

# Abelian varieties over finite fields

Lassina Dembélé

[lassina.dembele@kcl.ac.uk](mailto:lassina.dembele@kcl.ac.uk)

King's College London

Preliminary Arizona Winter School 2024

Version: October 5, 2023

## Contents

<b>1</b>	<b>Definition and properties of abelian varieties</b>	<b>3</b>
1.1	Definition . . . . .	3
1.2	Commutativity . . . . .	4
1.3	Theorem of the cube . . . . .	4
1.4	Theorem of the square . . . . .	5
1.5	Isogenies . . . . .	5
1.6	Structure of torsion . . . . .	5
<b>2</b>	<b>The dual variety</b>	<b>7</b>
2.1	Definition of the dual . . . . .	7
2.2	Construction of the dual . . . . .	7
2.3	Polarisations . . . . .	7
<b>3</b>	<b>Structure of the isogeny category</b>	<b>8</b>
3.1	Poincaré reducibility . . . . .	8
3.2	The isogeny category . . . . .	8
<b>4</b>	<b>Basic example: elliptic curves</b>	<b>8</b>
4.1	Definition of an elliptic curve . . . . .	8
4.2	Definition of the group law . . . . .	10
4.3	Computing with the group law . . . . .	12
<b>5</b>	<b>Endomorphism rings and Tate modules</b>	<b>14</b>
5.1	Endomorphism ring of an abelian variety . . . . .	14
5.2	The Tate module of an abelian variety . . . . .	15
5.3	The Tate module of the multiplicative group . . . . .	16
5.4	The Weil pairings . . . . .	16

## 1 Definition and properties of abelian varieties

We fix a field  $k$ , and let  $\bar{k}$  be an algebraic closure of  $k$ . We recall the definition and basic properties of abelian varieties. We give some indications as to how the theory is developed, but omit most of the arguments....

### 1.1 Definition

**Definition 1.1.** A algebraic variety  $X$  over  $k$  is a separated  $k$ -scheme  $X$  of finite type, which is geometrically integral (i.e.  $X \times_{\text{Spec}(k)} \text{Spec}(\bar{k})$  is integral). We say that  $X$  is complete if it is proper.

**Definition 1.2.** A group variety over a field  $k$  is a  $k$ -variety  $G$  together with  $k$ -morphisms  $m : G \times G \rightarrow G$  (the group law) and  $i : G \rightarrow G$  (the inverse) and a  $k$ -rational point  $e \in G(k)$  (the identity element) such that we have the following commutative diagrams:

(i) Associativity of the group law:

$$\begin{array}{ccccc}
 G \times G \times G & \xrightarrow{id_{G \times G \times G}} & (G \times G) \times G & \xrightarrow{m \times id_G} & G \times G \\
 id_{G \times G \times G} \downarrow & & & & \downarrow m \\
 G \times (G \times G) & \xrightarrow{id_G \times m} & G \times G & \xrightarrow{m} & G
 \end{array}$$

(ii) Identity element:

$$\begin{array}{ccccc}
 G \times \text{Spec}(k) & \xrightarrow{id_G \times e} & G \times G & \xleftarrow{e \times id_G} & \text{Spec}(k) \times G \\
 & \searrow j_1 & \downarrow m & \swarrow j_2 & \\
 & & G & & 
 \end{array}$$

where  $j_1 : \text{Spec}(k) \times G \rightarrow G$  and  $j_2 : G \times \text{Spec}(k) \rightarrow G$  are the projection maps on  $G$ .

(iii) Existence of inverse element:

$$\begin{array}{ccccc}
 G & \xrightarrow{\pi} & \text{Spec}(k) & \xleftarrow{\pi} & G \\
 (id_G, i) \downarrow & & \downarrow e & & \downarrow (i, id_G) \\
 G \times G & \xrightarrow{m} & G & \xleftarrow{m} & G \times G
 \end{array}$$

where  $\pi : G \rightarrow \text{Spec}(k)$  is the structure morphism.

**Definition 1.3.** An abelian variety  $A$  defined over  $k$  is a  $k$ -group variety which is complete as a  $k$ -variety.

## 1.2 Commutativity

We begin by explaining the most basic fact, which is commutativity. The main ingredient in proving this is the following general fact:

**Lemma 1.4** (Rigidity Lemma). *Let  $X$  be a complete variety over  $k$ , and  $Y$  and  $Z$  be arbitrary varieties. Let  $f : X \times Y \rightarrow Z$  be a map of varieties. Suppose there exists  $x_0 \in X$  and  $y_0 \in Y$  such that the restrictions of  $f$  to  $X \times \{y_0\}$  and  $\{x_0\} \times Y$  are constant. Then  $f$  is constant.*

**Corollary 1.5.** *Let  $X$  and  $Y$  be abelian varieties and let  $f : X \rightarrow Y$  be any map of varieties such that  $f(0) = 0$ . Then  $f$  is a morphism of abelian varieties, i.e.,  $f$  respects the group structure.*

*Proof.* Consider the map

$$\begin{aligned} h : X \times X &\rightarrow Y \\ (x, y) &\mapsto f(x + y) - f(x) - f(y). \end{aligned}$$

Then  $h(x, 0) = h(0, x) = 0$  for all  $x \in X$ . So, by the Rigidity Lemma  $h = 0$ , meaning that  $f$  is a homomorphism.  $\square$

**Corollary 1.6.** *An abelian variety is commutative.*

*Proof.* The map  $x \mapsto -x$  takes 0 to 0 and is therefore a homomorphism, which implies commutativity.  $\square$

## 1.3 Theorem of the cube

**Theorem 1.7** (Theorem of the cube). *Let  $X, Y$  and  $Z$  be varieties such that  $X$  and  $Y$  are complete. Let  $x_0 \in X, y_0 \in Y$  and  $z_0 \in Z$  be points. Let  $\mathcal{L}$  be a line bundle on  $X \times Y \times Z$  such that the restrictions of  $\mathcal{L}$  to  $X \times Y \times \{z_0\}, X \times \{y_0\} \times Z$  and  $\{x_0\} \times Y \times Z$  are trivial. Then  $\mathcal{L}$  is trivial.*

**Corollary 1.8.** *Let  $A$  be an abelian variety. Let  $\pi_i : A \times A \times A \rightarrow A$  denote the projection map on the  $i$ -th factor, and set  $\pi_{ij} := \pi_i + \pi_j$  and  $\pi_{123} := \pi_1 + \pi_2 + \pi_3$ . Let  $\mathcal{L}$  be a line bundle on  $A$ . Then the line bundle*

$$\mathcal{L}' := \pi_{123}^* \mathcal{L} \otimes \pi_{12}^* \mathcal{L}^{-1} \otimes \pi_{13}^* \mathcal{L}^{-1} \otimes \pi_{23}^* \mathcal{L}^{-1} \otimes \pi_1^* \mathcal{L} \otimes \pi_2^* \mathcal{L} \otimes \pi_3^* \mathcal{L}$$

