

# Abelian varieties over finite fields: Honda–Tate’s Theorem

Lassina Dembélé

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

King’s College London

Preliminary Arizona Winter School 2024

Version: November 3, 2023

## Contents

<b>1</b>	<b>Definition and properties of abelian varieties</b>	<b>4</b>
1.1	Definition	4
1.2	Commutativity	5
1.3	Theorem of the cube	5
1.4	Theorem of the square	6
1.5	Isogenies	6
1.6	Structure of torsion	6
<b>2</b>	<b>The dual variety</b>	<b>8</b>
2.1	Definition of the dual	8
2.2	Construction of the dual	8
2.3	Polarisations	8
<b>3</b>	<b>Structure of the isogeny category</b>	<b>9</b>
3.1	Poincaré reducibility	9
3.2	The isogeny category	9
<b>4</b>	<b>Basic example: elliptic curves</b>	<b>9</b>
4.1	Definition of an elliptic curve	9
4.2	Definition of the group law	11
4.3	Computing with the group law	13
<b>5</b>	<b>Endomorphism rings and Tate modules</b>	<b>15</b>
5.1	Endomorphism ring of an abelian variety	15
5.2	The Tate module of an abelian variety	17
5.3	The Tate module of the multiplicative group	18
5.4	The Weil pairings	18
<b>6</b>	<b>Tate's theorem</b>	<b>19</b>
6.1	Frobenius endomorphism	19
6.2	Tate's theorem	20
<b>7</b>	<b>Weil's conjectures</b>	<b>22</b>
7.1	Endomorphism rings of abelian varieties: Albert classification	22
7.2	Zeta functions of abelian varieties	23
<b>8</b>	<b>Jacobian varieties</b>	<b>25</b>
8.1	The functor	25
8.2	Obstruction to representability	26
8.3	The case when a rational point exists	27
8.4	Construction of the Jacobian	28
8.5	Basic properties	28
<b>9</b>	<b>Zeta functions of curves</b>	<b>29</b>
9.1	Hasse–Weil–Serre theorem	29
9.2	Examples: curves of genus $\leq 3$	30

<b>10 Dieudonné modules and <math>p</math>-divisible groups</b>	<b>31</b>
10.1 $p$ -divisible groups	31
10.2 Dieudonné modules	32
10.2.1 Commutative group schemes of $p$ -power order	32
10.3 Some basic examples	34
10.3.1 Group schemes of order $p$	34
10.3.2 A group scheme of order $p^2$	35
10.4 Dieudonné modules associated to abelian varieties	35
10.5 Local invariants associated to abelian varieties	39
<b>11 Honda–Tate’s theorem</b>	<b>40</b>
11.1 Statement of main result	40
11.2 Examples	40
11.2.1 The totally real case	41
11.2.2 Totally imaginary case	41
11.3 Proof of Theorem 11.2: Existence	42
<b>A Weil restriction of an abelian variety</b>	<b>43</b>
<b>B CM lifting of abelian varieties</b>	<b>44</b>
<b>C Background on non-commutative algebra</b>	<b>46</b>
C.1 Semi-simple modules	46
C.2 Brauer group	48
C.3 Local invariants of division algebras	52

# 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:

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

(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:

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

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  $Y$  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  $n \in \mathbf{Z}$ . 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  $(\mathbf{Z}/n\mathbf{Z})^{2g}$ .*

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 Polarisation

**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

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

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  $\mathrm{End}(A) \otimes \mathbf{Q}$  is a division algebra over  $\mathbf{Q}$ . (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

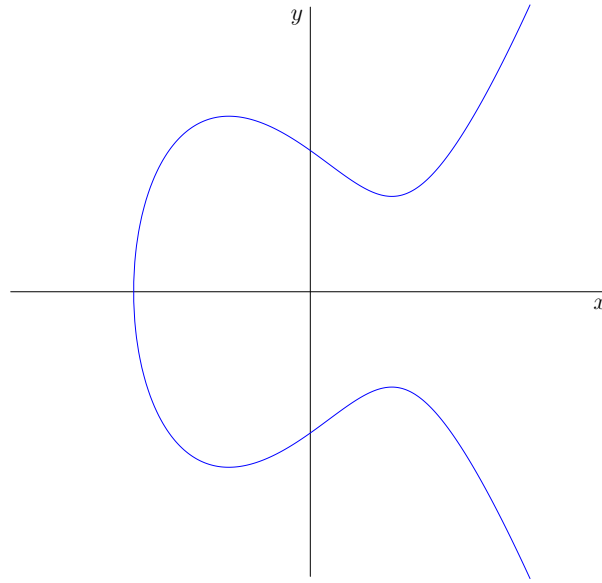
We will assume throughout this section, that  $k$  is a field of characteristic different from 2.

### 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  $\mathbf{Q}$  since  $\Delta_E = -4(-2)^3 - 27(1) = 5 \neq 0$ .

(b) For  $c \in \mathbf{Z}$  non-zero, the curve  $E: y^2 = x^3 + c$  is an elliptic curve over  $\mathbf{Q}$  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  $\mathbf{F}_3$ . Definition 4.1 shows that  $\Delta_E = -1 \neq 0 \in \mathbf{F}_3$ . Alternatively, letting  $f(x) = x^3 + x^2 + 1$ , we see that  $f'(x) = 3x^2 + 2x = 2x$  ( $\text{char}(\mathbf{F}_3) = 3$ ). So  $\text{gcd}(f, f') = 1$ , 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  $k = \mathbf{Q}$ , and  $E : y^2 = x^3 + 1$ . The set of  $\mathbf{Q}$ -rational points  $E(\mathbf{Q})$  is given by

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

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

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

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

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*.

