) and $[-n] := i \circ [n]$. For all $n \in \mathbb{Z}$, $[n]$ is an endomorphism in the category of abelian varieties as it is a group homomorphism.

Corollary 2.16. *Let $\mathcal{L}$ be an invertible sheaf on A. Then, for all $n \in \mathbb{N}$:*

$$[n]^*\mathcal{L} \simeq \mathcal{L}^{\otimes \frac{n(n+1)}{2}} \otimes [-1]^*\mathcal{L}^{\otimes \frac{n(n-1)}{2}}$$

where the exponents are iterations of the tensor products.

Proof. We proceed by induction on $n \in \mathbb{N}$. For $n = 0$, the equation is $\mathcal{O}_A \simeq \mathcal{O}_A$ so the result is trivial. For $n \in \mathbb{N}$, the preceding corollary with $f_1 := [n]$, $f_2 := [1]$ and $f_3 := [-1]$ ensures that:

$$[n]^*\mathcal{L} \otimes [n + 1]^*\mathcal{L}^{\otimes -1} \otimes [n - 1]^*\mathcal{L}^{\otimes -1} \otimes [0]^*\mathcal{L}^{\otimes -1} \otimes [n]^*\mathcal{L} \otimes [1]^*\mathcal{L} \otimes [-1]^*\mathcal{L} \simeq \mathcal{O}_A$$

$$\text{i.e.} \quad [n + 1]^*\mathcal{L} \simeq [n]^*\mathcal{L}^{\otimes 2} \otimes [n - 1]^*\mathcal{L}^{\otimes -1} \otimes \mathcal{L} \otimes [-1]^*\mathcal{L} \quad (\star)$$

with the use of lemma 1.41.(ii) to simplify the trivial term $[0]^*\mathcal{L}^{\otimes -1}$. Taking $n = 0$ in $(\star)$, we get the desired result for $n = 1$. Now, we assume that the result holds for n and $n - 1$. Then, by $(\star)$ and by the induction hypothesis, we get:

$$\begin{aligned}
[n+1]^*\mathcal{L} &\simeq [n]^*\mathcal{L}^{\otimes 2} \otimes [n-1]^*\mathcal{L}^{\otimes -1} \otimes \mathcal{L} \otimes [-1]^*\mathcal{L} \\
&\simeq \left(\mathcal{L}^{\otimes \frac{n(n+1)}{2}} \otimes [-1]^*\mathcal{L}^{\otimes \frac{n(n-1)}{2}}\right)^2 \otimes \mathcal{L}^{\otimes -\frac{(n-1)n}{2}} \otimes [-1]^*\mathcal{L}^{\otimes -\frac{(n-1)(n-2)}{2}} \otimes \mathcal{L} \otimes [-1]^*\mathcal{L} \\
&\simeq \mathcal{L}^{\otimes n(n+1)-\frac{n(n-1)}{2}+1} \otimes [-1]^*\mathcal{L}^{\otimes n(n-1)-\frac{(n-1)(n-2)}{2}+1} = \mathcal{L}^{\otimes \frac{(n+1)(n+2)}{2}} \otimes [-1]^*\mathcal{L}^{\otimes \frac{n(n+1)}{2}}
\end{aligned}$$

This completes the proof. □

Corollary 2.17 (theorem of the square)**.** *Let $\mathcal{L}$ be an invertible sheaf on A and $a, b \in A(k)$ two k-valued points. Then:*

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \simeq t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}$$

Proof. We only have to apply corollary 2.15 to $f_1 := \mathrm{id}_A$, $f_2 := a \circ \pi_{A/k}$ and $f_3 := b \circ \pi_{B/k}$ and use lemma 1.41.(ii) to simplify trivial terms. □

Let $a \in A(k)$. For all prime Z divisor of A, the translation $t_a(Z)$ is still closed irreducible and of codimension 1 so it is a prime divisor. By linearity, one defines the translation of any divisor on A.

Lemma 2.18. *For all $a \in A(k)$ and $D \in Div(A)$, we have $t_a^*\mathcal{L}(D) \simeq \mathcal{L}(t_{-a}(D))$.*

Proof. The translation $t_a : A \longrightarrow A$ induces a sheaf isomorphism $t_a^\# : t_a^{-1}\mathcal{O}_A \longrightarrow \mathcal{O}_A$, so that:

$$t_a^*\mathcal{L}(D) = \mathcal{O}_A \otimes_{t_a^{-1}\mathcal{O}_A} t_a^{-1}\mathcal{L}(D) \simeq t_a^{-1}\mathcal{L}(D)$$

But for all open subset $U \subseteq A$:

$$\Gamma(U, t_a^{-1}\mathcal{L}(D)) = \Gamma(t_a(U), \mathcal{L}(D)) = \{f \in k(X)^* \mid \mathrm{div}(f)_{|t_a(U)} + D_{|t_a(U)} \geq 0\}$$

and we get easily that $D_{|t_a(U)} = t_{-a}(D)$, so that $\Gamma(U, t_a^{-1}\mathcal{L}(D)) \simeq \Gamma(U, \mathcal{L}(t_{-a}(D)))$ and finally $t_a^*\mathcal{L}(D) \simeq \mathcal{L}(t_{-a}(D))$. □

With the formula above and proposition 1.48, the theorem of the square could be reformulated in terms of divisors as follows:

Corollary 2.19. *For all $a, b \in A(k)$ and divisor $D \in Div(A)$, we have $t_{a+b}(D) + D \sim t_a(D) + t_b(D)$.*

2.3.1 Abelian varieties are projective

Theorem 2.20. *Abelian varieties are projective.*

Proof. Let A be an abelian variety over k. By proposition 1.59.(iv), we may assume that k algebraically closed.

Step 1: We construct a divisor $D := \sum_{i=1}^r [Z_i]$ where the $Z_1, \cdots, Z_r$ are prime divisors on A such that:

(i) $\bigcap_{i=1}^r Z_i = \{0_A\}$, where 0_A is the neutral element of A.

(ii) $\bigcap_{i=1}^r T_{0_A}(Z_i) = \{0\}$, where 0 is the zero vector in the tangent space $T_{0_A}(A)$.