*on  $A \times A \times A$  is trivial.*

*Proof.* This follows immediately from the theorem of the cube. For example, if we restrict to  $A \times A \times \{0\}$  then  $\pi_{123}^* \mathcal{L} = \pi_{12}^* \mathcal{L}, \pi_{13}^* \mathcal{L} = \pi_1^* \mathcal{L}$ , and  $\pi_3^* \mathcal{L} = 1$ , so all factors cancel.  $\square$

**Corollary 1.9.** *Let  $A$  be an abelian variety, and  $X$  an arbitrary variety. Let  $f, g, h : X \rightarrow A$  be maps of varieties, and  $\mathcal{L}$  a line bundle on  $A$ . Then the line bundle*

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

*on  $X$  is trivial.*

*Proof.* This follows from Corollary 1.8 by considering the map  $X \rightarrow A \times A \times A$  given by  $(f, g, h)$ .  $\square$

### 1.4 Theorem of the square

**Theorem 1.10** (Theorem of the square). *Let  $A$  be an abelian variety and  $\mathcal{L}$  a line bundle on  $A$ , and  $x, y \in A(\bar{k})$ . Then  $t_{x+y}^* \mathcal{L} \otimes \mathcal{L} = t_x^* \mathcal{L} \otimes t_y^* \mathcal{L}$ . (Here  $t_x$  denotes translation by  $x$ .)*

*Proof.* Apply Corollary 1.9 with  $f = t_x$  (constant map),  $g = t_y$ , and  $h = id_A$ .  $\square$

Define  $\text{Pic}(A)$  to be the set of isomorphism classes of line bundles on  $A$ . For a line bundle  $\mathcal{L}$ , let  $\phi_{\mathcal{L}} : A(\bar{k}) \rightarrow \text{Pic}(A)$  be the map  $\phi_{\mathcal{L}}(x) = t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ . The theorem of the square states exactly that  $\phi_{\mathcal{L}}$  is a group homomorphism.

### 1.5 Isogenies

**Proposition 1.11.** *Let  $f : A \rightarrow B$  be a homomorphism of abelian varieties. Then the following conditions are equivalent:*

- (a)  *$f$  is surjective and  $\dim(A) = \dim(B)$ ;*
- (b)  *$\ker(f)$  is a finite group scheme and  $\dim(A) = \dim(B)$ ;*
- (c)  *$f$  is a finite, flat and surjective morphism.*

**Definition 1.12.** *Let  $f : A \rightarrow B$  be a homomorphism of abelian varieties. We say that  $f$  is an isogeny if it satisfies the three equivalent conditions (a), (b) and (c) in Proposition 1.11. The degree of an isogeny  $f$  is  $[k(A) : k(B)]$ , the degree of the function field extension  $k(A)/k(B)$ . (Note that we have a homomorphism  $k(B) \rightarrow k(A)$ , since an isogeny is surjective.)*

**Definition 1.13.** *Let  $f : A \rightarrow B$  be an isogeny. Then, we say that*

- (i)  *$f$  is separable if  $k(A)/k(B)$  is a separable extension.*
- (ii)  *$f$  is (purely) inseparable if  $k(A)/k(B)$  is a (purely) inseparable extension.*

**Proposition 1.14.** *Let  $f : A \rightarrow C$  be an isogeny. Then, there exist*

- (i) *an abelian variety  $B$ ;*
- (ii) *an inseparable isogeny  $g : A \rightarrow B$ ; and*
- (iii) *a separable isogeny  $h : B \rightarrow C$*

*such that  $f = h \circ g$ . This factorisation is unique up to isomorphism. In other words, if  $f = h' \circ g' : A \rightarrow B' \rightarrow C$  is a second such factorisation then there is an isomorphism  $\alpha : B \rightarrow B'$  such that  $g' = \alpha \circ g$  and  $h = h' \circ \alpha$ .*

### 1.6 Structure of torsion

For an integer  $n$ , let  $[n]_A$  (or simply  $[n]$ ) be the morphism

$$\begin{aligned} A(\bar{k}) &\rightarrow A(\bar{k}) \\ x &\mapsto nx. \end{aligned}$$

**Proposition 1.15.** *Let  $A$  be an abelian variety,  $\mathcal{L}$  a line bundle on  $A$ , and  $n \in \mathbb{Z}$ . Then, we have*

$$[n]^* \mathcal{L} = \mathcal{L}^{(n^2+n)/2} \otimes [-1]^* \mathcal{L}^{(n^2-n)/2}.$$

In particular,

(i) if  $\mathcal{L}$  is symmetric (i.e.  $[-1]^* \mathcal{L} = \mathcal{L}$ ) then  $[n]^* \mathcal{L} = \mathcal{L}^{n^2}$ ;

(ii) if  $\mathcal{L}$  is anti-symmetric (i.e.  $[-1]^* \mathcal{L} = \mathcal{L}^{-1}$ ) then  $[n]^* \mathcal{L} = \mathcal{L}^n$ .

*Proof.* Applying Corollary 1.9 to the maps  $[n]$ ,  $[1]$ , and  $[-1]$ , we see that

$$\mathcal{L}' := [n]^* \mathcal{L} \otimes [n+1]^* \mathcal{L}^{-1} \otimes [n-1]^* \mathcal{L}^{-1} \otimes [n]^* \mathcal{L} \otimes \mathcal{L} \otimes [-1]^* \mathcal{L}$$

is trivial. In other words, we have

$$[n+1]^* \mathcal{L} = [n]^* \mathcal{L}^2 \otimes [n-1]^* \mathcal{L}^{-1} \otimes \mathcal{L} \otimes [-1]^* \mathcal{L}.$$

The result now follows by induction.  $\square$

**Theorem 1.16.** *Let  $A$  be an abelian variety of dimension  $g$ , and  $n > 0$  an integer. Then  $[n]_A : A \rightarrow A$  is an isogeny; it is étale if and only if  $(\text{char}(k), n) = 1$ .*

*Proof.* One can show that abelian varieties are projective. Let  $\mathcal{L}$  be an ample line bundle on  $A$ . Replacing  $\mathcal{L}$  by  $\mathcal{L} \otimes [-1]^* \mathcal{L}$ , we can assume  $\mathcal{L}$  is symmetric. Since  $[n]^* \mathcal{L} = \mathcal{L}^{n^2}$ , it is ample. However, the restriction of this to the  $n$ -torsion is obviously trivial. Since the  $n$ -torsion is a complete variety on which the trivial bundle is ample, it must be finite. This implies that  $[n]$  is surjective, by reasoning with dimension.  $\square$