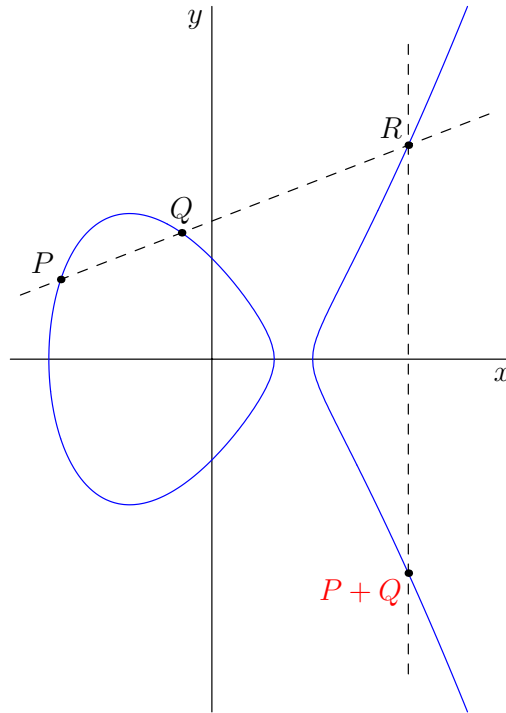


Figure 2: Group addition law

(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

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

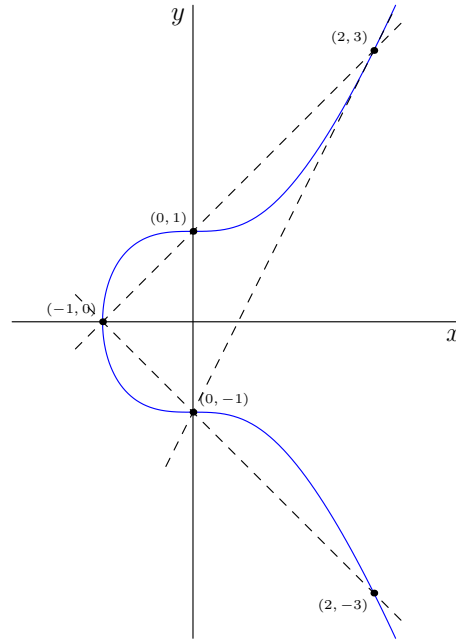
The addition law  $+$  on  $E(\bar{k})$  is defined as follows:

- (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  $\mathbf{Q}$  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  $E(\mathbf{Q})$ .

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  $\mathbf{F}_{11}$  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  $Q = (4, 0) \in E(\mathbf{F}_{11})$  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  $\#E(\mathbf{F}_{11}) = 10$ , we deduce from these computations that  $E(\mathbf{F}_{11})$  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  $(f + g) : A \rightarrow B$  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  $n \in \mathbf{Z}$  non-zero,  $n \cdot f = 0$  implies that  $f = 0$ .*

*Proof.* For  $n \in \mathbf{Z}$  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

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

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

**Example 5.6.** Here is an example of an abelian variety that is  $\mathbf{Q}$ -simple but not simple over  $F := \mathbf{Q}(\sqrt{29})$ . See Section 8 for the definition of Jacobian varieties. Let  $B$  be the Jacobian of the curve defined by

$$C : y^2 + (x^3 + 1)y = x^5 - 3x^4 - x^3 + 2x^2 - 2x - 2.$$

Then,  $B/\mathbf{Q}$  is a  $\mathbf{Q}$ -simple abelian surface such that  $\text{End}_{\mathbf{Q}}^0(B) = \mathbf{Q}(\sqrt{-5})$ . With a bit of analysis, one can show that the base change of  $B$  to  $F = \mathbf{Q}(\sqrt{29})$  is not  $F$ -simple. Namely, consider the elliptic curve

$$E : y^2 + xy + \epsilon^2 y = x^3,$$

where  $\epsilon = \frac{5+\sqrt{29}}{2}$  is the fundamental unit in  $F = \mathbf{Q}(\sqrt{29})$ ; it has discriminant  $\Delta_C = -\epsilon^{10}$ . So  $E$  is a curve that has everywhere good reduction. One can show that  $B$  admits the following decomposition over  $F$ :

$$B \times_{\mathbf{Q}} F \sim_F E \times E.$$

This example is one of my all time favourite!



## 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

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

of abelian groups (hence of  $\mathbf{Z}/n\mathbf{Z}$ -mdoules).

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

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

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  $\rho : G_k \rightarrow \text{GL}_{2g}(\mathbf{Z}_\ell)$ , 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  $\mathbf{Z}_\ell$ -linear and  $\text{Gal}(\bar{k}/k)$ -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 5.7.** *Let  $A$  and  $B$  be abelian varieties over a field  $k$ , and  $f \in \text{Hom}(A, B)$ . Let  $\ell$  be a prime number such that  $\ell \neq \text{char}(k)$ . If  $T_\ell(f)$  is divisible by  $\ell^m$  in  $\text{Hom}_{\mathbf{Z}_\ell}(T_\ell A, T_\ell B)$  then  $f$  is divisible by  $\ell^m$  in  $\text{Hom}(A, B)$ .*

*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  $\ell \neq \text{char}(k)$ . 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 5.8.** *Let  $A$  and  $B$  be abelian varieties over a field  $k$ . Let  $\ell$  be a prime number such that  $\ell \neq \text{char}(k)$ . Then the  $\mathbf{Z}_\ell$ -linear map*

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

*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.,  $\text{Spec}(k[t, t^{-1}])$ .

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

### 5.4 The Weil pairings

**Proposition 5.9.** *Let  $A/k$  be an abelian variety and  $n > 0$  an integer such that  $(n, \text{char} k) = 1$ . 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. *Non-degenerate:* if  $e_n(x, y) = 1$  for all  $y \in A^\vee[n]$  then  $x = 0$ .
3. *Galois equivariant:*  $e_n(\sigma x, \sigma y) = \sigma e_n(x, y)$  for  $\sigma \in G_k$ .
4. *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 5.10.** *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. *Alternating:*  $e_n^\lambda(x, x) = 1$ . This implies  $e_n^\lambda(x, y) = e_n^\lambda(y, x)^{-1}$ , but is stronger if  $n$  is even.
3. *Non-degenerate:* if  $e_n^\lambda(x, y) = 1$  for all  $y \in A[n]$  then  $x = 0$ .

4. *Galois equivariant:*  $e_n^\lambda(\sigma x, \sigma y) = \sigma e_n^\lambda(x, y)$  for  $\sigma \in G_k$ .

5. *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 5.11.** *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

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

The pairing  $e^\lambda$  satisfies the same properties as in Proposition 5.9.