Let $U := \mathrm{Spec}(R)$ be an open neighborhood of 0_A. Then, 0_A corresponds to a maximal ideal $\mathfrak{m}_0 \subseteq R$ because 0_A is a closed point by [6, corollary 3.36] (since $0_A \in A(k)$). As we have seen in chapter 1, the prime divisors Z passing through 0_A are determined by prime ideals $\mathfrak{p}$ of height 1 of R such that $\mathfrak{m}_0 \in V(\mathfrak{p})$ i.e. $\mathfrak{p} \subseteq \mathfrak{m}_0$. Therefore, we may see these ideals as prime ideals of height 1 in $R_{\mathfrak{m}_0}$. But A is smooth so $R_{\mathfrak{m}_0} = \mathcal{O}_{A,0_A}$ is regular by 1.19. By theorem 1.17, we get that $R_{\mathfrak{m}_0}$ is a unique factorization domain. Since the elements of $\mathfrak{m}_0 R_{\mathfrak{m}_0}$ are non-invertible, they all have irreducible factors. Besides, the principal ideals generated by irreducible elements are prime of height 1. It follows that $\mathfrak{m}_0$ is generated by the prime ideals of height 1 contained in $\mathfrak{m}_0$, so that:

$$\bigcap_{\substack{\mathfrak{p}\subseteq\mathfrak{m}_0\\ \mathrm{ht}(\mathfrak{p})=1}} V(\mathfrak{p}) = V\left(\sum_{\substack{\mathfrak{p}\subseteq\mathfrak{m}_0\\ \mathrm{ht}(\mathfrak{p})=1}} \mathfrak{p}\right) = V(\mathfrak{m}_0) = \{\mathfrak{m}_0\}$$

Then, the intersection of U and all the prime divisors of A containing 0_A is reduced to 0_A, and this is true for all open affine neighborhood U of 0_A. Then, to prove that the intersection of all prime divisors containing 0_A is reduced to 0_A, it suffices to prove that open affine neighborhoods of 0_A cover A.

Let $x \in A$ be a closed point (automatically k-valued) and U be an open affine neighborhood of 0_A. Then $t_x(U) \cap U \neq \emptyset$ because A is irreducible and the closed points are very dense so there exists a closed point $y \in t_x(U) \cap U$. Therefore, $0_A \in t_{x-y}(U)$ and $x = y + x - y \in t_{x-y}(U)$. Furthermore, $t_{x-y}(U)$ is still affine because t_{x-y} is an isomorphism. We conclude that the open subset V formed of all open affine neighborhoods of 0_A contains the set of closed points $A(k)$, so it is very dense. Suppose that there exists $x \in A \setminus V$. Then, $\overline{\{x\}} \subseteq A \setminus V$ because $A \setminus V$ is closed and therefore $\overline{\{x\}} = \overline{V \cap \overline{\{x\}}} = \emptyset$ because V is very dense. Then $V = A$ and we conclude that the intersection of all prime divisors containing 0_A is reduced to 0_A, as announced before. Since A is Noetherian, by the descending chain condition, there exists finitely many prime divisors $Z_1, \cdots, Z_s$ such that $\bigcap_{i=1}^{s} Z_i = \{0_A\}$.

Let $U := \mathrm{Spec}(R)$ be an open affine neighborhood of 0_A and $\mathfrak{m}_0$ the maximal ideal corresponding to $0 * A$. Then, as we have seen above, $\mathfrak{m}_{A,0_A} = \mathfrak{m}_0 R_{\mathfrak{m}_0}$ is generated by all the prime ideals of height 1 in $R_{\mathfrak{m}_0} = \mathcal{O}_{A,0_A}$ i.e. by the localized ideals $\mathcal{I}_{Z,0_A}$ for every prime divisor Z containing 0_A ($\mathcal{I}_Z$ being the coherent ideal associated to Z, as we saw in paragraph 1.3.4, on page 17). It follows that every vector t in the intersection of the tangent spaces at 0_A of the prime divisors Z containing 0_A vanishes on the $\mathcal{I}_{Z,0_A}$s, so on the whole of $\mathfrak{m}_{A,0_A}$ so it is zero. But $T_{0_A}(A)$ is finite dimensional so it verifies the descending chain condition and there are finitely many prime divisors containing 0_A : $Z_{s+1}, \cdots, Z_r$ such that $\bigcap_{i=s+1}^{r} T_{0_A}(Z_i) = \{0\}$. Finally, $Z_1, \cdots, Z_r$ verify (i) and (ii) and we set $D := \sum_{i=1}^{r} [Z_i]$.

Step 2: We prove that $3D$ is very ample i.e. that the complete linear system $\mathfrak{d}(3D)$ it defines is base point free, separates points and tangent directions, which is necessary and sufficient by theorem 1.56.

Let $a, b \in A(k)$ be two distinct closed points. We prove that there exists a positive divisor linearly equivalent to $3D$ whose support contains a but not b. By the theorem of the square 2.19, we have for all $c, d \in A(k)$ and all divisor $D' \in \mathrm{Div}(A)$, $t_c(D') + t_d(D') + t_{-c-d}(D') \sim 3D'$, so that :

$$3D = \sum_{i=1}^{r} 3[Z_i] \sim \sum_{i=1}^{r} ([t_{a_i}(Z_i)] + [t_{b_i}(Z_i)] + [t_{-a_i-b_i}(Z_i)])$$

for all $a_1, \cdots, a_r, b_1, \cdots, b_r \in A(k)$. Since $b - a \neq 0_A$, by (i) there exists $i \in [\![1\ ;\ r]\!]$ such that $b - a \notin Z_i$, so that $b \notin t_a(Z_i)$. But $a \in t_a(Z_i)$. Then, we may chose $a_i := b - a$. Now we chose b_i such that $b \notin t_{b_i}(Z_i) \cup t_{-a_i-b_i}(Z_i)$ i.e. $b_i \notin (b - Z_i) \cup t_{-a_i-b}(Z_i)$. But $b - Z_i$ and $t_{-a_i-b}(Z_i)$ are closed and proper subsets and A is irreducible so they do not cover the whole of A. Since $A(k)$ is dense, there exists a convenient $b_i \in A(k)$. For $1 \leq j \neq i \leq r$, we take $a_j \in A(k) \setminus t_{-b}(Z_j)$ so that $b \notin t_{a_j}(Z_j)$ and $b_j \in A(k) \setminus (b - Z_j) \cup t_{-a_j-b}(Z_j)$ so that $b \notin t_{b_j}(Z_j)$ and $b \notin t_{-a_j-b_j}(Z_j)$. We conclude that $a \in \mathrm{Supp}(D')$ but $b \notin \mathrm{Supp}(D')$ for a certain positive divisor $D' \sim 3D$ (given by the a_i and b_i), so that $\mathfrak{d}(3D)$ separates points.

Given $a \in A$, we can use the same ideas to find the a_i and b_i such that a avoids $t_{a_i}(Z_i)$, $t_{b_i}(Z_i)$ and $t_{-a_i-b_i}(Z_i)$ for all $i \in [\![1\ ;\ n]\!]$, so that $a \notin \mathrm{Supp}(D')$ for a certain $D' \in \mathfrak{d}(3D)$ and $\mathfrak{d}(3D)$ has no base point.