**Proposition 1.17.** *The degree of  $[n]_A$  is  $n^{2g}$ .*

*Proof.* Let  $f : X \rightarrow Y$  be a finite map of complete varieties of degree  $d$ . If  $D_1, \dots, D_n$  are divisors on  $Y$ , where  $n = \dim(X) = \dim(Y)$ , then there is an equality of intersection numbers:

$$(f^* D_1 \cdots f^* D_n) = d(D_1 \cdots D_n).$$

Now, let  $D$  be an ample divisor such that  $[-1]^* D$  is linearly equivalent to  $D$  (e.g., the divisor associated to the line bundle used above). Then  $[n]^* D$  is linearly equivalent to  $n^2 D$ . We thus find

$$\deg([n])(D \cdots D) = ((n^2 D) \cdots (n^2 D)) = n^{2g}(D \cdots D).$$

Since  $D$  is ample,  $(D \cdots D) \neq 0$ , and thus  $\deg([n]) = n^{2g}$ .  $\square$

One can show that  $[n] : A \rightarrow A$  induces multiplication by  $n$  on the tangent space. This shows that  $[n]$  is separable if and only if  $n$  is prime to the characteristic. Combined with the above (and the usual induction argument), we see that:

**Corollary 1.18.** *If  $(\text{char}(k), n) = 1$ , then  $A[n](\bar{k})$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^{2g}$ .*

Since  $[p]$  is not separable,  $A[p](\bar{k})$  must have fewer than  $p^{2g}$  points. We will see later, when studying group schemes, that it can have at most  $p^g$  points.

**Corollary 1.19.** *Let  $f : A \rightarrow B$  be an isogeny of degree  $n$ . Then there exists an isogeny  $g : B \rightarrow A$  such that  $g \circ f = [n]_A$  and  $f \circ g = [n]_B$ .*

## 2 The dual variety

### 2.1 Definition of the dual

Let  $k$  be an arbitrary field, and  $A$  an abelian variety defined over  $k$ . We define  $\text{Pic}(A)$  to be the set of isomorphism classes of line bundles on  $A$ . Then, we let  $\text{Pic}^0(A)$  be the subgroup consisting of those line bundles  $\mathcal{L}$  which are translation invariant, i.e., which satisfy  $t_x^*(\mathcal{L}) \simeq \mathcal{L}$  for all  $x \in A$ . We define the following functor. For each variety  $T$  over  $k$ , let  $F(T)$  be the set of isomorphism classes of line bundles  $\mathcal{L}$  on  $A \times T$  satisfying the following two conditions:

- (a) for all  $t \in T$ , the restriction of  $\mathcal{L}$  to  $A \times \{t\}$  belongs to  $\text{Pic}^0(A)$ ; and
- (b) the restriction of  $\mathcal{L}$  to  $\{0\} \times T$  is trivial.

We see that  $F(k) = \text{Pic}^0(A)$ . We define the *dual abelian variety*  $A^\vee$  to be the variety that represents  $F$ , if it exists. We will always assume that the dual variety  $A^\vee$  exists. Then, it automatically comes with a universal bundle  $\mathcal{P}$  on  $A \times A^\vee$ , which is called the *Poincaré bundle*.

### 2.2 Construction of the dual

Let  $\mathcal{L}$  be an ample bundle on  $A$ . We then have the map

$$\begin{aligned} \phi_{\mathcal{L}} : A &\rightarrow \text{Pic}^0(A) \\ x &\mapsto [t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}]. \end{aligned}$$

By the theorem of the square, the image is in  $\text{Pic}^0(A)$ . One can prove the map  $\phi_{\mathcal{L}}$  is surjective, and has finite kernel  $K(\mathcal{L})$ . In fact,  $K(\mathcal{L})$  has a natural structure of a group scheme. This suggests that  $A^\vee$  should be the quotient  $A/K(\mathcal{L})$ , and one can show that this is indeed the case.

**Proposition 2.1.** *Let  $f : A \rightarrow B$  be a homomorphism of abelian varieties over  $k$ , and  $\mathcal{P}_A$  and  $\mathcal{P}_B$  be the Poincaré line bundles on  $A$  and  $B$ , respectively. Then, there exists an induced homomorphism  $f^\vee : B^\vee \rightarrow A^\vee$ , called the dual or transpose of  $f$ . Thus,  $f^\vee$  is the unique homomorphism such that*

$$(id_A \times f^\vee)^* \mathcal{P}_A \simeq (f \times id_B)^* \mathcal{P}_B$$

*as line bundles on  $A \times B^\vee$  with rigidification along  $\{0\} \times B^\vee$ .*

### 2.3 Polarisations

**Definition 2.2.** *Let  $A$  be an abelian variety. A polarisation on  $A$  is an isogeny  $\lambda : A \rightarrow A^\vee$  such that  $\lambda_{\bar{k}} : A(\bar{k}) \rightarrow \text{Pic}^0(A)$  is given by  $\lambda_{\bar{k}} = \phi_{\mathcal{L}}$  for some ample line bundle  $\mathcal{L}$  on  $A$  over  $\bar{k}$ . The degree of the polarisation  $\lambda$  is its degree as an isogeny. An abelian variety together with a polarisation is called a polarised abelian variety.*

There is an obvious notion of morphisms of polarised abelian varieties. If  $\lambda$  has degree 1, then we say that  $(A, \lambda)$  is a *principally polarised* abelian variety.

### 3 Structure of the isogeny category

#### 3.1 Poincaré reducibility

**Theorem 3.1** (Poincaré reducibility). *Let  $A$  be an abelian variety, and let  $B$  be an abelian subvariety. Then there exists an abelian subvariety  $C$  such that  $B \cap C$  is finite and  $B \times C \rightarrow A$  is an isogeny.*

*Proof.* Choosing polarisations on  $A$  and  $A/B$  to identify them with their duals, the dual to the quotient map  $A \rightarrow A/B$  is a map  $A/B \rightarrow A$ . We let  $C$  be its image. The properties are easy to verify.  $\square$

We say that an abelian variety  $A$  is *simple* if the only abelian subvarieties of  $A$  are 0 and  $A$ .

*Proof.* Every abelian variety is isogenous to a product of simple varieties.  $\square$

#### 3.2 The isogeny category

Define a category **Isog** as follows. The objects are abelian varieties. For two abelian varieties  $A$  and  $B$ , we put

$$\mathrm{Hom}_{\mathbf{Isog}}(A, B) = \mathrm{Hom}(A, B) \otimes \mathbb{Q}.$$

One can show that if  $f : A \rightarrow B$  is an isogeny then there exists an isogeny  $g : B \rightarrow A$  such that  $gf = [n]$ , for some  $n$ ; it follows that  $\frac{1}{n}g$  is the inverse to  $f$  in **Isog**. Thus isogenies become isomorphisms in **Isog**.

It is not difficult to see that **Isog** is in fact an abelian category. The simple objects of this category are exactly the simple abelian varieties. Poincaré's theorem shows that **Isog** is semi-simple as an abelian category. From this formalism, and general facts about abelian varieties, we deduce two results:

1. The decomposition (up to isogeny) into a product of simple abelian varieties is unique (up to isogeny). (Reason: in any semi-simple abelian category, the decomposition into simples is unique up to isomorphism.)
2. If  $A$  is a simple abelian variety then  $\mathrm{End}(A) \otimes \mathbb{Q}$  is a division algebra over  $\mathbb{Q}$ . (Reason: if  $A$  is a simple object in an abelian category and  $\mathrm{End}(A)$  contains a field  $k$ , then it is a division algebra over  $k$ .)