**Proposition 5.12.** *Let  $A$  be an abelian variety over  $k$ . The degree map*

$$\begin{aligned} \text{End}^0(A) &\rightarrow \mathbf{Q} \\ c \otimes \phi &\mapsto c \deg(\phi) \end{aligned}$$

is a homogeneous polynomial function of degree  $2g$  on  $\text{End}^0(A)$ , i.e.

$$\deg(n\phi) = n^{2g} \deg(\phi), \text{ for all } n \in \mathbf{Q}, \phi \in \text{End}^0(A).$$

**Corollary 5.13.** *Let  $A$  be an abelian variety over  $k$ . Then, for each  $\phi \in \text{End}^0(A)$ , there is a polynomial  $P_\phi(X) \in \mathbf{Q}[X]$  of degree  $2g$  such that  $P_\phi(n) = \deg(\phi - [n]_A)$ , for all  $n \in \mathbf{Q}$ .*

We see that  $P_\phi$  is monic and that it has integer coefficients when  $\phi \in \text{End}(A)$ . We call  $P_\phi$  the *characteristic polynomial* of  $\phi$  and we define the *trace* of  $\phi$  by the equation

$$P_\phi(X) = X^{2g} - \text{Tr}(\phi)X^{2g-1} + \dots + \deg(\phi).$$

**Proposition 5.14.** *Let  $A$  be an abelian variety over  $k$  and  $\phi \in \text{End}(A)$ . For each prime number  $\ell$  such that  $\ell \neq \text{char}(k)$ ,  $P_\phi(X)$  is the characteristic polynomial of  $\phi$  acting on  $V_\ell A$ ; hence the trace and degree of  $\phi$  are the trace and determinant of  $\phi$  acting  $V_\ell A$ .*

## 6 Tate's theorem

### 6.1 Frobenius endomorphism

We let  $k := \mathbf{F}_q$  be the finite field with  $q$  elements, where  $q = p^n$  for some prime  $p$  and an integer  $n \geq 1$ . We let  $\mathbf{F}$  be an algebraic closure of  $\mathbf{F}_q$ .

For a variety  $V$  over  $k$ , the *Frobenius map*  $\pi_V : V \rightarrow V$  is defined to be the map which is the identity on the underlying topological space of  $V$  and is the map  $\mathcal{O}_V \rightarrow \mathcal{O}_V, f \mapsto f^q$  on the structure sheaves. When  $V := \mathbf{P}^n(\mathbf{F}) = \text{Proj}(k[x_0, \dots, x_n])$ , then  $\pi_V$  is given by the ring homomorphism

$$\begin{aligned} k[x_0, \dots, x_n] &\rightarrow k[x_0, \dots, x_n] \\ x_i &\mapsto x_i^q. \end{aligned}$$

On points, this induces the map

$$\begin{aligned} \mathbf{P}^n(\mathbf{F}) &\rightarrow \mathbf{P}^n(\mathbf{F}) \\ (x_0 : \cdots : x_n) &\mapsto (x_0^q : \cdots : x_n^q). \end{aligned}$$

As a result, when  $V \subseteq \mathbf{P}^n$  is a projective embedding of  $V$ , then  $\pi_V : V \rightarrow V$  induces the map

$$\begin{aligned} V(\mathbf{F}) &\rightarrow V(\mathbf{F}) \\ (x_0 : \cdots : x_n) &\mapsto (x_0^q : \cdots : x_n^q). \end{aligned}$$

Thus  $V(\mathbf{F}_q)$  is the set of fixed points of  $\pi_V : V(\mathbf{F}) \rightarrow V(\mathbf{F})$ .

Let  $A$  be an abelian variety over  $\mathbf{F}_q$ . Then  $\pi_A$  maps  $0$  to  $0$  (because  $0 \in V(\mathbf{F})$ , and so it is an endomorphism of  $A$ ). We write  $f_A = P_{\pi_A}$  for the characteristic polynomial of  $\pi_A$ . It is a monic polynomial of degree  $2g$  with coefficients in  $\mathbf{Z}$ , where  $g = \dim A$ . For any prime number  $\ell \neq p$ , we know by Corollary 5.13 that  $f_A$  is also the characteristic polynomial of the induced endomorphism  $T_\ell(\pi_A)$  of the Tate module  $T_\ell A$ . We will refer to  $f_A$  as the characteristic polynomial of (geometric) Frobenius.

**Proposition 6.1.** *Let  $A$  be an abelian variety over  $\mathbf{F}_q$ .*

- (i) *Let  $\ell$  be a prime such that  $\ell \neq p$ . Then  $V_\ell(\pi_A)$  is a semisimple automorphism of  $V_\ell A$ .*
- (ii) *Assume  $A$  is elementary over  $\mathbf{F}_q$  (i.e., isogenous to a power of a simple abelian variety). Then  $\mathbf{Q}[\pi_A] \subset \text{End}^0(A)$  is a field, and  $f_A$  is a power of the minimum polynomial  $f_{\mathbf{Q}}^{\pi_A}$  of  $\pi_A$  over  $\mathbf{Q}$ .*

*Proof.* (i) As observed above,  $\pi_A$  lies in the centre of  $\text{End}^0(A)$ , which is a product of number fields. Hence  $\mathbf{Q}[\pi_A] \subset \text{End}^0(A)$  is a product of (number) fields, too. It follows that also  $\mathbf{Q}_\ell[\pi_A] \subset \mathbf{Q}_\ell \otimes \text{End}^0(A)$  is a product of fields; in particular  $\mathbf{Q}_\ell[\pi_A]$  is a semisimple ring. Now  $V_\ell A$  is a module of finite type over  $\mathbf{Q}_\ell[\pi_A]$ , with  $\pi_A$  acting as the automorphism  $V_\ell(\pi_A)$ . Hence  $V_\ell A$  is a semisimple  $\mathbf{Q}_\ell[\pi_A]$ -module, and this means that  $V_\ell(\pi_A)$  is a semisimple automorphism.