Let $a \in A(k)$ and $t \in T_a(A) \setminus \{0\}$. Since t_a is an isomorphism its differential at 0_A is an isomorphism between $T_{0_A}(A)$ and $T_a(A)$ and we have $\bigcap_{i=1}^{r} T_a(t_a(Z_i)) = \{0_A\}$ by (ii). Then, there exists $i \in [\![1\ ;\ r]\!]$ such that $t \notin T_a(t_a(Z_i))$ and we may chose $a_i := a$. As previously, we may chose b_i such that $a \notin$

$t_{b_i}(Z_i) \cup t_{-a_i-b_i}(Z_i)$ and a_j, b_j for $1 \leq j \neq i \leq r$ such that $b \notin t_{a_j}(Z_j) \cup t_{b_j}(Z_i) \cup t_{-a_j-b_j}(Z_j)$. Let:

$$D' := \sum_{i=1}^{r} ([t_{a_i}(Z_i)] + [t_{b_i}(Z_i)] + [t_{-a_i-b_i}(Z_i)])$$

Then, the stalk at b of the sheaf of ideals associated to D' (see the definition on page 17) is:

$$\mathcal{I}_{D',b} = \prod_{j=1}^{r} \mathcal{I}_{t_{a_j}(Z_j),b} \cdot \mathcal{I}_{t_{b_j}(Z_j),b} \cdot \mathcal{I}_{t_{-a_j-b_j}(Z_j),b}$$

And $a \in t_{a_i}(Z_i)$ only so these ideals are locally trivial (i.e. contain 1) on an open neighborhood of a, $\mathcal{I}_{t_{a_i}(Z_i)}$ excepted, so that $\mathcal{I}_{D',b} = \mathcal{I}_{t_{a_i}(Z_i),b} = \mathcal{I}_{t_a(Z_i),b}$ and $T_a(D') = T_a(t_a(Z_i))$. Finally, $t \notin T_a(D')$ and $b \in \text{Supp}(D')$ so $\mathfrak{d}(3D)$ separates tangent directions. This completes the proof. □

2.3.2 Study of the multiplication by n map and torsions subgroups

Proposition 2.21. *Let $g := dim(A)$. The multiplication by n map $[n] : A \longrightarrow A$ is an isogeny of degree n^{2g}.*

Proof. Let $\mathcal{L}$ be an ample invertible sheaf on A (it does exist by theorem 2.20). Let $\mathcal{L}' := \mathcal{L} \otimes [-1]^*\mathcal{L}$. Then $[-1]^*\mathcal{L}' \simeq \mathcal{L}'$ because $[-1]$ is an involutory isomorphism. Then by corollary 2.16, we have $[n]^*\mathcal{L}' \simeq \mathcal{L}'^{\otimes \frac{n(n+1)}{2}} \otimes [-1]^*\mathcal{L}'^{\otimes \frac{n(n-1)}{2}} \simeq \mathcal{L}^{\otimes n^2}$.

By proposition 2.11 and lemma 2.12, to prove that $[n]$ is an isogeny, it suffices to prove that $\dim(\ker([n])) = 0$. By contradiction, if $\dim(\ker([n])) > 0$, then there exists $Z \subseteq \dim(\ker([n]))$, a closed irreducible subvariety of dimension 1. But $[n]_{|Z}$ is constant so $[n]^*\mathcal{L}'_{|Z} \simeq \mathcal{L}'^{\otimes n^2}_{|Z}$ is trivial by lemma 1.41.(ii). As a consequence, the numerical polynomial function:

$$m \in \mathbb{Z} \longmapsto \chi(Z, \mathcal{L}'^{\otimes n^2 m}_{|Z})$$

is constant, so $(\mathcal{L}'^{\otimes n^2} \cdot Z) = 0$ (as the dominant coefficient of this polynomial). Besides, $\mathcal{L}' = \mathcal{L} \otimes [-1]^*\mathcal{L}$ and $\mathcal{L}$ is ample so $[-1]^*\mathcal{L}$ is ample since $[-1]$ is an isomorphism[1], so that $\mathcal{L}'$ is ample and $\mathcal{L}'^{\otimes n^2}_{|Z}$ as well (by proposition 1.59.(i) and (ii)). It follows that $(\mathcal{L}'^{\otimes n^2} \cdot Z) > 0$ by lemma 1.62.(ii). Contradiction. So $[n]$ is indeed an isogeny.

By lemma 1.63, we have:

$$([n]^*\mathcal{L}'^g \cdot A) = \deg([n])(\mathcal{L}'^g \cdot A)$$

Where $\mathcal{L}'^g$ denotes $\mathcal{L}' \cdots \mathcal{L}'$ (g times) and the same for $[n]^*\mathcal{L}'$. But by lemma 1.62.(iii), we also have:

$$([n]^*\mathcal{L}'^g \cdot A) = \left(\left(\mathcal{L}'^{\otimes n^2}\right)^g \cdot A\right) = n^{2g}(\mathcal{L}'^g \cdot A)$$

Since $(\mathcal{L}'^g \cdot A) > 0$ by lemma 1.62.(ii), we conclude that $\deg([n]) = n^{2g}$. □

Lemma 2.22. *Let $m : A \times_k A \longrightarrow A$ be the addition map of A and $0_A \in A(k)$ the neutral element. Then, the differential:*

$$dm_{(0_A,0_A)} : T_{(0_A,0_A)}(A \times_k A) \simeq T_{0_A}(A) \times T_{0_A}(A) \longrightarrow T_{0_A}(A)$$

is the additive map of the k-vector space $T_{0_A}(A)$.

Proof. Let $k[\epsilon] := k(T)/(T^2)$ (where ϵ is the image of the indeterminate T in the quotient). The reader may refer to [6, 6.4, p.149] for a presentation of the following invoked results. We know that $T_{0_A}(A) = (\mathfrak{m}_{A,0_A}/\mathfrak{m}^2_{A,0_A})^*$ can be identified with the set $A(k[\epsilon])_{0_A}$ of homomorphisms $\text{Spec}(k[\epsilon]) \longrightarrow A$ with image

[1] It is an easy consequence of theorem 1.58.

0_A. $0_A \circ \pi_{k[\epsilon]/k} : \mathrm{Spec}(k[\epsilon]) \longrightarrow A$ corresponds to 0_A in $T_{0_A}(A)$, where $\pi_{k[\epsilon]/k} : \mathrm{Spec}(k[\epsilon]) \longrightarrow \mathrm{Spec}(k)$ is the structural map. We also have a k-vector space isomorphism $T_{0_A}(A) \times T_{0_A}(A) \longrightarrow T_{(0_A,0_A)}(A \times_k A)$ induced by:

$$\theta : (\phi_1, \phi_2) \in A(k[\epsilon])_{0_A} \times A(k[\epsilon])_{0_A} \longmapsto \phi_1 \times \phi_2 \in (A \times_k A)(k[\epsilon])_{(0_A,0_A)}$$

and $dm_{(0_A,0_A)}$ corresponds to the map:

$$\phi \in (A \times_k A)(k[\epsilon])_{(0_A,0_A)} \longmapsto m \circ \phi \in A(k[\epsilon])_{0_A}$$