### 4 Basic example: elliptic curves

We will assume throughout this section, that  $k$  is a field of characteristic different from 2.

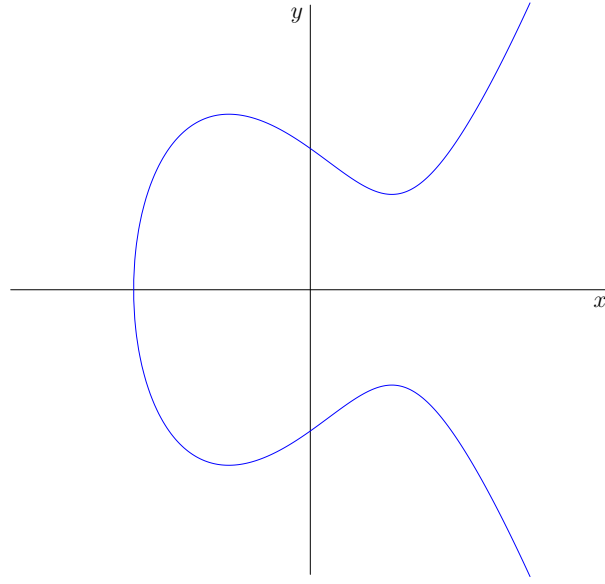
#### 4.1 Definition of an elliptic curve

**Definition 4.1.** *Let  $E : y^2 = f(x)$  be a cubic curve, where  $f(x) = x^3 + ax^2 + bx + c$ . Then, the discriminant  $\Delta_E$  of  $E$  is the discriminant  $\Delta_f$  of the polynomial  $f$ :*

$$\Delta_E := \Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

**Example 4.2.** For a cubic curve  $E : y^2 = x^3 + ax + b$ ,  $a, b \in k$ , the discriminant  $\Delta_E = -4a^3 - 27b^2$ .



Figure 1: Real points of the elliptic curve  $y^2 = x^3 - 8$ 

We can now give the definition of an elliptic curve.

**Definition 4.3.** Let  $k$  be a field with characteristic different from 2. An elliptic curve over  $k$  is a cubic curve  $E: y^2 = f(x) = x^3 + ax^2 + bx + c$ , with  $a, b, c \in k$ , such that  $\Delta_E \neq 0$ .

The following lemma expresses the discriminant of a cubic polynomial in terms of its roots.

**Lemma 4.4.** Let  $f(x) = x^3 + ax^2 + bx + c$ , with  $a, b, c \in k$ , and  $e_1, e_2, e_3$  the roots of  $f$  in  $\bar{k}$ . Then the discriminant of  $f$  is given by

$$\Delta_f = [(e_1 - e_2)(e_2 - e_3)(e_1 - e_3)]^2.$$

A useful criteria to check whether a cubic is an elliptic curve.

**Proposition 4.5.** Let  $E: y^2 = f(x)$  be a cubic curve, with  $f(x) = x^3 + ax^2 + bx + c$  and  $a, b, c \in k$ . Then, we have  $E$  is an elliptic curve  $\iff f$  has **no** repeated roots  $\iff \Delta_E \neq 0$ .

**Example 4.6.** (a) The cubic  $E: y^2 = x^3 - 2x + 1$  is an elliptic curve over  $\mathbb{Q}$  since  $\Delta_E = -4(-2)^3 - 27(1) = 5 \neq 0$ .

(b) For  $c \in \mathbb{Z}$  non-zero, the curve  $E: y^2 = x^3 + c$  is an elliptic curve over  $\mathbb{Q}$  since  $\Delta_E = -27c^2 \neq 0$ . (See Figure 1 for the real locus of this curve.)

(c) The curve  $E: y^2 = x^3 + x^2 + 1$  is an elliptic curve over  $\mathbb{F}_3$ . Definition 4.1 shows that  $\Delta_E = -1 \neq 0 \in \mathbb{F}_3$ . Alternatively, letting  $f(x) = x^3 + x^2 + 1$ , we see that  $f'(x) = 3x^2 + 2x = 2x$  ( $\text{char}(\mathbb{F}_3) = 3$ ). So  $\gcd(f, f') = 1$ , which implies that  $f$  has distinct roots.

## 4.2 Definition of the group law

The homogenisation of the curve  $E$  in Definition 4.3 is given by

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3. \quad (1)$$

The *only* point at infinity on  $E$  is  $[0 : 1 : 0]$ , which we denote by  $\infty$  from now on. We will see that this point is the *neutral* element in the group structure on  $E$ .

**Definition 4.7.** Let  $E$  be an elliptic curve over  $k$ , and  $k'$  a field containing  $k$ . The set of  $k'$ -rational points of  $E$  is the set of  $k'$ -rational points on the homogenisation of  $E$ , namely

$$E(k') := \{[x : y : z] \in \mathbf{P}^2(k') : zy^2 = x^3 + ax^2z + bxz^2 + cz^3\}.$$

Since  $\mathbf{P}^2(k') = \mathbf{A}^2(k') \sqcup \{Z = 0\}$ , and  $\infty = [0 : 1 : 0]$  is the unique point at infinity, we can write

$$E(k') := \{(x, y) \in K'^2 : y^2 = x^3 + ax^2 + bx + c\} \sqcup \{\infty\}.$$

**Example 4.8.** Let  $k = \mathbb{Q}$ , and  $E : y^2 = x^3 + 1$ . The set of  $\mathbb{Q}$ -rational points  $E(\mathbb{Q})$  is given by

$$E(\mathbb{Q}) = \{(-1, 0), (0, \pm 1), (2, \pm 3)\} \cup \{\infty\}.$$

We have the natural inclusions  $E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$ . (See Figure 3 for the sets  $E(\mathbb{Q}) \subset E(\mathbb{R})$ .)

**Example 4.9.** Let  $E : y^2 = x^3 + 2x + 5$  be the curve over  $\mathbb{F}_{11}$ . Then, we have

$$E(\mathbb{F}_{11}) = \{(0, \pm 4), (3, \pm 4), (4, 0), (-3, \pm 4), (-2, \pm 2)\} \cup \{\infty\}.$$

Let  $h \in k[x]$  be a polynomial of degree  $n$ . The number of roots of  $h$  counted with multiplicity in  $\bar{k}$  is  $n$ . The following theorem can be seen as a generalisation of that statement to elliptic curves.

**Theorem 4.10** (Bézout). Let  $k$  be a field,  $E : y^2 = x^3 + ax^2 + bx + c$  an elliptic curve over  $k$ , and  $L \subset \mathbf{P}^1(\bar{k})$  a line. The set  $L \cap E$  contains three points counted with multiplicity.

