

Chapter I. Definitions and basic examples.

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

(1.1) Definition. A group consists of a non-empty set G together with maps

$$m: G \times G \rightarrow G \quad (\text{the group law}) \quad \text{and} \quad i: G \rightarrow G \quad (\text{the inverse})$$

and a distinguished element

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

such that we have the following equalities of maps.

- (i) Associativity: $m \circ (m \times \text{id}_G) = m \circ (\text{id}_G \times m): G \times G \times G \rightarrow G$.
- (ii) Defining property of the identity element:

$$\begin{aligned} m \circ (e \times \text{id}_G) &= j_1: \{e\} \times G \rightarrow G, & \text{and} \\ m \circ (\text{id}_G \times e) &= j_2: G \times \{e\} \rightarrow G, \end{aligned}$$

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

- (iii) Left and right inverse:

$$e \circ \pi = m \circ (\text{id}_G \times i) \circ \Delta_G = m \circ (i \times \text{id}_G) \circ \Delta_G: G \rightarrow G,$$

where $\pi: G \rightarrow \{e\}$ is the constant map and Δ_G is the diagonal map.

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

- (i) Associativity:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\text{id}_G \times m} & G \times G \\ m \times \text{id}_G \downarrow & & \downarrow m \\ G \times G & \xrightarrow{m} & G \end{array} .$$

- (ii) Identity element:

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

(iii) Two-sided inverse:

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

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

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

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

$$m: X \times X \rightarrow X \quad (\text{the group law}) \quad \text{and} \quad i: X \rightarrow X \quad (\text{the inverse})$$

and a k -rational point

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

such that we have the following equalities of morphisms:

- (i) $m \circ (m \times \text{id}_X) = m \circ (\text{id}_X \times m): X \times X \times X \rightarrow X$.
- (ii) $m \circ (e \times \text{id}_X) = j_1: \text{Spec}(k) \times X \rightarrow X$ and $m \circ (\text{id}_X \times e) = j_2: X \times \text{Spec}(k) \rightarrow X$, where $j_1: \text{Spec}(k) \times X \xrightarrow{\sim} X$ and $j_2: X \times \text{Spec}(k) \xrightarrow{\sim} X$ are the canonical isomorphisms.
- (iii) $e \circ \pi = m \circ (\text{id}_X \times i) \circ \Delta_{X/k} = m \circ (i \times \text{id}_X) \circ \Delta_{X/k}: X \rightarrow X$, where $\pi: X \rightarrow \text{Spec}(k)$ is the structure morphism.

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

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

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

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

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

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

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

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

and

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

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

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

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

and

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

where we write $x_T: T \rightarrow X_T$ for the morphism $(x, \text{id}_T): T \rightarrow X \times_k T = X_T$.

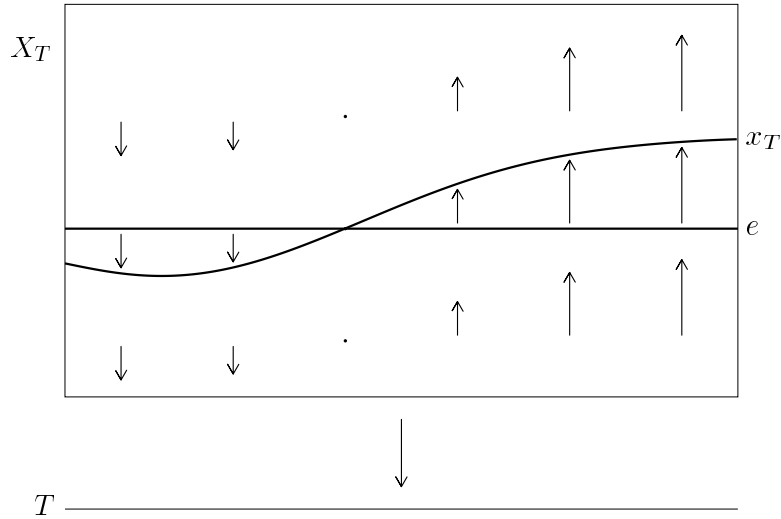


Figure 1.