If $\varphi_1 \in T_{0_A}(A)$ corresponds to $\phi_1 \in A(k[\epsilon])_{0_A}$, then $(\varphi_1, 0_A)$ corresponds to $(\phi_1, 0_A \circ \pi_{k[\epsilon]/k})$ and we have:

$$dm_{(0_A,0_A)} \circ \theta(\phi_1, 0_A \circ \pi_{k[\epsilon]/k}) = m \circ (\phi_1 \times 0_A \circ \pi_{k[\epsilon]/k}) = \phi_1$$

which corresponds to φ_1, so that $dm_{(0_A,0_A)}$ sends $(\varphi_1, 0)$ to φ_1. By similar arguments, we get that the image of $(0, \varphi_2)$ is φ_2 for all $\varphi_2 \in T_{0_A}(A)$. By linearity of $dm_{(0_A,0_A)}$ we conclude that (φ_1, φ_2) maps to $\varphi_1 + \varphi_2$. □

Proposition 2.23. *$[n] : A \longrightarrow A$ is étale if and only if $p := char(k)$ does not divide n.*

Proof. By proposition 2.21, $[n]$ is an isogeny so it is finite locally free by 2.11, so $[n]$ is flat and we only have to determine when it is unramified.

By lemma 2.22, we get that $d[n]_{0_A} : T_{0_A}(A) \longrightarrow T_{0_A}(A)$ is the multiplication by n map which is injective when p does not divide n and zero otherwise. With the use of translation automorphisms of A, we get that the differential of $[n]$ is either injective on the whole of A when p does not divide n or zero otherwise. Therefore, by lemma 1.35, $[n]$ is étale if and only if p does not divide n. □

Theorem 2.24 (structure of torsion subgroups)**.** *Assume that k is algebraically closed. Let $p := char(k)$ and $g := dim(A)$.*

(i) *If p does not divide n, then $A[n] := ker([n] : A \longrightarrow A) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.*

(ii) *If $p > 0$, then there exists $f \in [\![0\ ;\ g]\!]$ such that $A[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^f$ for all $m \in \mathbb{N}$.*

Proof. (i) We already know that $[n]$ is finite locally free and unramified of degree n^{2g}. By proposition 1.37, we get that $|A[n]| = n^{2g}$. Since we also have $|A[m]| = m^{2g}$ for all divisor m of n, we conclude by the following lemma.

(ii) is much more difficult. See [3, lemma 39.9.10]. The idea is to factor $[p]$ locally by a homeomorphism of degree p^g. □

Lemma 2.25. *Let $(G, +)$ be a finite abelian group of order n^r (for $n, r \in \mathbb{N}^*$) such that for all divisor m of n, the order of the m-torsion subgroup is $|G[m]| = m^r$. Then, $G \simeq (\mathbb{Z}/n\mathbb{Z})^r$.*

Proof. By the structure theorem of finite abelian groups, there exists $s \in \mathbb{N}^*$ and $d_1, \cdots, d_s \in \mathbb{N}^*$ such that $G \simeq \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$ and $2 \leq d_1 | \cdots | d_s$. Then, we immediately get that:

$$G[d_1] \simeq \prod_{i=1}^{s} (\mathbb{Z}/d_i\mathbb{Z})[d_1] \simeq \prod_{i=1}^{s} \mathbb{Z}/d_1\mathbb{Z}$$

so that $|G[d_1]| = d_1^s = d_1^r$, so that $s = r$. Besides, $|G| = \prod_{i=1}^r d_i = n^r$ and $G = G[n]$, so $d_i | n$ for all $i \in [\![1\ ;\ r]\!]$ and necessarily $d_1 = \cdots = d_r = n$. This completes the proof. □

Chapter 3

The $\mathbb{Z}$-module Hom(A, B)

Throughout this chapter, k will be assumed algebraically closed (unless otherwise stated) and we will denote $p := \mathrm{char}(k)$.

3.1 The Tate module

Throughout this paragraph, ℓ will be a prime number. Let A be an abelian variety. Then, the family of torsion subgroups $(A[\ell^n])_{n\in\mathbb{N}^*}$, together with the maps $A[\ell^m] \longrightarrow A[\ell^n]$ induced by the ℓ^{m-n} multiplication for all positive integers $n \leq m$ form a projective system. Then, we can consider the *Tate module* of A as the projective limit:

$$T_\ell(A) = \varprojlim A[\ell^m]$$

$T_\ell(A)$ has a natural structure of $\mathbb{Z}_\ell$-module. Indeed, we have the following descriptions:

$$\mathbb{Z}_\ell = \left\{ (\lambda_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/\ell^n\mathbb{Z} \;\middle|\; \forall m \geq n \geq 1,\ \lambda_n \equiv \lambda_m\ [\ell^n] \right\}$$

$$T_\ell(A) = \left\{ (x_n)_{n\in\mathbb{N}^*} \in \prod_{n\in\mathbb{N}} A[\ell^n] \;\middle|\; \forall m \geq n \geq 1,\ x_n \equiv \ell^{m-n} x_m \right\}$$

And we can define the external law as follows:

$$\forall \lambda := (\lambda_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}_\ell,\ x := (x_n)_{n\in\mathbb{N}^*} \in T_\ell(A), \quad \lambda \cdot x := (\lambda_n x_n)_{n\in\mathbb{N}^*}$$

This law is well defined because we have for all positive integers $m \geq n$, $\ell^{m-n}\lambda_m x_m = \lambda_n x_n$ (since $\lambda_n \equiv \lambda_m\ [\ell^n]$ and x_n is of order ℓ^n).

Proposition 3.1. *$T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module. Let us denote $g := dim(A)$. Then:*

$$rank_{\mathbb{Z}_\ell} T_\ell(A) = \begin{cases} 2g & if\ \ell \neq p \\ f & if\ \ell = p \end{cases}$$

for a certain $f \in [\![0\ ;\ g]\!]$.

Proof. It is a direct consequence of 2.23: there exists $r \in \mathbb{N}^*$ such that for all $n \in \mathbb{N}^*$, $A[\ell^n] \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^r$ and $r = 2g$ if $\ell \neq \mathrm{char}(k)$ and $r \in [\![0\ ;\ g]\!]$ otherwise.

We will recursively construct a basis for $T_\ell(A)$. Let $e_1^{(1)}, \cdots, e_1^{(r)} \in A[\ell]$ be a $\mathbb{Z}/\ell\mathbb{Z}$ basis for $A[\ell]$. For all, $i \in [\![0\ ;\ r]\!]$, we easily construct recursively $e^{(r)} := (e_n^{(i)})_{n\in\mathbb{N}^*}$ such that $[\ell]e_{n+1}^{(i)} = e_n^{(i)}$ because $[\ell]$ is surjective as any isogeny (by 2.21). $(e^{(1)}, \cdots, e^{(r)})$ is actually a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$.