Let  $L : \alpha x + \beta y + \gamma = 0$  be a line, with  $\alpha, \beta, \gamma \in k$ . We want to find  $L \cap E \subset \mathbf{P}^1(\bar{k})$ , so we first homogenise  $L : \alpha X + \beta Y + \gamma Z = 0$ . Then we have two cases:

**Case 1:** The *unique* point infinity  $\infty = [0 : 1 : 0] \in L \cap E$ .

In that case, we see that  $\alpha x + \beta y + \gamma z = 0$  implies that  $\beta = 0$ . This means that either:

- (a)  $L$  is the line at infinity  $Z = 0$ . In that case  $P = \infty$  is the *only* point of intersection, hence has multiplicity *three*.
- (b)  $L$  is vertical line  $\alpha X + \gamma Z = 0$  ( $\alpha \neq 0$ ). The other points of intersection are  $(x_0, \pm y_0)$ , where  $x_0 = -\frac{\gamma}{\alpha}$  and  $y_0 = \sqrt{f(x_0)}$ . If  $y_0 = 0$ , then we get a unique point  $P = (x_0, 0)$  with multiplicity *two*; otherwise, we get two distinct points  $P = (x_0, y_0)$  and  $Q = (x_0, -y_0)$ , with multiplicity *one* each. In either case, the point  $\infty$  has multiplicity *one*.

**Case 2:**  $L \cap E$  consists of three *affine* points counted with multiplicity.

- (a)  $L \cap E$  has *two distinct* points  $P$  and  $Q$ : In this case,  $L$  is a tangent to  $E$  at  $P$  or  $Q$ . The tangent point has multiplicity *two*, and the other point has multiplicity *one*.

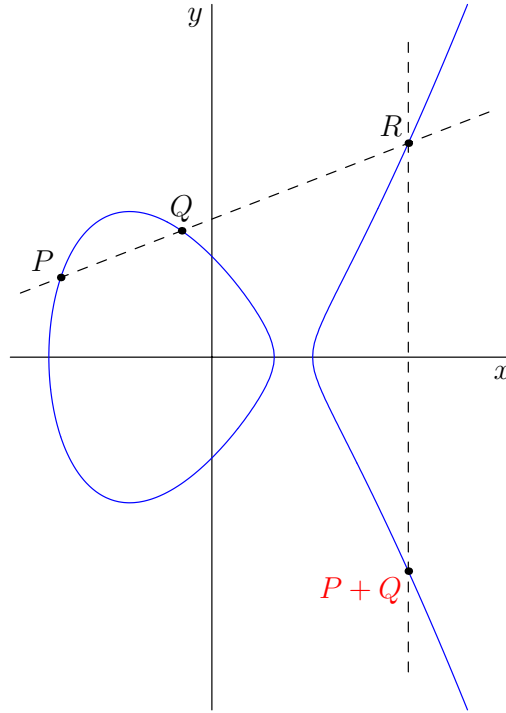


Figure 2: Group addition law

(b)  $L \cap E$  has three distinct points  $P$ ,  $Q$  and  $R$ . In that case, each point has multiplicity one.

We are now ready to define the group structure on  $E(\bar{k})$ .

**Definition 4.11.** Let  $E$  be an elliptic curve over  $k$ , and

$$E(\bar{k}) = \{(x, y) \in \bar{k}^2 : y^2 = x^3 + ax^2 + bx + c\} \sqcup \{\infty\}.$$

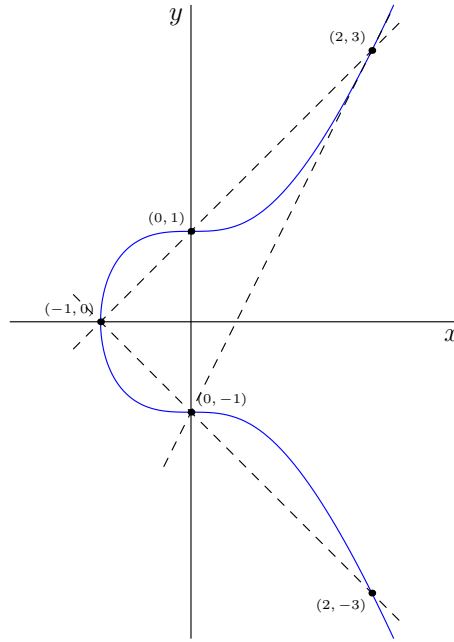
The addition law  $+$  on  $E(\bar{k})$  is defined as follows:

- (i) The neutral element is  $\infty$ ;
- (ii) If  $P, Q, R \in E(\bar{k})$  are collinear, then  $P + Q + R = \infty$  ( $\Leftrightarrow P + Q = -R$ ).

In words, to obtain the sum  $P + Q$ , we first draw the line  $L$  through  $P$  and  $Q$  (if  $P \neq Q$ ) or the tangent line (if  $P = Q$ ), and let  $R$  be its third intersection point with  $E(\bar{k})$ . If  $R = (x_R, y_R)$  is affine, then  $P + Q = -R = (x_R, -y_R)$ ; otherwise,  $P + Q = \infty$ . (See Figure 2.)

**Remark 4.12.** By Definition 4.11 and the discussion preceding it, if  $P = (x, y)$  is affine, then the negative of  $P$  is  $-P = (x, -y)$  since  $(x, y)$  and  $(x, -y)$  are on a vertical line, which intersects  $E$  at  $\infty$ .

**Example 4.13.** Let  $E : y^2 = x^3 + 1$  over  $\mathbb{Q}$  be the curve in Example 4.8. Let  $P = (-1, 0)$  and  $Q = (0, 1)$ . The equation of the line through  $P$  and  $Q$  is  $y = x + 1$ . So, we see that the point  $R = (2, 3)$ . The line through  $R$  and  $\infty$  is the vertical line  $x = 2$ . It intersects  $E$  at  $(2, -3)$ , so  $P + Q = (2, -3)$  (see Figure 3). Similarly, one can compute the sum of any two points in  $E(\mathbb{Q})$ .

Figure 3: Euler cubic:  $y^2 = x^3 + 1$ 

The theorem below says that Definition 4.11 makes  $E(\bar{k})$  into an abelian group.

**Theorem 4.14.** *Let  $E$  be an elliptic curve defined over a field  $K$ . Then,  $E(\bar{k})$  is an abelian group under the operation  $+$ , with identity element  $\infty (= [0 : 1 : 0])$ . In other words, we have*

- (i)  $P + Q = Q + P \quad \forall P, Q \in E(\bar{k})$  (commutativity).
- (ii)  $P + \infty = P \quad \forall P \in E(\bar{k})$  (identity element).
- (iii) If  $P = (x, y)$ , then  $-P = (x, -y)$  (opposite element).
- (iv)  $P + (Q + R) = (P + Q) + R, \quad \forall P, Q, R \in E(\bar{k})$  (associativity).