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

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

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

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

Set $S = \text{Spec}(k[\varepsilon]/(\varepsilon^2))$. Let $X_S := X \times_k S$, where the morphism $S \rightarrow \text{Spec}(k)$ is given on rings by $a \mapsto a + 0 \cdot \varepsilon$. We may think of X_S as a “thickened” version of X . Tangent vectors $\tau \in T_{X,e}$ correspond to S -valued points $\tilde{\tau}: S \rightarrow X$ which reduce to $e: \text{Spec}(k) \rightarrow X$ modulo ε . (See Exercise 1.3.) A vector field on X is given by an automorphism $X_S \rightarrow X_S$ which reduces to the identity on X . To a tangent vector τ we can thus associate the vector field $\xi(\tau)$ given by

the right translation $t_{\bar{\tau}}$. The map $T_{X,e} \rightarrow \Gamma(X, \mathcal{T}_{X/k})$ given by $\tau \mapsto \xi(\tau)$ is k -linear and induces a homomorphism $\alpha: T_{X,e} \otimes_k O_X \rightarrow \mathcal{T}_{X/k}$.

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

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

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

The last assertion of the proposition now follows from the identities $\Omega_{X/k}^1 = \mathcal{T}_{X/k}^\vee$ and $\Omega_{X/k}^n = \wedge^n \Omega_{X/k}^1$. \square

With notations as in the proof, note that $t_{\bar{\tau}}$ commutes with all left translations. It follows that the vector field $\xi(\tau)$ is left invariant, i.e., for every left translation t' we have $t'_*\xi(\tau) = \xi(\tau)$. The map $\tau \mapsto \xi(\tau)$ identifies $T_{X,e}$ with the space of left invariant vector fields on X . In case X is an abelian variety, so that $\Gamma(X, O_X) = k$, we can restate (1.5) by saying that all global vector fields are left invariant.

If X is an abelian variety, these are the only global vector fields on X , since $\Gamma(X, O_X) = k$.

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

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

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

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

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

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

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

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

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{with } a_i \in k. \quad (1)$$

The functions x and y define a rational map

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

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

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

$$\alpha: E(k) \rightarrow \text{Cl}^0(E) \quad \text{given by } Q \mapsto [Q - P]$$

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

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

The group law just defined has the following geometric interpretation. Here we shall write $A \oplus B$ for the group law and $\ominus A$ for the inverse.

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

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

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

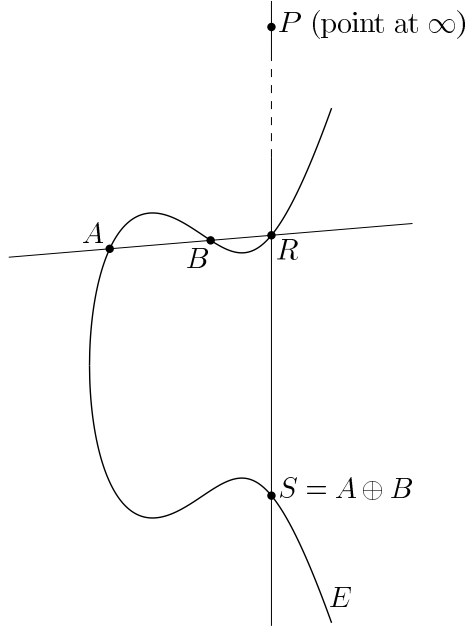


Figure 2.

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

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

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

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

1
6
20
1357
8385
12551561
1849037896
4881674119706
2786836257692691
79799551268268089761
280251129922563291422645
54202648602164057575419038802
3239336802390544740129153150480400
1425604881483182848970780090473397497201
596929565407758846078157850477988229836340351
1356533706384096591887827693333962338847777347485221
2389750519110914018630990937660635435269956452770356625916
47551938020942325784141569050513811957803129798534598981096547726
43276783438948886312588030404441444313405755534366254416432880924019065
66655479518893093532610447590226207125008330695731551720689810858664307580428417

Figure 3.

grows quadratically in n ; see Figure 3.

(1.9) Example. Now we try to generalize the above example, taking a curve of genus 2. So, let C be a smooth projective curve of genus $g = 2$ over a field k . Then C is a hyperelliptic curve and can be described as a double covering $\pi: C \rightarrow \mathbb{P}_k^1$ of the projective line. Let i be the hyperelliptic involution of C . Consider the surface $C \times C$, on which we have an involution ι given by $(a, b) \mapsto (b, a)$. The quotient $S^2C = (C \times C)/\iota$ is a non-singular surface. The image of the anti-diagonal $\Delta^- = \{(a, i(a)) : a \in C\}$ on S^2C is a curve D which is isomorphic to $C/i = \mathbb{P}^1$ and has self-intersection number $\frac{1}{2}(\Delta^-)^2 = (2 - 2g)/2 = -1$, i.e., D is an exceptional curve. By elementary theory of algebraic surfaces we can blow D down, obtaining a non-singular projective surface S .