To prove the linear independence of the $e^{(i)}$s, it suffices to prove that the $e_n^{(i)}$ are linearly independent over $\mathbb{Z}/\ell^n\mathbb{Z}$ for all $n \in \mathbb{N}^*$. We proceed by induction. For $n = 1$ this is trivial by hypothesis. Let $n \geq 2$ and suppose that the $e_{n-1}^{(i)}$ are linearly independent over $\mathbb{Z}/\ell^{n-1}\mathbb{Z}$. Let $\lambda_1, \cdots, \lambda_r \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that $\sum_{i=1}^r \lambda_i e_n^{(i)} = 0$. Then, we multiply this equality by ℓ to obtain $0 = \sum_{i=1}^r \lambda_i [\ell] e_n^{(i)} = \sum_{i=1}^r \lambda_i e_{n-1}^{(i)}$ and we get $\lambda_i \equiv 0\ [\ell^{n-1}]$ so that $\lambda_i = \mu_i \ell^{n-1}$ for a certain $\mu_i \in \mathbb{Z}$ for all $i \in [\![1\ ;\ r]\!]$. Then, we have:

$$0 = \sum_{i=1}^r \lambda_i e_n^{(i)} = \sum_{i=1}^r \mu_i [\ell^{n-1}] e_n^{(i)} = \sum_{i=1}^r \mu_i e_1^{(i)}$$

and we conclude that the μ_i are zero by linear independence of the $e_1^{(i)}$s, so that $\lambda_1 = \cdots = \lambda_r = 0$, which completes the induction.

Let $x \in T_\ell(A)$. Then, for all $n \in \mathbb{N}^*$, $(e_n^{(i)})_{n\in\mathbb{N}^*}$ is a basis of $A[\ell^n]$ so there exist $\lambda_n^{(1)}, \cdots, \lambda_n^{(r)} \in \mathbb{Z}/\ell^n\mathbb{Z}$ such that $x_n = \sum_{i=1}^r \lambda_n^{(i)} e_n^{(i)}$. Then, for all positive integers $m \geq n$, $[\ell^{m-n}]x_m = x_n$ so:

$$\sum_{i=1}^r \lambda_m^{(i)} [\ell^{m-n}] e_m^{(i)} = \sum_{i=1}^r \lambda_m^{(i)} e_n^{(i)} = \sum_{i=1}^r \lambda_n^{(i)} e_n^{(i)}$$

So that $\lambda_m^{(i)} \equiv \lambda_n^{(i)}\ [\ell^n]$ for all $i \in [\![1\ ;\ n]\!]$ by linear independence of the $e_n^{(i)}$s. Then, we get that $\lambda^{(i)} := (\lambda_n^{(i)})_{n\in\mathbb{N}^*} \in \mathbb{Z}_\ell$ for all $i \in [\![1\ ;\ n]\!]$ and that $x = \sum_{i=1}^r \lambda^{(i)} e^{(i)}$, which completes the proof. □

Taking the Tate module T_ℓ is actually functorial. Indeed, if A and B are abelian varieties, and if $\varphi \in \operatorname{Hom}(A, B)$, then φ induces a $\mathbb{Z}/\ell^n\mathbb{Z}$-linear map $A[\ell^n] \longrightarrow B[\ell^n]$ for all $n \in \mathbb{N}^*$ (as φ is a group homomorphism) and we can define a $\mathbb{Z}_\ell$-linear map:

$$\begin{array}{rcl} T_\ell(\varphi) : T_\ell(A) & \longrightarrow & T_\ell(B) \\ (x_n)_{n\in\mathbb{N}^*} & \longmapsto & (\varphi(x_n))_{n\in\mathbb{N}^*} \end{array}$$

This defines a $\mathbb{Z}$-linear map $\operatorname{Hom}(A, B) \longrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$. Mapping $(\lambda, \varphi) \in \mathbb{Z}_\ell \times \operatorname{Hom}(A, B)$ to $\lambda \cdot T_\ell(\varphi)$ defines a $\mathbb{Z}$-bilinear map which induces a $\mathbb{Z}_\ell$-linear map:

$$\rho_\ell : \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(A, B) \longrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

by the universal property of the tensor product. The purpose of this chapter is to study this map. The climax will be reached with theorem 3.11.

3.2 More results on morphisms and isogenies

3.2.1 Factorization

Lemma 3.2. *Let $\alpha : A \longrightarrow B$ be an étale isogeny and $\beta : A \longrightarrow C$ a morphism of abelian varieties. Suppose that $\ker(\alpha) \subseteq \ker(\beta)$. Then, there exists a (unique) morphism of abelian avrieties $\gamma : B \longrightarrow C$ such that $\beta = \gamma \circ \alpha$.*

Proof. We only give a sketch for the proof of this very subtle result. For more details, the reader may refer to [2, chapter II.7]. If G is a finite subgroup (variety) of A, then G acts freely by translation on A. Therefore, we can define the quotient A/G which is topologically and schematically what we expect for a group quotient (see [2, theorem p.66]). In addition, A/G is an abelian variety, the projection $\pi : A \longrightarrow A/G$ is an étale isogeny and A/G satisfies the following universal property: every morphism of abelian varieties $A \longrightarrow A'$ whose kernel contains G factors through π.

Taking $G := \ker(\alpha)$, it follows immediately that α and β factor through $\pi : A \longrightarrow A/G$. But π and α are essentially the same. Indeed, if we write $\alpha = h \circ \pi$ with a given morphism $h : A/G \longrightarrow B$, we get that h is bijective and étale so it is an isomorphism (as a consequence of Zariski's main theorem [3, lemma 37.39.1]). □

Lemma 3.3. *Let A and B be abelian varieties. If there is an isogeny $A \longrightarrow B$, then there exists an isogeny $B \longrightarrow A$.*

Proof. Let $\alpha : A \longrightarrow B$ be an isogeny. We can assume that α is étale because otherwise, we can factor it by an étale isogeny (this is a difficult result proved in [12, corollary 5.8]). Since $\ker(\alpha)$ is a finite subgroup (scheme) of A, we have an inclusion $\ker(\alpha) \subseteq A[n]$ for some $n \in \mathbb{N}^*$ and 3.2 ensures that there is a morphism $\beta : B \longrightarrow A$ such that $[n] = \beta \circ \alpha$. This morphism is surjective because $[n]$ is an isogeny (by proposition 2.21) and has finite kernel (because α is surjective and $[n]$ has finite kernel) so it is an isogeny. □

The preceding lemma ensures that the existence of isogenies between abelian varieties is a symmetric relation. We say that two abelian varieties A and B are *isogenous* if there exists an isogeny between A and B.

3.2.2 The degree map

Lemma 3.4. *Let A and B be abelian varieties. Then $Hom(A, B)$ is a torsion-free $\mathbb{Z}$-module. As a consequence, there is an embedding $Hom(A, B) \hookrightarrow Hom^0(A, B)$ where $Hom^0(A, B) := \mathbb{R} \otimes_{\mathbb{Z}} Hom(A, B)$ ($\mathbb{R}$ may be replaced by $\mathbb{Q}$).*

Proof. Let $\varphi \in \mathrm{Hom}(A, B)$. Suppose that there exists $n \in \mathbb{N}^*$ such that $[n]\varphi = 0$. Then, $\varphi(A) \subseteq B[n]$. But A is connected then so does $\varphi(A)$ (because φ is a continuous map). Furthermore, $B[n]$ is a finite set (by 2.23) compound of closed points (by 1.30) so $\varphi(A)$ must be a singleton, and then $\varphi = 0$.

