Gerard van der Geer
Ben Moonen

ABELIAN VARIETIES

(PRELIMINARY VERSION OF THE FIRST CHAPTERS)

Contents

Notation and conventions **1**

1. Definitions and basic examples **5**

2. Line bundles and divisors on abelian varieties **17**
§ 1. The theorem of the square 17
§ 2. Projectivity of abelian varieties 22
§ 3. Projective embeddings of abelian varieties 26

3. Basic theory of group schemes **29**
§ 1. Definitions and examples 29
§ 2. Elementary properties of group schemes 34
§ 3. Cartier duality 41
§ 4. The component group of a group scheme 43

4. Quotients by group schemes **49**
§ 1. Categorical quotients 49
§ 2. Geometric quotients, and quotients by finite group schemes 52
§ 3. FPPF quotients 61
§ 4. Finite group schemes over a field 66

5. Isogenies **72**
§ 1. Definition of an isogeny, and basic properties 72
§ 2. Frobenius and Verschiebung 76
§ 3. Density of torsion points 83

6. The Picard scheme of an abelian variety **87**
§ 1. Relative Picard functors 87
§ 2. Digression on graded bialgebras 91
§ 3. The dual of an abelian variety 95

7. Duality **98**
§ 1. Formation of quotients and the descent of coherent sheaves 98
§ 2. Two duality theorems 100
§ 3. Further properties of $\mathrm{Pic}^0_{X/k}$ 101
§ 4. Applications to cohomology 108
§ 5. The duality between Frobenius and Verschiebung 110

8. The Theta group of a line bundle **113**
§ 1. The theta group $\mathscr{G}(L)$ 113
§ 2. Descent of line bundles over homomorphisms 116
§ 3. Theta groups of non-degenerate line bundles 118
§ 4. Representation theory of non-degenerate theta groups 122

9. The cohomology of line bundles **126**

10. Tate modules, p-divisible groups, and the fundamental group **141**
§ 1. Tate-ℓ-modules 141

§ 2. The p-divisible group 145
§ 3. The algebraic fundamental group—generalities 149
§ 4. The fundamental group of an abelian variety 154

11. Polarizations and Weil pairings 159
§ 1. Polarizations 159
§ 2. Pairings 162
§ 3. Existence of polarizations, and Zarhin's trick 169
§ 4. Polarizations associated to line bundles on torsors 174
§ 5. Symmetric line bundles 178

12. The endomorphism ring 180
§ 1. First basic results about the endomorphism algebra 180
§ 2. The characteristic polynomial of an endomorphism 184
§ 3. The Rosati involution 188
§ 4. The Albert classification 190

13. The Fourier transform and the Chow ring 192
§ 1. The Chow ring 192
§ 2. The Hodge bundle 196
§ 3. The Fourier transform of an abelian variety 199
§ 4. Decomposition of the diagonal 204
§ 5. Motivic decomposition 210

14. Jacobian Varieties 218
§ 1. The Jacobian variety of a curve 218
§ 2. Comparison with the g-th symmetric power of C 221
§ 3. Universal line bundles and the Theta divisor 224
§ 4. Riemann's Theorem on the Theta Divisor 231
§ 5. Examples 233
§ 6. A universal property—the Jacobian as Albanese 235
§ 7. Any Abelian Variety is a Factor of a Jacobian 236
§ 8. The Theorem of Torelli 237
§ 9. The Criterion of Matsusaka-Ran 239

15. Dieudonné theory 245
§ 1. Dieudonné theory for finite commutative group schemes and for p-divisible groups 245
§ 2. Classification up to isogeny 246
§ 3. The Newton polygon of an abelian variety 262

16. Abelian Varieties over Finite Fields 265
§ 1. The eigenvalues of Frobenius 265
§ 2. The Hasse-Weil-Serre bound for curves 272
§ 3. The theorem of Tate 275
§ 4. Corollaries of Tate's theorem, and the structure of the endomorphism algebra . . . 281
§ 5. Abelian varieties up to isogeny and Weil numbers 289
§ 6. Isomorphism classes contained in an isogeny class 293
§ 7. Elliptic curves 296
§ 8. Newton polygons of abelian varieties over finite fields 302
§ 9. Ordinary abelian varieties over a finite field 303

Appendix A. Algebra **308**
References **314**
Index **321**

Notation and conventions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The absolute Frobenius. Let p be a prime number. Let Y be a scheme of characteristic p. Then we have a morphism $\mathrm{Frob}_Y \colon Y \to Y$, called the *absolute Frobenius morphism of* Y; it is given by

(a) Frob_Y is the identity on the underlying topological space $|Y|$;

(b) $\mathrm{Frob}_Y^\sharp \colon O_Y \to O_Y$ is given on sections by $f \mapsto f^p$.

To describe Frob_Y in another way, consider a covering $\{U_\alpha\}$ of Y by affine open subsets, say $U_\alpha = \mathrm{Spec}(A_\alpha)$. The endomorphism of A_α given by $f \mapsto f^p$ defines a morphism $\mathrm{Frob}_\alpha \colon U_\alpha \to U_\alpha$. On the intersections $U_\alpha \cap U_\beta$ the morphisms Frob_α and Frob_β agree, and by gluing we obtain the absolute Frobenius morphism Frob_Y of Y. Note that Frob_α is none other than the absolute Frobenius morphism of the scheme U_α.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

and

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

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

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