*Proof.* Properties (i)-(iii) follow easily from Definition 4.11 and the discussion preceding it. However, the last statement (iv) is very hard to prove, and beyond the scope of this course.  $\square$

### 4.3 Computing with the group law

We now give a more explicit description of the group law on  $E(\bar{k})$ .

**Proposition 4.15.** *Let  $E$  be as above, and  $P_1, P_2 \in E(\bar{k})$ . Then  $P_1 + P_2$  is given by*

- (1) *If  $P_1 = \infty$  then  $P_1 + P_2 = P_2$ ; if  $P_2 = \infty$ , then  $P_1 + P_2 = P_1$ .*

*Assume that  $P_1, P_2 \neq \infty$ , so that  $P_i = (x_i, y_i)$ ,  $i = 1, 2$ ; then*

- (2) *If  $x_1 = x_2$  and  $y_1 = -y_2$  then  $P_1 + P_2 = \infty$ .*

(3) Set

$$\lambda := \begin{cases} \frac{3x_1^2 + 2ax_1 + b}{2y_1}, & \text{if } x_1 = x_2 \text{ and } y_1 = y_2 \neq 0; \\ \frac{y_1 - y_2}{x_1 - x_2}, & \text{else.} \end{cases}$$

Let  $x_3 = \lambda^2 - a - x_1 - x_2$ ,  $y_3 = y_1 + \lambda(x_3 - x_1)$  and  $P_3 = (x_3, -y_3)$ , then  $P_1 + P_2 = P_3$ .

*Proof.* We note that (1) and (2) are just a restatement of Theorem 4.14 (ii) and (iii). So we only need to prove (3). In that case, let  $L : y = \lambda x + \nu$  be the line through  $P_1$ ,  $P_2$ , and  $R = (x_3, y_3)$  its 3rd point of intersection with  $E$ . If  $P_1 = P_2$ , then  $L$  is the tangent line at  $P_1$  with  $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$  and  $\nu = y_1 - \lambda x_1$ . Otherwise,  $L$  is the line with slope  $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$  and  $x$ -intercept  $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$ . The  $x$ -coordinates  $x_1, x_2$  and  $x_3$  of the points in  $L \cap E$  (counted with multiplicity) satisfy the equation

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

By moving all terms to the same side, expanding and then factorising, we get

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + c - \nu^2 = (x - x_1)(x - x_2)(x - x_3) = 0.$$

By equating the terms of degree 2, we get  $x_1 + x_2 + x_3 = -(a - \lambda^2)$ . From this, we recover  $R = (x_3, y_3)$ , which gives  $P_1 + P_2 = P_3 = (x_3, -y_3)$ .  $\square$

**Remark 4.16.** From proof above, we note that if  $x_i \in k$ , then  $y_i = \lambda x_i + \nu \in k$  and the intersection point  $(x_i, y_i)$  is defined over  $k$ . We also note that, if two of the roots  $x_1, x_2, x_3$  are defined over  $k$ , then so is the third one since  $x_1 + x_2 + x_3 = -(a - \lambda^2) \in k$ .

**Example 4.17.** Let  $E : y^2 = x^3 + 73$ , and  $P = (2, 9)$ ,  $Q = (3, 10)$ .

(a) The slope of the line through  $P$  and  $Q$  is  $\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{10 - 9}{3 - 2} = 1$ . Let  $R = (x_R, y_R)$  be the 3rd point of intersection of this line with  $E$ . Then, we have  $x_P + x_Q + x_R = \lambda^2$ . So  $x_R = (1)^2 - 2 - 3 = -4$ , and  $y_R = y_P + \lambda(x_R - x_P) = 9 + (-4 - 2) = 3$ . Hence  $P + Q = -R = (-4, -3)$ .

(b) The slope of the tangent line at  $P$  is  $\lambda = \frac{3x_P^2}{2y_P} = \frac{3(2)^2}{2(9)} = \frac{2}{3}$ . For the 3rd point of intersection  $R = (x_R, y_R)$ , we have  $2x_P + x_R = \lambda^2$ . So  $x_R = (\frac{2}{3})^2 - 2(2) = -\frac{32}{9}$ , and  $y_R = y_P + \lambda(x_R - x_P) = 9 + \frac{2}{3}(-\frac{32}{9} - 2) = \frac{143}{27}$ . Hence  $2P = -R = -(x_R, y_R) = (x_R, -y_R) = (-\frac{32}{9}, -\frac{143}{27})$ .

**Example 4.18.** Let  $E : y^2 = x^3 + 2x + 5$  be the curve defined  $\mathbb{F}_{11}$  in Example 4.9, and  $P = (-3, 4)$ . We compute  $2P$  using Proposition 4.15. We have  $\lambda = \frac{3x_P^2 + 2}{2y_P} = \frac{3(-3)^2 + 2}{2(4)} = 5 \pmod{11}$ . So, we have  $x_{2P} = \lambda^2 - 2x_P = (5^2) - 2(-3) = 25 + 6 = -2 \pmod{11}$ . So, we get that  $-y_{2P} = y_P + \lambda(x_{2P} - x_P) = 4 + 5(-2 - (-3)) = -2 \pmod{11}$ . This gives  $y_{2P} = 2$  and  $2P = (-2, 2)$ . If we compute  $4P$ , we obtain  $4P = 2(2P) = 2(-2, 2) = (-3, -4) = -P$ .

This means that  $5P = (4 + 1)P = \infty$ . Since  $P \neq \infty$ , we see that  $P$  is a point of order 5. Now, let us observe that  $Q = (4, 0) \in E(\mathbb{F}_{11})$  is a point of order 2 since  $y_Q = 0$ , hence  $Q = -Q$ . (Observe that, if  $Q = (x, y) \in E(K)$  then  $-Q = (x, -y)$ .) This means that  $P + Q$  is a point of order 10. Since  $\#E(\mathbb{F}_{11}) = 10$ , we deduce from these computations that  $E(\mathbb{F}_{11})$  is a cyclic group of order 10.

**Corollary 4.19.** *If  $k \subseteq k' \subseteq \bar{k}$  is a subfield, then  $E(k')$  is a subgroup of  $E(\bar{k})$ .*

*Proof.* By definition, the identity element  $\infty \in E(k')$ ; also  $P = (x, y) \in E(k')$  implies that  $-P = (x, -y) \in E(k')$ . So we only need to show that

$$P, Q \in E(k') \Rightarrow P + Q \in E(k').$$

But this follows from Proposition 4.15 and Remark 4.16.  $\square$

## 5 Endomorphism rings and Tate modules

### 5.1 Endomorphism ring of an abelian variety

Let  $A$  and  $B$  be abelian varieties over a field  $k$ . If  $f$  and  $g$  are homomorphisms from  $A$  to  $A$ , then we have a homomorphism  $(f + g) : A \rightarrow A$  given on points by addition  $x \mapsto f(x) + g(x)$ . This gives the set  $\text{Hom}(A, B)$  of homomorphisms  $A \rightarrow B$  the structure of an abelian group. For  $A = B$  we see that  $\text{End}(A)$  has a natural ring structure, with composition of endomorphisms as the ring multiplication. We will always write  $\text{Hom}(A, B)$  for the group of homomorphisms from  $A$  to  $B$ , and  $\text{End}(A)$  for the ring of endomorphisms of  $A$ . We will use the notations  $\text{Hom}_k(A, B)$  and  $\text{End}_k(X)$  for the homomorphisms (resp. endomorphisms defined over  $k$ ).