(ii) If  $A$  is elementary then the centre of  $\text{End}^0(A)$  is a field, so also  $\mathbf{Q}[\pi_A]$  is a field. Let  $g := f_A$  be the minimum polynomial of  $\pi_A$  over  $\mathbf{Q}$ . If  $\alpha \in \overline{\mathbf{Q}}_\ell$  is an eigenvalue of  $V_\ell(\pi_A)$  then  $g(\alpha)$  is an eigenvalue of  $g(V_\ell(\pi_A)) = V_\ell(g(\pi_A)) = V_\ell(0) = 0$ . Note that these eigenvalues (the roots of  $f_A$ ) are algebraic over  $\mathbf{Q}$ , as  $f_A$  has rational coefficients. So every root of  $f$  in  $\mathbf{Q}$  is also a root of  $g$ , which just means that  $f_A$  divides a power of  $g$ . Because  $g$  is irreducible this implies that  $f$  is a power of  $g$ .  $\square$

## 6.2 Tate's theorem

**Theorem 6.2.** *Let  $k$  be a finite field; for each integer  $g$ , there exist only finitely many isomorphism classes of abelian varieties of dimension  $g$  over  $k$ .*

**Lemma 6.3.** *Let  $k$  be a field,  $k_s$  a separable closure, and let  $\ell$  be a prime number such that  $\ell \neq \text{char}(k)$ .*

- (i) *If  $A$  and  $B$  are abelian varieties over  $k$  then the map*

$$T_\ell : \mathbf{Z}_\ell \otimes \text{Hom}(A, B) \rightarrow \text{Hom}_{\text{Gal}(k_s/k)}(T_\ell A, T_\ell B)$$

is an isomorphism if and only if the map

$$V_\ell : \mathbf{Q}_\ell \otimes \mathrm{Hom}^0(A, B) \rightarrow \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(V_\ell A, V_\ell B) \quad (2)$$

is an isomorphism.

(ii) Assume that for every abelian variety  $C$  over  $k$ , the map

$$\mathbf{Q}_\ell \otimes \mathrm{End}^0(C) \rightarrow \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell C)$$

is an isomorphism. Then, for any two abelian varieties  $A$  and  $B$  over  $k$ , the map in (2) is an isomorphism.

*Proof.* (i) By Theorem 5.8, the map  $T_\ell$  is injective and  $\mathrm{coker}(T_\ell)$  is torsion-free (hence free). Hence  $T_\ell$  is an isomorphism if and only if  $\mathbf{Q}_\ell \otimes \mathrm{coker}(T_\ell) = 0$ . Now use that  $\mathbf{Q}_\ell$  is flat over  $\mathbf{Z}_\ell$ , so the map  $V_\ell$  is again injective and  $\mathrm{coker}(V_\ell) = \mathbf{Q}_\ell \otimes \mathrm{coker}(T_\ell)$ .

(ii) Take  $C := A \times B$ . We have a decomposition of vector spaces

$$\mathrm{End}^0(C) = \mathrm{End}^0(A) \oplus \mathrm{Hom}^0(A, B) \oplus \mathrm{Hom}^0(B, A) \oplus \mathrm{End}^0(B).$$

Likewise we have, writing  $\Gamma := \mathrm{Gal}(k_s/k)$ , a decomposition

$$\mathrm{End}_\Gamma(V_\ell C) = \mathrm{End}_\Gamma(V_\ell A) \oplus \mathrm{Hom}_\Gamma(V_\ell A, V_\ell B) \oplus \mathrm{Hom}_\Gamma(V_\ell B, V_\ell A) \oplus \mathrm{End}_\Gamma(V_\ell B).$$

The map  $V_{\ell, C} : \mathbf{Q}_\ell \otimes \mathrm{End}(C) \rightarrow \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell C)$  respects these decompositions. In particular it follows that if  $V_{\ell, C}$  is an isomorphism then so is the map

$$\mathbf{Q}_\ell \otimes \mathrm{Hom}^0(A, B) \rightarrow \mathrm{Hom}_{\mathrm{Gal}(k_s/k)}(V_\ell A, V_\ell B).$$

□

**Lemma 6.4.** *Let  $A$  an abelian variety over a field  $k$ , and let  $\ell$  be a prime number such that  $\ell \neq \mathrm{char}(k)$ . Then for every  $\mathbf{Q}_\ell$ -subspace  $W \subset V_\ell A$  that is stable under the action of  $\mathrm{Gal}(k_s/k)$  there exists an element  $u \in \mathbf{Q}_\ell \mathrm{End}(A)$  such that  $W = u \cdot V_\ell A$ .*

*Proof.*

Give a reference!

□

**Theorem 6.5.** *Let  $A$  an abelian variety over a field  $k$ , and let  $\ell$  be a prime number such that  $\ell \neq \mathrm{char}(k)$ . Then the representation*

$$\rho_\ell : \mathrm{Gal}(k_s/k) \rightarrow \mathrm{GL}(V_\ell A)$$

is semisimple and the map

$$\mathbf{Q}_\ell \mathrm{End}^0(A) \rightarrow \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell A)$$

is an isomorphism.

*Proof.* To prove that  $\rho_\ell$  is a semisimple representation, suppose we have a Galois-stable subspace  $W \subset V_\ell A$ . By Lemma 6.4, there exists an element  $u \in \mathbf{Q}_\ell \text{End}(A)$  with  $W = u \cdot V_\ell A$ . Since  $\mathbf{Q}_\ell \text{End}(A)$  is semisimple, the right ideal  $u \cdot \mathbf{Q}_\ell \text{End}(A)$  is generated by an idempotent  $e$ . Write  $u = e \cdot a$  and  $e = u \cdot b$  for some  $a, b \in \mathbf{Q}_\ell \text{End}(A)$ ; this gives

$$u \cdot V_\ell A = e \cdot (a \cdot V_\ell A) \subseteq e \cdot V_\ell A = u \cdot (b \cdot V_\ell A) \subseteq u \cdot V_\ell A.$$

Hence  $W = e \cdot V_\ell A$ . Then  $W' := (1 - e) \cdot V_\ell A$  is a complement for  $W$ , and  $W'$  is again Galois-stable because  $\rho_\ell(g)$  commutes with  $(1 - e)$  for every  $g \in \text{Gal}(k_s/k)$ . This proves that  $\rho_\ell$  is semisimple.