Consider $\varphi \in \mathrm{Hom}(A, B) \longmapsto 1 \otimes \varphi \in \mathrm{Hom}^0(A, B)$. We prove that this map is injective. Indeed, if $\varphi \neq 0$, then $M := \mathbb{Z}\varphi$ is a free $\mathbb{Z}$-module so we have a bilinear map $(\lambda, [n] \circ \varphi)\mathbb{R} \times M \longmapsto \lambda n \in \mathbb{R}$ factoring through the tensor product $\mathbb{R} \otimes_{\mathbb{Z}} M \subseteq \mathrm{Hom}^0(A, B)$ and $1 \otimes \varphi$ is the image of $(1, [1] \circ \varphi)$ in the tensor product whose image is $1 \neq 0$, so that $1 \otimes \varphi \neq 0$. □

Lemma 3.5. *Set $g := dim(A)$. Given $\varphi_1, \cdots, \varphi_r \in End(A)$, the map:*

$$(n_1, \cdots, n_r) \in \mathbb{Z}^r \longmapsto deg\left(\sum_{i=1}^{r} n_i \varphi_i\right) \in \mathbb{Z}$$

is a numerical polynomial which is homogenous and of degree $2g$ (with the convention $deg(\varphi) = 0$ if $\varphi \in End(A)$ is not an isogeny).

Proof. By multiplicativity of the degree of field extensions, the degree map is also multiplicative and, we have for all $\varphi \in \mathrm{End}(A)$ and $n \in \mathbb{N}$, $\deg([n] \circ \varphi) = \deg([n])\deg(\varphi) = n^{2g}\deg(\varphi)$ by proposition 2.21. If the degree map is a polynomial, it is immediate that it is homogeneous of degree $2g$.

First, we prove that given $\varphi, \psi \in \mathrm{End}(A)$, the map $n \longmapsto \deg(n\varphi + \psi)$ is a numerical polynomial. Let $\mathcal{L}$ be an ample invertible sheaf on A (it does exist by theorem 2.20). Then, we have by lemma 1.63:

$$((n\varphi + \psi)^*\mathcal{L}^g \cdot A) = \deg(n\varphi + \psi)(\mathcal{L}^g \cdot A)$$

(where the exponent g means that terms are repeated g times). By 1.62.(ii), $(\mathcal{L}^g \cdot A) > 0$ because $\mathcal{L}$ is ample, so it suffices to prove that the left term is polynomial of degree $\leq 2g$. Set $\mathcal{L}_n := (n\varphi + \psi)^*\mathcal{L}$. Applying 2.19 with $f_1 := n\varphi + \psi$ and $f_2 = f_3 := \varphi$, we get that:

$$\mathcal{L}_{n+2} \otimes \mathcal{L}_{n+1}^{\otimes -2} \otimes \mathcal{L}_n \otimes (2\varphi)^*\mathcal{L}^{\otimes -1} \otimes \varphi^*\mathcal{L}^{\otimes 2} \simeq \mathcal{O}_A$$

Let $\mathcal{L}' := (2\varphi)^*\mathcal{L} \otimes \varphi^*\mathcal{L}^{\otimes -2}$. Then, we get easily by induction on n that for all $n \geq 2$:

$$\mathcal{L}_n = \mathcal{L}'^{\otimes \frac{n(n-1)}{2}} \otimes \mathcal{L}_1^{\otimes n} \otimes \mathcal{L}_0^{\otimes (n-1)}$$

By lemma 1.62.(iii), we get that for all $n \in \mathbb{N}^*$:

$$(\mathcal{L}_n^g \cdot A) = \left(\frac{n(n-1)}{2}\right)^g (\mathcal{L}'^g \cdot A) + n^g(\mathcal{L}_1^g \cdot A) + (n-1)^g(\mathcal{L}_0^g \cdot A)$$

It follows that $n \longmapsto \deg(n\varphi + \psi)$ is a numerical polynomial.

We conclude by induction on $r \in \mathbb{N}^*$. For $\varphi_1, \cdots, \varphi_r, \psi \in \mathrm{End}(A)$, we prove that $f : (n_1, \cdots, n_r) \longmapsto \deg\left(\sum_{i=1}^r n_i\varphi_i + \psi\right)$ is polynomial. For $r = 1$, we already proved the result. Let $r \geq 2$ and assume the result for $r - 1$. Then, by the case $n = 1$, we may write f as follows:

$$\forall n_1, \cdots, n_r \in \mathbb{Z}^r, \quad f(n_1, \cdots, n_r) := \sum_{j=1}^{d} a_j(n_1, \cdots, n_{r-1})n_r^j \quad (\star)$$

where $a_0, \cdots, a_j$ are functions defined on $\mathbb{Z}^{r-1}$. Fixing n_r in a finite set of $d+1$ distinct values $c_0, \cdots, c_r \in \mathbb{Z}$, $(\star)$ becomes a Vandermonde linear system for the variables a_j, so we obtain that the $a_j(n_1, \cdots, n_{r-1})$ are linear combinations of the $f(n_1, \cdots, c_j)$ (independent of the c_j) so they are polynomial by the induction hypothesis. This completes the proof. □

Remark 3.6. One can extend the definition of the degree map to $\mathrm{End}^0(A) = \mathbb{R} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ by homogeneity. It becomes a homogenous polynomial function of degree $2g$.

3.3 Simple isogenies and Poincaré's decomposition

Definition 3.7. An abelian variety A is *simple* if it is non trivial and the only abelian subvarieties of A are $\{0\}$ and A.

Lemma 3.8. *Let A and B be simple abelian varieties and let $\varphi : A \longrightarrow B$ be a morphism. Then φ is either zero or an isogeny.*

Proof. By lemma 2.6, $\varphi(A)$ is an abelian subvariety of B so it is either zero or the whole of B. It remains to prove that $\ker(\varphi)$ is finite i.e. that it is of dimension 0 by lemma 2.12. If not, $\ker(\varphi)$ the irreducible component of 0_A in $\ker(\varphi)$ is a proper non-trivial abelian subvariety of A (a justification of this fact is needed and may be found in [13, theorem 1]), contradicting the simpleness of A. □

Theorem 3.9 (Poincaré's decomposition)**.** *Let A be an abelian variety. Then, there exist simple abelian subvarieties $A_1, \cdots, A_n \subseteq A$ and an isogeny $\prod_{i=1}^n A_i \longrightarrow A$ mapping $(a_1, \cdots, a_n) \in \prod_{i=1}^n A_i(k)$ to $\sum_{i=1}^n a_i$. This decomposition is unique, meaning that the A_i are determined up to isogney.*

Proof. The proof uses dual abelian varieties, a notion we did not study in the course of this seminar so we will admit the theorem. The reader may refer to [2, p. 173]. □

3.4 Towards Tate's theorem

3.4.1 The main theorem

Lemma 3.10. *Let A and B be abelian varieties over k and M a finitely generated subgroup of $Hom(A, B)$. Then the subgroup:*

$$M^{div} := \{\varphi \in Hom(A, B) \mid \exists n \in \mathbb{N}^*, \quad [n] \circ \varphi \in M\}$$

is finitely generated.