We claim that there is a bijection

$$\alpha: S(k) \xrightarrow{\sim} \text{Cl}^0(C).$$

To define α we look at the map $S^2C(k) \rightarrow \text{Cl}^0(C)$ given by $(a, b) \mapsto [a + b] - [K]$, where $[K]$ is the canonical divisor class. Since $[a + i(a)] = [K]$ for every $a \in C$, this map factors through the contraction of D and we get a map $\alpha: S(k) \rightarrow \text{Cl}^0(C)$. If $a + b \sim c + d$ with $a \neq c \neq b$ then $\ell(a + b) \geq 2$, and it follows by Riemann-Roch that $[a + b] = [K]$. (Indeed, we have $\ell(a + b) - \ell(K - a - b) = 1$, so $\ell(a + b) \geq 2$ implies that the degree zero divisor $K - a - b$ is effective, hence equivalent to zero.) This shows that α is injective. It is surjective by Riemann-Roch.

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

We claim that the addition and inverse on $S(k)$ are given by morphisms. For the inverse this is easy: the inverse of (a, b) is given by $(i(a), i(b))$, again using that $x + i(x) \sim K$ for all points x . To see that addition is given by a morphism, consider the projection $\pi: C^5 \rightarrow C^4$ onto the first four factors. This map has four natural sections $(p_1, p_2, p_3, p_4) \mapsto (p_1, \dots, p_4, p_i)$, and this defines a relative effective divisor D of degree 4 on C^5 over C^4 . Let K be a fixed canonical divisor on the last factor C . By the Riemann-Roch theorem for the curve C over the function field $k(C^4)$ the divisor $D - K$ is linearly equivalent to an effective divisor of degree 2 on C over $k(C^4)$. It follows that D is linearly equivalent to a divisor of the form $E + \pi^*(G)$, with E

a relative effective divisor of degree 2 and G a divisor on C^4 . The restriction of E to a fibre $\{P = (p_1, p_2, p_3, p_4)\} \times C$ is of degree 2, hence determines a point $\psi(P)$ of S^2C . This gives a map $\psi: C^4 \rightarrow S^2C$ which is clearly a morphism. If $\beta: S^2C \rightarrow S$ is the blowing-down of Δ^- then the composition $C^4 \rightarrow S^2C \rightarrow S$ factors through $\beta \times \beta$. The resulting morphism $S \times S \rightarrow S$ is precisely the addition on S .

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

(1.10) Example. In this example we work over the field $k = \mathbb{C}$. Consider a complex vector space V of finite dimension n . For an additive subgroup $L \subset V$ the following conditions are equivalent: (i) $L \subset V$ is discrete and co-compact, i.e., the euclidean topology on V induces the discrete topology on L and the quotient $X := V/L$ is compact for the quotient topology; (ii) the natural map $L \otimes_{\mathbb{Z}} \mathbb{R} \rightarrow V$ is bijective; (iii) there is an \mathbb{R} -basis e_1, \dots, e_{2n} of V such that $L = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_{2n}$. A subgroup satisfying these conditions is called a *lattice* in V .

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

Let us first consider the case $n = 1$. By a well-known theorem of Riemann, every compact Riemann surface is algebraic. Since X has genus 1, it can be embedded as a non-singular cubic curve in $\mathbb{P}_{\mathbb{C}}^2$, see (1.7). If $\varphi: X \hookrightarrow \mathbb{P}_{\mathbb{C}}^2$ is such an embedding, write $E = \varphi(X)$ and $P = \varphi(0)$. We see that (E, P) is an elliptic curve (taking P to be the identity element). The structure of a group variety on E as defined in (1.7) is the same as the group structure on X , in the sense that $\varphi: X \xrightarrow{\sim} E^{\text{an}}$ is an isomorphism of Lie groups.

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

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

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

Proof. We may assume that $k = \bar{k}$. Choose a point $x_0 \in X(k)$, and define a morphism $g: Y \rightarrow Z$ by $g(y) = f(x_0, y)$. Our goal is to show that $f = g \circ \text{pr}_Y$. As $X \times Y$ is reduced it suffices to prove this on k -rational points.

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. (i) If (X, m, i, e) and (X, n, j, e) are abelian varieties then m and n are equal when restricted to $X \times \{e\}$ and $\{e\} \times X$. Applying (1.11) to $m \circ (m, i \circ n): X \times X \rightarrow X$, which is constant when restricted to $X \times \{e\}$ and $\{e\} \times X$, we get $m = n$. This readily implies that $i = j$ too.