**Lemma 5.1.** *Let  $A$  and  $B$  be abelian varieties over a field  $k$ . Then the group  $\text{Hom}(A, B)$  is torsion-free, i.e. for  $f \in \text{Hom}(A, B)$  and  $n \in \mathbb{Z}$  non-zero,  $n \cdot f = 0$  implies that  $f = 0$ .*

*Proof.* For  $n \in \mathbb{Z}$  and  $f \in \text{Hom}(A, B)$ , we have  $n \cdot f = f \circ [n]_A = [n]_B \circ f$ . But for  $n \neq 0$ , we know that  $[n]_A$  is an isogeny, so is in particular surjective. From this, we see that  $n \cdot f = 0$  implies that  $f = 0$ .  $\square$

We write

$$\text{Hom}^0(A, B) := \text{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q} \text{ and } \text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

By definition, we see that  $\text{End}^0(A)$  is a  $\mathbb{Q}$ -algebra.

**Theorem 5.2** (Poincaré reducibility). *Let  $A$  be an abelian variety, and let  $B$  be an abelian subvariety. Then there exists an abelian subvariety  $C$  such that  $B \cap C$  is finite and  $B \times C \rightarrow A$  is an isogeny.*

*Proof.* Let  $i : B \hookrightarrow A$  be the inclusion map and  $i^\vee : A^\vee \rightarrow B^\vee$  its dual. Let  $\lambda : A \rightarrow A^\vee$  be a polarisation on  $A$ . Then, let

$$X = \ker(i^\vee \circ \lambda),$$

$C$  the reduced subscheme of the zero component  $X$ . Then  $C$  is an abelian variety. From the theorem on the dimension of fibres of morphisms,  $\dim C \geq \dim A - \dim B$ . The restriction of the morphism  $i^\vee \circ \lambda : A \rightarrow B^\vee$  to  $B$  is  $\lambda|_B : B \rightarrow B^\vee$ , whose kernel is finite since  $\lambda$  arises from an ample bundle  $\mathcal{L}$ . Therefore  $B \cap C$  is finite, and so  $B \times C \rightarrow A$  is an isogeny.  $\square$

**Definition 5.3.** *Let  $A$  be a non-zero abelian variety  $X$  over a field  $k$ . We say that  $A$  is simple if  $A$  the only subvarieties of  $A$  are  $0$  and  $A$ .*

Note that an abelian variety that is simple over the ground field  $k$  need not be simple over an extension of  $k$ . To avoid confusion we sometimes use the terminology *k-simple*.

**Proposition 5.4.** *Let  $A$  be a non-zero abelian variety over  $k$ . Then,  $A$  is isogenous to a product of  $k$ -simple abelian varieties. More precisely, there exists  $k$ -simple abelian varieties  $B_1, \dots, B_r$ , which are pairwise non  $k$ -isogenous, and positive integers  $n_1, \dots, n_r$  such that  $A$  is  $k$ -isogenous to  $B_1^{n_1} \times \dots \times B_r^{n_r}$ , which we denote by  $A \sim_k B_1^{n_1} \times \dots \times B_r^{n_r}$ . Up to permutation, the abelian varieties  $B_i$  are unique up to  $k$ -isogeny, and the corresponding multiplicities  $n_i$  are uniquely determined.*

*Proof.* The existence of a decomposition is immediate from the Poincaré Splitting Theorem. The uniqueness statement is an easy exercise—note that a homomorphism between two simple abelian varieties is either zero or an isogeny.  $\square$

**Corollary 5.5.** *Let  $A$  be an abelian variety defined over  $k$ .*

- (i) *if  $A$  is  $k$ -simple, then  $\text{End}_k^0(A)$  is a division algebra;*
- (ii) *If  $A \sim_k B_1^{n_1} \times \dots \times B_r^{n_r}$ , where the  $B_i$  are  $k$ -simple abelian varieties, then we have*

$$\text{End}_k^0(A) = M_{n_1}(D_1) \times \dots \times M_{n_r}(D_r),$$

*where  $D_i = \text{End}_k^0(B_i)$ .*

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

*Proof.* First we observe that a homomorphism between two  $k$ -simple abelian varieties is either zero or an isogeny. But the isogenies from  $A$  to itself are invertible elements of  $\text{End}_k^0(A)$ . So if  $A$  is  $k$ -simple  $\text{End}_k^0(A)$  is a division algebra. For the second part of the statement, note that  $\text{Hom}(B_i, B_j) = 0$  if  $i \neq j$  since  $B_i$  and  $B_j$  are simple and non-isogenous.  $\square$

## 5.2 The Tate module of an abelian variety

Let  $A/k$  be an abelian variety of dimension  $g$  and let  $n$  be an integer such that  $(\text{char } k, n) = 1$ . From Proposition 1.17, we know that  $[n]$  is a separable map of degree  $n^{2g}$ . Furthermore, all fibers of the map  $[n] : A(\bar{k}) \rightarrow A(\bar{k})$  have cardinality  $n^{2g}$ ; in other words,  $A[n](\bar{k})$  has cardinality  $n^{2g}$ , where  $A[n] = \ker[n]$ . By Corollary 1.18 we have an isomorphism

$$A[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$$

of abelian groups (hence of  $\mathbb{Z}/n\mathbb{Z}$ -modules).

Let  $\ell$  be a prime number different from the  $\text{char } k$ . The  $\ell$ -adic Tate module of  $A$ , denoted  $T_\ell(A)$ , is defined by

$$T_\ell(A) := \varprojlim A[\ell^n],$$

the inverse limit of the groups  $A[n](\bar{k})$ , where the transition maps are multiplication by  $\ell$ . Explicitly, an element of  $T_\ell(A)$  is a sequence  $(x_0, x_1, \dots)$  of  $\bar{k}$ -points of  $A$ , where  $x_0 = 0$  and  $\ell x_i = x_{i-1}$  for  $i > 0$ . The results of the previous paragraph imply that we have an isomorphism

$$T_\ell(A) \simeq \mathbb{Z}_\ell^{2g}.$$

An extremely important property of the Tate module is that it comes equipped with a Galois action. If  $k$  is not algebraically closed then the  $n$ -torsion of  $A$  will typically not be defined over  $k$ , and so the absolute Galois group  $G_k = \text{Gal}(\bar{k}/k)$  will move the  $n$ -torsion points around.

This carries through the inverse limit, and so there is an action of  $G_k$  on  $T_\ell(A)$ . Picking a basis for  $T_\ell(A)$ , this action can be thought of as a homomorphism  $\rho : G_k \rightarrow \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ , i.e., an  $\ell$ -adic representation of the Galois group. This perspective has proved to be very useful.