The map  $\mathbf{Q}_\ell \text{End}(A) \rightarrow \text{End}_{\text{Gal}(k_s/k)}(V_\ell A)$  is injective by Theorem 5.8. Letting  $C = \text{End}_{\mathbf{Q}_\ell \text{End}(A)}(V_\ell A)$ , Theorem C.6 implies that  $\mathbf{Q}_\ell \text{End}(A) = \text{End}_C(V_\ell A)$ . Hence it suffices to show that for every  $\varphi \in \text{End}_{\text{Gal}(k_s/k)}(V_\ell A)$  and  $c \in C$  we have  $\varphi c = c\varphi$ . The graph  $\Gamma_\varphi \subset V_\ell A \oplus V_\ell A$  is a Galois-stable subspace. Applying Lemma 6.4 it follows that there exists an element  $u \in \mathbf{Q}_\ell \text{End}(A^2) = M_2(\mathbf{Q}_\ell \text{End}(A))$  such that  $\Gamma_\varphi = u \cdot V_\ell A^2$ . But  $\gamma := \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \in M_2(\mathbf{Q}_\ell \text{End}(A))$  commutes with  $u$ , so

$$\gamma \cdot \Gamma_\varphi = \gamma \cdot u \cdot V_\ell A^2 = u \cdot \gamma \cdot V_\ell A^2 \subseteq \Gamma_\varphi.$$

This means precisely that for every  $v \in V_\ell A$  we have  $c \cdot \varphi(v) = \varphi(c \cdot v)$ ; hence  $\varphi c = c\varphi$  and the theorem is proved.  $\square$

**Theorem 6.6** (Tate's Theorem). *Let  $k$  be a finite field. Let  $\ell$  be a prime such that  $\ell = \text{char}(k)$ .*

(i) *For any abelian variety  $A$  over  $k$  the representation*

$$\rho_\ell = \rho_{\ell, A} : \text{Gal}(k_s/k) \rightarrow \text{GL}(V_\ell A)$$

*is semisimple.*

(ii) *For any two abelian varieties  $A$  and  $B$  over  $k$  the map*

$$\mathbf{Z}_\ell \otimes \text{Hom}^0(A, B) \rightarrow \text{Hom}_{\text{Gal}(k_s/k)}(T_\ell A, T_\ell B)$$

*is an isomorphism.*

## 7 Weil's conjectures

### 7.1 Endomorphism rings of abelian varieties: Albert classification

Let  $A$  be a  $k$ -simple abelian variety of dimension  $g$ . Let  $D = \text{End}_k^0(A)$  be the endomorphism algebra of  $A$ . Then, by Wedderburn theorem, we know that  $D$  is a division algebra. Let  $F$  the centre of  $D$ . Also, let  $(D \rightarrow D, x \mapsto x^\dagger)$  be the Rosati involution on  $A$ . This is a positive involution. So, its fixed field  $F^\dagger := \{x \in D \mid x^\dagger = x\}$  is a *totally real number field*, i.e. every embedding  $F^\dagger \hookrightarrow \mathbf{C}$  factors through  $\mathbf{R}$ . Clearly,  $F^\dagger \subseteq F$ . We let  $e = [F : \mathbf{Q}]$  and  $e^\dagger = [F^\dagger : \mathbf{Q}]$ , and we let  $d \in \mathbf{Z}_{\geq 1}$  be such that  $[D : F] = d^2$ .

**Theorem 7.1** (Albert Classification). *Let  $A$  be a  $k$ -simple abelian variety of dimension  $g$ , and  $D = \text{End}_k^0(A)$  the endomorphism algebra of  $A$ . Keeping the notations above,  $D$  is isomorphic to an algebra of one of the following four types:*

(i) *TYPE I.  $D = F = F^\dagger$ , and the Rosati involution  $^\dagger$  is the identity map. In this case,  $e \mid g$ .*

- (ii) *TYPE II.*  $F = F^\dagger$ , and  $D$  is a totally indefinite quaternion division algebra over  $F$ . That is, for any embedding  $\sigma : F \hookrightarrow \mathbf{R}$ , one has that  $D \otimes_\sigma \mathbf{R} \simeq M_2(\mathbf{R})$ . In this case  $2e \mid g$ .
- (iii) *TYPE III.*  $F = F^\dagger$ , and  $D$  is a totally definite quaternion division algebra over  $F$ . That is, for any embedding  $\sigma : F \hookrightarrow \mathbf{R}$ , one has that  $D \otimes_\sigma \mathbf{R} \simeq \mathbb{H}$ , where  $\mathbb{H}$  is the Hamilton quaternion algebra. In this case  $e^2 \mid g$ .
- (iv) *TYPE IV.*  $F$  is a CM extension of  $F^\dagger$  (i.e a totally imaginary quadratic extension of  $F^\dagger$ ) and  $D$  is a division algebra with centre  $F$ . In this case  $e^\dagger d^2 \mid g$  if  $\text{char}(k) = 0$ , and  $e^\dagger d \mid g$  if  $\text{char}(k) > 0$ .

## 7.2 Zeta functions of abelian varieties

**Theorem 7.2.** *Let  $A$  be an abelian variety of dimension  $g$  over  $\mathbf{F}_q$ , where  $q = p^n$ .*

- (i) *Every complex root  $\alpha$  of  $f_A$  has absolute value  $|\alpha| = \sqrt{q}$ .*
- (ii) *If  $\alpha$  is a complex root of  $f_A$  then so is  $\bar{\alpha} = q/\alpha$ , and the two roots occur with the same multiplicity. If  $\alpha = \sqrt{q}$  or  $\alpha = -\sqrt{q}$  occurs as a root then it occurs with even multiplicity.*

*Proof.* (i) We first reduce to the case that  $A$  is simple (over  $\mathbf{F}_q$ ). For this, choose an isogeny

$$h : A \rightarrow A' = A_1 \times \cdots \times A_s,$$

where the factors  $A_i$  are simple. Then  $h$  induces an isomorphism

$$V_\ell(h) : V_\ell A \xrightarrow{\simeq} V_\ell A' = V_\ell A_1 \oplus \cdots \oplus V_\ell A_s.$$

Since  $h \circ \pi_A = \pi_{A'} \circ h$ , the automorphism  $V_\ell(h) \circ V_\ell(\pi_A) \circ V_\ell(h)^{-1}$  of  $V_\ell A_1 \oplus \cdots \oplus V_\ell A_s$  is the one given by

$$(\xi_1, \dots, \xi_s) \mapsto (V_\ell(\pi_{A_1})(\xi_1), \dots, V_\ell(\pi_{A_s})(\xi_s)).$$

So  $f_A = f_{A_1} \cdots f_{A_s}$ , and it suffices to prove the theorem for simple abelian varieties.