Proof. By Poincaré's decomposition (theorem 3.9) and the symmetry of isogenous relation (remark 3.6), there exists two isogenies $\varphi : \prod_{i=1}^{r} A_i \longrightarrow A$ and $\psi : B \longrightarrow \prod_{j=1}^{s} B_i$ where the A_i and B_j are simple abelian varieties. The map:

$$\alpha \in \mathrm{Hom}(A,B) \longmapsto \left(\psi \circ \alpha \circ \varphi_{|A_i}^{|B_j}\right)_{\substack{1\leq i\leq r\\ 1\leq j\leq s}} \in \prod_{i=1}^{r}\prod_{j=1}^{s} \mathrm{Hom}(A_i,B_j)$$

is injective. Indeed, given $\alpha \in \mathrm{Hom}(A,B)$, if we have $\psi \circ \alpha \circ \psi_{|A_i}^{|B_j} = 0$ for all $1 \leq i \leq r, 1 \leq j \leq s$, then by surjectivity of φ, we get $\alpha(A) \subseteq \ker(\psi)$ so the image of α is connected and finite and we conclude that $\alpha = 0$ as in the proof of lemma 3.4. Hence we can assume that A and B are simple. If A and B are not isogenous, we get that $\mathrm{Hom}(A,B) = \{0\}$ by lemma 3.8 and the result is trivial so we assume that A and B are isogenous and get an injection $\mathrm{Hom}(A,B) \hookrightarrow \mathrm{End}(A)$ mapping $\alpha \in \mathrm{Hom}(A,B)$ to $\varphi \circ \alpha$ where $\varphi : B \longrightarrow A$ is an isogeny. Hence, we can assume $A = B$.

With the natural inclusions $\mathrm{End}(A) \subseteq \mathrm{End}^0(A) = \mathbb{R} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ (see lemma 3.5) and $\mathbb{Q} \subseteq \mathbb{R}$, we get easily that $M^{div} = \mathbb{Q} \otimes_{\mathbb{Z}} M \cap \mathrm{End}(A)$. As a consequence, $M^{div} \subset \mathbb{Q} \otimes_{\mathbb{Z}} M \subset \mathbb{R} \otimes_{\mathbb{Z}} M$. Since M is finitely generated, $\mathbb{R} \otimes_{\mathbb{Z}} M$ is a finite dimensional $\mathbb{R}$-vector space. Moreover, lemma 3.5 and the following remark ensure that the degree function $\alpha \in \mathbb{R} \otimes_{\mathbb{Z}} M \longmapsto \deg(\alpha) \in \mathbb{R}$ is a polynomial function so it is continuous, whence the subset $U := \{\alpha \in \mathbb{R} \otimes_{\mathbb{Z}} M \mid \deg(\alpha) < 1\}$ is open. But A is simple so every nonzero endomorphism of A is an isogeny, so is finite locally free by proposition 2.11 and its degree is therefore a positive integer. Since deg maps $\mathrm{End}(A)$ to $\mathbb{N}$, it follows that $M^{div} \cap U = \{0\}$. We have proved that M^{div} is a discrete submodule of a finite dimensional $\mathbb{R}$-vector space. Therefore M^{div} is a Euclidean lattice, hence it is finitely generated. □

Theorem 3.11. *Let A and B be abelian varieties defined over k. If ℓ is a prime number distinct from $p :=$ char(k), then the map:*

$$\rho_\ell : \mathbb{Z}_\ell \otimes_{\mathbb{Z}} Hom(A,B) \longrightarrow Hom_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

defined at the end of section 3.1 is injective.

Proof. Let $\alpha \in \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(A,B)$ such that $\rho_\ell(\alpha) = 0$. Then, we may write $\alpha := \sum_{i=1}^{r} \lambda_i \otimes \varphi_i$ with $\lambda_1, \cdots, \lambda_r \in \mathbb{Z}_\ell$ and $\varphi_1, \cdots, \varphi_r \in \mathrm{Hom}(A,B)$. Let M be the subgroup of $\mathrm{Hom}(A,B)$ generated by the φ_is. It is finitely generated so by lemma 3.10 $M^{div} = \{\varphi \in \mathrm{Hom}(A,B) \mid \exists n \in \mathbb{N}^*, \quad [n] \circ \varphi \in M\}$ is finitely generated. By lemma 3.4, $\mathrm{Hom}(A,B)$ is torsion free and M^{div} as well. Since M^{div} is finitely generated, it is a free $\mathbb{Z}$-module of finite type and it admits a $\mathbb{Z}$-basis. Since $M \subseteq M^{div}$, rewriting α if necessary, we may assume that the φ_i are a $\mathbb{Z}$-basis of M^{div}.

Let $n \in \mathbb{N}^*$ and $c_1, \cdots, c_r \in \mathbb{Z}$ such that $c_i \equiv \lambda_i \ [\ell^n]$ for all $i \in [\![1 \ ; \ r]\!]$. If we look the equality $\rho_\ell(\alpha) = 0$ modulo ℓ^n, we get that $\sum_{i=1}^{r} [c_i] \circ \varphi_i$ vanishes on $A[\ell^n]$. Since $[\ell^n]$ is an étale isogeny (by 2.23), the lemma 3.2 implies the existence of a morphism $\psi : A \longrightarrow B$ such that $\sum_{i=1}^{r} [c_i] \circ \varphi_i = \psi \circ [\ell^n] = [\ell^n] \circ \psi$. But $\psi \in M^{div}$, so there exists $d_1, \cdots, d_r \in \mathbb{Z}$ such that $\psi = \sum_{i=1}^{r} [d_i] \circ \varphi_i$. Since the φ_i are free over $\mathbb{Z}$, $c_i = \ell^n d_i$, so that $\lambda_i \equiv 0 \ [\ell^n]$ for all $i \in [\![1 \ ; \ r]\!]$. These congruences hold for all $n \in \mathbb{N}^*$. Therefore, the λ_i are all zero so $\alpha = 0$. This completes the proof. □

Corollary 3.12. *Let A and B be abelian varieties over k. Then $Hom(A,B)$ is a free $\mathbb{Z}$-module of rank $\leq 4 dim(A) dim(B)$.*