(ii) By the previous proposition, the map $i: X \rightarrow X$ is a homomorphism. This implies that the group structure is abelian. \square

(1.15) Remark. It is worthwhile to note that in deriving the commutativity of the group the completeness of the variety is essential. Examples of non-commutative group varieties are linear algebraic groups (i.e., matrix groups) like GL_n for $n > 1$, the orthogonal groups O_n for $n > 1$ and symplectic groups Sp_{2n} .

(1.16) Notation. From now on we shall mostly use the additive notation for abelian varieties, writing $x + y$ for $m(x, y)$, writing $-x$ for $i(x)$, and 0 for e . Since abelian varieties are abelian as group varieties, we no longer have to distinguish between left and right translations. Also

we can add homomorphisms: given two homomorphisms of abelian varieties $f, g: X \rightarrow Y$, we define $f + g$ to be the composition

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

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

As we have seen, also $\text{Hom}_{\text{Sch}/k}(X, Y) = Y(X)$ —the set of X -valued points of Y —has a natural structure of an abelian group. By Prop. (1.13), $\text{Hom}_{\text{AV}}(X, Y)$ is just the subgroup of $\text{Hom}_{\text{Sch}/k}(X, Y)$ consisting of those morphisms $f: X \rightarrow Y$ such that $f(0_X) = 0_Y$, and $\text{Hom}_{\text{Sch}/k}(X, Y) = \text{Hom}_{\text{AV}}(X, Y) \times Y(k)$ as groups. We shall adopt the convention that $\text{Hom}(X, Y)$ stands for $\text{Hom}_{\text{AV}}(X, Y)$. If there is a risk of confusion we shall indicate what we mean by a subscript “AV” or “Sch/ k ”.

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

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

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

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

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

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

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

where the sum runs over all codimension 1 points $P \in |V \times V|$ with $\text{ord}_P(F^\sharp(\varphi)) < 0$. If (w, w) is a k -valued point in $\Delta \cap |D|$ then $F^\sharp(\varphi)$ is not in $O_{V \times V, (w,w)}$, hence F is not regular at (w, w) . But $V \times V$ is a regular scheme, so $D \subset V \times V$ is locally a principal divisor. Then also $\Delta \cap |D|$ is locally defined, inside Δ , by a single equation, and it follows that $\Delta \cap |D|$ has codimension ≤ 1 in Δ . Hence f is not regular on a subset of V of codimension ≤ 1 , contradicting our earlier conclusion that $\text{codim}_X(X \setminus U) \geq 2$. \square

Exercises.

(1.1) Let X_1 and X_2 be varieties over a field k .

- (i) If X_1 and X_2 are given the structure of a group variety, show that their product $X_1 \times X_2$ naturally inherits the structure of a group variety.
- (ii) Suppose $Y := X_1 \times X_2$ carries the structure of an abelian variety. Show that X_1 and X_2 each have a unique structure of an abelian variety such that $Y = X_1 \times X_2$ as abelian varieties.

(1.2) Check that an equivalent definition of an abelian variety is the following. An abelian variety is a 4-tuple (X, m, i, e) consisting of a complete k -variety X together with morphisms

$$m: X \times X \rightarrow X, \quad i: X \rightarrow X \quad \text{and} \quad e: \text{Spec}(k) \rightarrow X$$

such for every k -scheme T the set of T -valued points $X(T)$ together with the maps m, i and e forms a group, and such that the map $T \mapsto X(T)$ defines a contravariant functor from the category of k -schemes to the category of groups.

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

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

$$H^0(X, \mathcal{T}_{X/k}) \cong \text{Hom}_k(\Omega_{A/k}^1, A) \cong \text{Der}_k(A, A).$$

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

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

$$h: H^0(X, \mathcal{T}_{X/k}) \xrightarrow{\sim} \text{Aut}^{(1)}(X_S/S).$$

- (iv) Suppose X is a group variety over k . If $x \in X(k)$ and $\tau: S \rightarrow X$ is a tangent vector at x , check that the associated global vector field $\xi := h^{-1}(t_\tau)$ is right-invariant, meaning that $t_y^* \xi = \xi$ for all $y \in X$.

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

(1.5) Let E be the elliptic curve over \mathbb{Q} given by the Weierstrass equation $y^2 + y = x^3 - x$, with origin $P_\infty = (0 : 1 : 0)$. Let Q be the rational point $(-1, -1)$. Compute $m \cdot Q$ for $m = 2, 4$ and 10 .

(1.6) Let X_1, X_2, Y_1 and Y_2 be abelian varieties over a field k . Show that

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

Does a similar statement hold if we everywhere replace “ Hom_{AV} ” by “ Hom_{Sch} ” ?

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

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

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