Let  $\lambda$  be any polarisation on  $A$ , and  $\dagger$  the associated Rosati involution on  $\text{End}^0(A)$ . We will first show that  $\pi_A \cdot \pi_A^\dagger = [q]_A$ . Since

$$\pi_A \cdot \pi_A^\dagger = \pi_A \cdot \lambda^{-1} \cdot \pi_A^\vee \cdot \lambda = \lambda^{-1} \cdot \pi_{A^\vee} \cdot \pi_A^\vee \cdot \lambda,$$

it suffices to show that  $\pi_{A^\vee} \cdot \pi_A^\vee = [q]_{A^\vee}$ . By definition,  $\pi_A = F_A^n / \mathbf{F}_q$ . So by the properties of the Verschiebung map  $V_{A/\mathbf{F}_q}$  (see next section), we have  $\pi_A^\vee = V_{A^\vee/\mathbf{F}_q}$ , and

$$\pi_{A^\vee} \cdot \pi_A^\vee = F_{A^\vee/\mathbf{F}_q}^n \cdot V_{A^\vee/\mathbf{F}_q}^n = [p^n]_{A^\vee} = [q]_{A^\vee}.$$

This gives  $\pi_A \cdot \pi_A^\dagger = [q]_A$ .

Now, since  $A$  is simple,  $\mathbf{Q}[\pi_A]$  is a number field. Furthermore, by Proposition 6.1,  $f_A$  is a power of the minimum polynomial of  $g$  of  $\pi_A$  over  $\mathbf{Q}$ . So, the complex roots of  $f_A$  are precisely the complex numbers of the form  $\iota(\pi_A)$  for some embedding  $\iota : \mathbf{Q}[\pi_A] \rightarrow \mathbf{C}$ . The relation  $\pi_A^\dagger = q/\pi_A$  shows that  $\mathbf{Q}[\pi_A] \subset \text{End}^0(A)$  is stable under the Rosati involution, which is a positive involution. This leads to two possible cases:

- (a) *Totally real case:*  $\mathbf{Q}[\pi_A]$  is a totally real field and  $\dagger$  is the identity on  $\mathbf{Q}[\pi_A]$ .

- (b) CM case:  $\mathbf{Q}[\pi_A]$  is a CM-field and for every complex embedding  $\iota : \mathbf{Q}[\pi_A] \rightarrow \mathbf{C}$  we have  $\iota(x^\dagger) = \iota(x)$ , for all  $x \in \mathbf{Q}[\pi_A]$ .

In either cases,  $\pi_A \cdot \pi_A^\dagger = q$  implies that all roots  $\alpha \in \mathbf{C}$  of  $f_A$  have absolute value  $|\alpha| = \sqrt{q}$ .

(ii) The first two assertions are trivial, because  $f_A$  has rational (hence real) coefficients. The only non-trivial point is that  $\sqrt{q}$  and  $-\sqrt{q}$  can only occur as roots with even multiplicity. Again, it is enough to show this for  $A$  is simple. The field  $\mathbf{Q}[\pi_A]$  cannot have any real embedding if its CM. Therefore, the cases  $\alpha = \pm\sqrt{q}$  only occur when  $\mathbf{Q}[\pi_A]$  is totally real. In that case, they are the only possible roots since  $\bar{\alpha} \cdot \alpha = q$ . If  $\sqrt{q}$  occurs with multiplicity  $m$  then  $-\sqrt{q}$  occurs with multiplicity  $2g - m$ , so  $f_A(0) = (-1)^m q^g$ . But  $f_A(0) = \deg(-\pi_A) = q^g$ , so  $m$  is even.  $\square$

Let  $X$  be a scheme of finite type over  $\mathbf{F}_q$ . For any positive integer  $n$  the number, let  $N_n := \#X(\mathbf{F}_{q^n})$  of  $\mathbf{F}_{q^n}$ -rational points of  $X$ . The *zeta function* of  $X$  is defined by

$$Z(X; t) := \exp\left(\sum_{n=1}^{\infty} N_n \frac{t^n}{n}\right) \in \mathbf{Q}[[t]] \quad (3)$$

**Theorem 7.3.** *Let  $A$  be an abelian variety of dimension  $g$  over  $\mathbf{F}_q$ . Let  $\alpha_1, \dots, \alpha_{2g}$  be the sequence of complex roots of the characteristic polynomial  $f_A$  (counted with multiplicity), so that we have*

$$f_A = \prod_{i=1}^{2g} (t - \alpha_i).$$

- (i) *For any positive integer  $n$  we have*

$$\#A(\mathbf{F}_{q^n}) = \prod_{i=1}^{2g} (1 - \alpha_i^n) = \sum_{k=0}^{2g} (-1)^k \operatorname{Tr}\left(\pi_A^n; \bigwedge^k V_\ell A\right),$$

where  $\ell$  is any prime number different from  $p$  and  $\operatorname{Tr}(\pi_A^n; \bigwedge^k V_\ell A)$  is the trace of the automorphism  $\bigwedge^k V(\pi_A^n)$  acting on  $\bigwedge^k V_\ell A$ .