Proof. Let ℓ be a prime number distinct fro $p :=$ cahr(k). By proposition 3.1, $T_\ell(A)$ and $T_\ell(B)$ are free $\mathbb{Z}_\ell$-modules of rank $2\mathrm{dim}(A)$ and $2\mathrm{dim}(B)$ respectively so $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$ is a free $\mathbb{Z}_\ell$-module of rank $4\mathrm{dim}(A)\mathrm{dim}(B)$. Since $\mathrm{Hom}(A,B)$ is torsion free, it follows by the preceding discussion and theorem 3.11 that $\mathrm{Hom}(A,B)$ is of finite type and we get that $\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}(A,B) = \mathrm{rank}_{\mathbb{Z}_\ell}\mathbb{Z}_\ell \otimes \mathrm{Hom}(A,B) \leq 4\mathrm{dim}(A)\mathrm{dim}(B)$. □

3.4.2 Further developments and applications

In this paragraph, k is not algebraically closed. If A and B are abelian varieties defined over k, we have a natural embedding $\operatorname{Hom}(A,B) \hookrightarrow \operatorname{Hom}(A_{\overline{k}}, B_{\overline{k}})$ (defined by extension of scalars). By theorem 3.11, we still get an embedding $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(A,B) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell(A_{\overline{k}}), T_\ell(B_{\overline{k}}))$. It would be interesting to know when this map is surjective. This way, we would be able to understand morphisms between abelian varieties as $\mathbb{Z}_\ell$-linear maps between Tate modules, which are much simpler objects.

Actually, the map is not surjective because the image of $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(A,B)$ is invariant under the action of the Galois group $G := \operatorname{Gal}(\overline{k}/k)$. Let us explain how this action works. Given a k-scheme X, and $\sigma \in G$, we have a morphism of schemes $\operatorname{Spec}(\sigma) : \operatorname{Spec}(\overline{k}) \longrightarrow \operatorname{Spec}(\overline{k})$ and an automorphism $\mathrm{id}_X \times \operatorname{Spec}(\sigma) : X_{\overline{k}} := X \times_k \operatorname{Spec}(\overline{k}) \longrightarrow X_{\overline{k}}$ induced by σ. When $X = A$, the G-action commutes with the multiplication map so it stabilizes $A_{\overline{k}}[\ell^n]$ for all $n \in \mathbb{N}^*$. It follows that G acts on $T_\ell(A_{\overline{k}})$, $T_\ell(B_{\overline{k}})$ and $\operatorname{Hom}(T_\ell(A_{\overline{k}}), T_\ell(B_{\overline{k}}))$. We denote $\operatorname{Hom}_G(T_\ell(A_{\overline{k}}), T_\ell(B_{\overline{k}}))$, the submodule of G-stable elements. It is easy to see that $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \operatorname{Hom}(A,B)$ maps to $\operatorname{Hom}_G(T_\ell(A_{\overline{k}}), T_\ell(B_{\overline{k}}))$.

Theorem 3.13 (Tate 1966). *We assume that k is a finite field. Then, the map*

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} Hom(A,B) \longrightarrow Hom_G(T_\ell(A_{\overline{k}}), T_\ell(B_{\overline{k}}))$$

is bijective for all prime ℓ (including when $\ell = p$).

Proof. See [4] for the original proof and [5] for the conference proceeding of Waterhouse and Milne. □

This theorem has a very interesting application: characterizing isogenous abelian varieties over finite fields. Before going any further, we need to introduce some notions and notations. Let A be an abelian variety defined over a finite field $k := \mathbb{F}_q$ and $\overline{A} := A_{\overline{\mathbb{F}_q}}$.

1. We denote $V_\ell(A) := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A)$ for all prime ℓ.

2. We define the *Frobenius endomorphism* $\pi_A : \overline{A} \longrightarrow \overline{A}$ given by $\mathrm{id}_{\overline{A}}$ topologically and for all open subset $U \subseteq \overline{A}$ by $s \in \Gamma(U, \mathcal{O}_{\overline{A}}) \longmapsto s^q \in \Gamma(U, \mathcal{O}_{\overline{A}})$. Since the Frobenius $x \in \overline{\mathbb{F}_q} \longmapsto x^q \in \overline{\mathbb{F}_q}$ stabilizes $\mathbb{F}_q$, the multiplication map commutes with the Frobenius π_A so it is actually an endomorphism of abelian varieties.

3. Every endomorphism of $\operatorname{End}(\overline{A})$ can be seen as $\mathbb{Z}_\ell$-linear endomorphism in $T_\ell(\overline{A})$ so we can associate a characteristic polynomial to it. We will denote f_A the characteristic polynomial of π_A.

4. We associate to A a *Zeta function* defined as the formal series:

$$Z(A,T) := \exp\left(\sum_{n=1}^{+\infty} |A(\mathbb{F}_{q^n})| \frac{T^n}{n}\right)$$

Theorem 3.14 (Tate 1966). *Let A and B be two abelian varieties defined over $\mathbb{F}_q$. Then, the following statements are equivalent:*

(i) *A and B are isogenous (over $\mathbb{F}_q$).*

(ii) *There exists a prime ℓ such that $V_\ell(A)$ and $V_\ell(B)$ are G-isomorphic (there is an isomorphism commuting with the G-action).*

(iii) $f_A = f_B$.

(iv) $Z(A,T) = Z(B,T)$.

(v) *For all $n \in \mathbb{N}^*$, $|A(\mathbb{F}_{q^n})| = |B(\mathbb{F}_{q^n})|$.*

Proof. See [4] or [5]. □

Bibliography

[1] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[2] David Mumford. *Abelian Varieties.* Oxford University Press, 1970.

[3] Johan de Jong et al. The stack project, 2018. Available at https://stacks.math.columbia.edu/browse.

[4] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2:134–144, september 1966.

[5] W.C. Waterhouse and J.S. Milne. Abelian varieties over finite fields. volume 20 of *Proceedings of Symposia in Pure Mathematics*, pages 53–64, 1971.

[6] Ulrich Görtz and Torsten Wedhorn. *Algebraic Geometry I, Schemes with Examples and Exercices.* Vieweg+Teubner, 2010.

[7] Robin Hartshorne. *Algebraic Geometry.* Springer, 1977.

[8] Hideyuki Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1989.

[9] Ian G. Macdonald Michael Atiyah. *Introduction to commutative algebra.* Addison-Wesley Publishing Company, 1969.

[10] Brian Conrad and Tony Feng. Abelian varieties, 2015. Available at http://math.stanford.edu/ conrad/249CS15Page/handouts/abvarnotes.pdf.

[11] Serge Lang. *Algèbre.* Dunod, 2004.

[12] Gerard van der Geer and Ben Moonen. Abelian varieties, 2020. Available at https://www.math.ru.nl/ bmoonen/research.html.

[13] Quing Liu. Subgroups of semi-abelian varieties, 2011. Available at https://www.math.u-bordeaux.fr/∼qliu/Notes/sub-abelian_varieties.pdf.