Let  $f : A \rightarrow B$  be a homomorphism of abelian varieties defined over  $k$ . Then,  $f$  induces a  $\mathbb{Z}_\ell$ -linear and  $\mathrm{Gal}(\bar{k}/k)$ -equivariant map

$$T_\ell f : T_\ell A \rightarrow T_\ell B.$$

For  $x = (0, x_1, x_2, \dots) \in T_\ell A$ , we have

$$(T_\ell f)(x) := (0, f(x_1), f(x_2), \dots).$$

**Lemma 5.6.** *Let  $A$  and  $B$  be abelian varieties over a field  $k$ , and  $f \in \mathrm{Hom}(A, B)$ . Let  $\ell$  be a prime number such that  $\ell \neq \mathrm{char}(k)$ . If  $T_\ell(f)$  is divisible by  $\ell^m$  in  $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$  then  $f$  is divisible by  $\ell^m$  in  $\mathrm{Hom}(A, B)$ .*

*Proof.* If  $T_\ell(f)$  is divisible by  $\ell^m$ , then  $f$  vanishes on  $A[\ell^m](\bar{k})$ . But  $A[\ell^m]$  is an étale group scheme since  $\ell \neq \mathrm{char}(k)$ . Hence  $f$  is zero on  $A[\ell^m]$ . This means that  $A[\ell^m] \subseteq \ker f$  and  $f$  factors through  $[\ell^m]_A$ .  $\square$

**Theorem 5.7.** *Let  $A$  and  $B$  be abelian varieties over a field  $k$ . Let  $\ell$  be a prime number such that  $\ell \neq \mathrm{char}(k)$ . Then the  $\mathbb{Z}_\ell$ -linear map*

$$\begin{aligned} T_\ell : \mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell &\rightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B), \\ f \otimes c &\mapsto c \cdot T_\ell(f) \end{aligned}$$

*is injective and has a torsion-free cokernel.*

*Proof.*  $\square$

### 5.3 The Tate module of the multiplicative group

The multiplicative group, denoted  $G_m$  is the algebraic group which represents the functor  $R \rightarrow R^\times$  (where  $R$  is a  $k$ -algebra). As a scheme, it is simply  $\mathbf{A}^1 \setminus \{0\}$ , i.e.,  $\mathrm{Spec}(k[t, t^{-1}])$ .

The construction of the Tate module in the previous section can be applied equally well to  $G_m$ . If  $n$  is prime to  $\mathrm{char} k$  then the  $n$ -torsion  $G_m[n]$  is just the group of  $n$ -th roots of unity; its  $\bar{k}$ -points is isomorphic to  $\mathbb{Z}/n\mathbb{Z}$ . It follows that  $T_\ell(G_m)$  is isomorphic to  $\mathbb{Z}_\ell$  as a group. Of course, it also carries a Galois action, which can be recorded as a homomorphism  $\chi : G_k \rightarrow \mathrm{GL}_1(\mathbb{Z}_\ell) = \mathbb{Z}_\ell^\times$ . This homomorphism is called the *cyclotomic character*, and describes how the Galois group acts on roots of unity. A common notation, which we will use, is to write  $\mathbb{Z}_\ell(1)$  for  $T_\ell(G_m)$ . The idea is that the underlying group is  $\mathbb{Z}_\ell$  and the (1) records that the Galois group is acting through the first power of the cyclotomic character.

### 5.4 The Weil pairings

**Proposition 5.8.** *Let  $A/k$  be an abelian variety and  $n > 0$  an integer such that  $(n, \mathrm{char} k) = 1$ . Then there exists a pairing*

$$e_n : A[n] \times A^\vee[n] \rightarrow \mu_n$$

*satisfying the following:*



1. *Bilinear:*  $e_n(x + y, z) = e_n(x, z)e_n(y, z)$ .
2. *Alternating:*  $e_n(x, x) = 1$ . This implies  $e_n(x, y) = e_n(y, x)^{-1}$ , but is stronger if  $n$  is even.
3. *Non-degenerate:* if  $e_n(x, y) = 1$  for all  $y \in A^\vee[n]$  then  $x = 0$ .
4. *Galois equivariant:*  $e_n(\sigma x, \sigma y) = \sigma e_n(x, y)$  for  $\sigma \in G_k$ .
5. *Compatibility:* if  $x \in A[nm]$  and  $y \in A^\vee[n]$  then  $e_{nm}(x, y) = e_n(mx, y)$ .

(Note: the group law on  $A[n]$  is typically written additively, while the one on  $\mu_n$  is written multiplicatively.)

Let  $\lambda : A \rightarrow A^\vee$  be a polarisation on  $A$ . Then, we obtain the pairing

$$e_n^\lambda : A[n] \times A[n] \rightarrow \mu_n$$

$$(x, y) \mapsto e_n(x, \lambda(y)).$$

We call  $e_n$  and  $e_n^\lambda$  *Weil pairings*. The Weil pairings have the following important compatibility property.

**Proposition 5.9.** *Let  $A/k$  be a polarised abelian variety, with polarisation  $\lambda : A \rightarrow A^\vee$  and  $n > 0$  an integer such that  $(n, \text{char } k) = 1$ . The pairing*

$$e_n^\lambda : A[n] \times A[n] \rightarrow \mu_n$$

*satisfies the following properties:*

1. *Bilinear:*  $e_n^\lambda(x + y, z) = e_n^\lambda(x, z)e_n^\lambda(y, z)$ .
2. *Non-degenerate:* if  $e_n^\lambda(x, y) = 1$  for all  $y \in A[n]$  then  $x = 0$ .
3. *Galois equivariant:*  $e_n^\lambda(\sigma x, \sigma y) = \sigma e_n^\lambda(x, y)$  for  $\sigma \in G_k$ .
4. *Compatibility:* if  $x \in A[nm]$  and  $y \in A[n]$  then  $e_{nm}^\lambda(x, y) = e_n^\lambda(mx, y)$ .

(Note: the group law on  $A[n]$  is typically written additively, while the one on  $\mu_n$  is written multiplicatively.)

**Proposition 5.10.** *Let  $f : A \rightarrow B$  be an isogeny of polarised abelian varieties, where  $\lambda_A$  and  $\lambda_B$  are the polarisations on  $A$  and  $B$ , respectively. Then, we have*

$$e_n^{\lambda_A}(f(x), y) = e_n^{\lambda_B}(x, f^\vee(y)), \text{ for all } x \in A[n], y \in B[n].$$

The compatibility condition allows us to take the inverse limit of the  $e_{\ell^n}^\lambda$  to obtain a pairing on the Tate module

$$e^\lambda : T_\ell(A) \times T_\ell(A) \rightarrow \mathbb{Z}_\ell(1).$$

The pairing  $e^\lambda$  satisfies the same properties as in Proposition 5.8.