- (ii) *The zeta function of  $A$  is given by*

$$Z(A; t) = \frac{P_1 P_3 \cdots P_{2g-1}}{P_0 P_2 \cdots P_{2g}}$$

where  $P_k \in \mathbf{Z}[t]$ ,  $k = 0, \dots, 2g$ , is the polynomial given by

$$P_k(t) = \prod_{1 \leq i_1 < \dots < i_k \leq 2g} (1 - \alpha_{i_1} \cdots \alpha_{i_k} t) = \det(\operatorname{id} - t\pi_A; \bigwedge^k V_\ell A).$$

- (iii) *The zeta function satisfies the functional equation*

$$Z(A; \frac{1}{q^g t}) = Z(X; t).$$

*Proof.* (i) The characteristic polynomial  $f_{\pi_A^n}$  is given by

$$f_{\pi_A^n} := \prod_{i=1}^{2g} (t - \alpha_i^n).$$



Now, recall that

$$A(\mathbf{F}_{q^n}) = \ker(1 - \pi_A^n).$$

Since  $\#A(\mathbf{F}_{q^n}) < \infty$ ,  $1 - \pi_A^n$  is an isogeny. But  $\pi_A$  is purely inseparable (using the differential criterion of separability). Hence,  $1 - \pi_A^n$  is a separable isogeny. This implies that

$$\#A(\mathbf{F}_{q^n}) = \deg(1 - \pi_A^n) = f_{\pi_A^n}(1) = \prod_{i=1}^{2g} (1 - \alpha_i^n).$$

The eigenvalues of  $\wedge^k V_\ell(\pi_A^n)$  are the numbers the products

$$\alpha_{i_1}^n \cdots \alpha_{i_k}^n \text{ with } 1 \leq i_1 < i_2 < \cdots < i_k \leq 2g.$$

The second identity in (i) follows from the elementary relation

$$\prod_{i=1}^{2g} (1 - \alpha_i^n) = \sum_{k=0}^{2g} \left( (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq 2g} \alpha_{i_1}^n \cdots \alpha_{i_k}^n \right).$$

(ii) We use the general fact (see Hartshorne [8, Appendix C, Lemma 4.1]) that for  $\phi \in \text{End}(V)$ , where  $V$  is a finite dimensional vector space  $V$  over a field  $K$ , we have an identity of formal power series

$$\exp\left(\text{Tr}(\phi^n; V) \cdot \frac{t^n}{n}\right) = \det(1 - t \cdot \phi; V)^{-1}.$$

Applying (i) then gives

$$Z(A; t) = \exp\left(\sum_{n=1}^{\infty} \sum_{k=0}^{2g} (-1)^k \text{Tr}(\pi_A^n; \wedge^k V_\ell A) \frac{t^n}{n}\right) = \prod_{k=0}^{2g} \exp\left(\sum_{n=1}^{\infty} (-1)^k \text{Tr}(\pi_A^n; \wedge^k V_\ell A) \frac{t^n}{n}\right)^{(-1)^k}$$

The eigenvalues of  $\wedge V_\ell(\pi_A)$  are the numbers the products

$$\alpha_{i_1} \cdots \alpha_{i_k}, \text{ with } 1 \leq i_1 < i_2 < \cdots < i_k \leq 2g.$$

Therefore

$$\det(1 - t\pi_A; \wedge^k V_\ell A) = \prod_{1 \leq i_1 < i_2 < \cdots < i_k \leq 2g} (1 - t\alpha_{i_1} \cdots \alpha_{i_k}) =: P_k.$$

Since  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$  acts naturally on the set of sequences  $(\alpha_{i_j})_{1 \leq j \leq k}$ ,  $P_k \in \mathbf{Q}[x]$ . Furthermore, since  $P_k$  is a monic, all its roots are algebraic integers; hence  $P_k \in \mathbf{Z}[t]$ . □

## 8 Jacobian varieties

### 8.1 The functor

Let  $X$  be a complete nonsingular curve over  $k$ . We recall that the set of divisors on  $X$ , denoted  $\text{Div}(X)$  is the set formal sums

$$D = \sum_{i=1}^n n_i P_i, \text{ with } n_i \in \mathbf{Z}, P_i \in X(\bar{k}).$$

The *degree map*  $\deg : \text{Div}(X) \rightarrow \mathbf{Z}$  is given by  $\deg(D) = \sum_{i=1}^n n_i$ . Since every invertible sheaf  $\mathcal{L}$  on  $X$  is of the form  $\mathcal{L}(D)$  for some divisor  $D$ , and  $D$  is uniquely determined up to linear equivalence, we can define  $\deg(\mathcal{L}) = \deg(D)$ . By the Riemann-Roch theorem says that

$$\chi(X, \mathcal{L}) = \deg(\mathcal{L}) + 1 - g.$$

We recall  $\text{Pic}(X)$  is the set of isomorphism classes of invertible sheaves on  $X$ , and we define

$$\text{Pic}^0(X) := \{ \mathcal{L} \in \text{Pic}(X) \mid \deg \mathcal{L} = 0 \}.$$

Let  $T$  be a connected scheme over  $k$ , and write on  $X \times T = X \times_k T$  for  $X \times_{\text{Spec}(k)} T$ , or simply  $X \times_k k'$  when  $T = \text{Spec}(k')$  for a field extension  $k'/k$ . For  $t \in T$ , let  $X_t$  be the fibre at  $t$ . For  $\mathcal{L} \in \text{Pic}(X \times T)$ , one can show that the map  $t \mapsto \chi(X_t, \mathcal{L}_t)$  is locally constant. Therefore  $\deg(\mathcal{L}_t)$ , is independent of  $t$ . Moreover, the constant degree of  $\mathcal{L}_t$  is invariant under base change relative to maps  $T' \rightarrow T$ . Let

$$F(T) = \{ \mathcal{L} \in \text{Pic}(X \times T) \mid \deg(\mathcal{L}_t) = 0, \text{ for all } t \in T \} / p_T^* \text{Pic}(T),$$

where  $p_T : X \times_k T \rightarrow T$  is the projection onto  $T$ . Then  $F$  is a functor from schemes over  $k$  to abelian groups. For  $T$  a connected scheme over  $k$ , we may think of  $F(T)$  as being the group of families of invertible sheaves on  $X$  of degree 0 parametrised by  $T$ , modulo the trivial families. Indeed, for any sheaf  $\mathcal{M} \in \text{Pic}(T)$ ,  $(p_T^* \mathcal{M})_t$  is isomorphic to  $\mathcal{O}_{X_t}$  and so  $\deg(p_T^* \mathcal{M})_t = 0$ . The Jacobian attempts to represent the functor  $F$ .

**Theorem 8.1.** *There is an abelian variety  $\text{Jac}(X)$  over  $k$  and a morphism of functors  $\iota : F \rightarrow \text{Jac}(X)$  such that  $\iota : F(T) \rightarrow \text{Jac}(X)(T)$  is an isomorphism whenever  $X(T)$  is nonempty.*

## 8.2 Obstruction to representability

The functor  $F$  is representable if and only if it is a sheaf. However, there can some obstruction to this being the case. Indeed, let  $k'/k$  be a Galois extension with group  $\Gamma$ . Then the natural map  $F(k) \rightarrow F(k')^\Gamma$  need not be a bijection, which is a requirement for representability.

**Proposition 8.2.** *Let  $k'/k$  be a Galois extension of group  $\Gamma$ . Then there is a natural exact sequence*

$$0 \rightarrow \text{Pic}(X) \rightarrow \text{Pic}(X \times_k k')^\Gamma \rightarrow \text{Br}(k),$$

where  $\text{Br}(k)$  is the Brauer group of  $k$ . In particular, given  $\mathcal{L} \in \text{Pic}(X \times_k k')$  there is an obstruction in  $\text{Br}(k)$  measuring the failure of  $\mathcal{L}$  to descend to  $X$ .

*Proof.* We first show that the first map is injective. Let  $p_X : X \times_k k' \rightarrow X$  be the projection onto  $X$ , and  $\mathcal{L}$  and  $\mathcal{L}'$  are two line bundles on  $X$ . We need to show that, if  $p_X^* \mathcal{L}$  and  $p_X^* \mathcal{L}'$  are isomorphic over  $X \times_k k'$ , then  $\mathcal{L}$  and  $\mathcal{L}'$  are isomorphic. Let  $i : p_X^* \mathcal{L} \simeq p_X^* \mathcal{L}'$  be an isomorphism over  $X \times_k k'$ . For  $\sigma \in \Gamma$ , the map  $i \circ \sigma : p_X^* \mathcal{L} \rightarrow p_X^* \mathcal{L}'$  is also an isomorphism. Thus  $i$  and  $i \circ \sigma$  differ by an element  $c_\sigma \in \text{Aut}(\mathcal{L}) = k'^\times$ . One easily sees that  $c$  satisfies the cocycle condition. By Hilbert's Theorem 90, the class of  $c$  in  $H^1(\Gamma, k'^\times)$  vanishes. Thus  $c$  is a coboundary, i.e., is of the form  $c_\sigma = \sigma(\alpha)/\alpha$  for some  $\alpha \in k'^\times$ . One easily sees that  $\alpha^{-1} i : p_X^* \mathcal{L} \simeq p_X^* \mathcal{L}'$  is a  $\Gamma$ -invariant isomorphism over  $X \times_k k'$ , and thus descends to  $X$ .

Now, let  $\mathcal{L} \in \text{Pic}(X \times_k k')^\Gamma$ . We will construct an element of  $\text{Br}(k)$  measuring the obstruction that  $\mathcal{L}$  comes from  $\text{Pic}(X)$ . Since  $\mathcal{L} \in \text{Pic}(X \times_k k')^\Gamma$ , we see that, for all

$\sigma \in \Gamma$ , there exists an isomorphism  $i_\sigma : \mathcal{L} \simeq \sigma^* \mathcal{L}$ . The collection of isomorphisms  $(i_\sigma)_{\sigma \in \Gamma}$  is not *a priori* compatible, which is a requirement for descent. In fact, the failure of the compatibility is what defines the Brauer obstruction. Indeed, for each  $\sigma, \tau \in \Gamma$ , both  $\sigma^*(i_\tau) \circ i_\sigma$  and  $i_{\sigma\tau}$  are isomorphisms  $\mathcal{L} \simeq (\sigma\tau)^* \mathcal{L}$ ; thus they differ by an element  $c_{\sigma,\tau} \in \text{Aut}(\mathcal{L}) = k'^\times$ . It is easy to see that  $c$  satisfies the 2-cocycle condition, and thus defines an element of  $H^2(\text{Gal}(k'/k), k'^\times) \subset \text{Br}(k)$ . If this 2-cocycle is a coboundary, then the choice of  $i$ 's can be modified to give descent data on  $\mathcal{L}$ , and  $\mathcal{L}$  belongs to  $\text{Pic}(X)$ . This completes the proof.  $\square$

**Example 8.3.** Let  $k = \mathbf{R}$ ,  $k' = \mathbf{C}$ , and  $X$  the curve given by  $X^2 + Y^2 + Z^2 = 0$ . Then  $X$  is isomorphic to  $\mathbf{P}^1$  over  $k'$  but not over  $k$ . Therefore,  $\text{Pic}(X \times_k k')$  is isomorphic to  $\mathbf{Z}$ . Since  $\Gamma = \mathbf{Z}/2\mathbf{Z}$ ,  $\text{Pic}(X)$  has index at most 2 inside  $\text{Pic}(X \times_k k')$ . But the bundle  $\mathcal{O}(1)$  on  $X \times_k k'$  does not descend to  $X$ , as this would give an isomorphism  $X \rightarrow \mathbf{P}^1$  over  $k$ . Therefore  $\Gamma$  acts trivially on  $\text{Pic}(X \times_k k')$  given the exact sequence

$$0 \rightarrow 2\mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow 0.$$

**Remark 8.4.** Suppose  $k$  is a finite extension of  $\mathbf{Q}_p$ . Then  $\text{Br}(k) = \mathbf{Q}/\mathbf{Z}$ , and Lichtenbaum showed that the image of the map  $\text{Pic}(X \times_k \bar{k})^\Gamma \rightarrow \text{Br}(k)$  is  $N^{-1}\mathbf{Z}/\mathbf{Z}$ , where  $N$  is the gcd of the degrees of divisors on  $X$ . Thus  $\text{Pic}(X) = \text{Pic}(X \times_k \bar{k})^\Gamma$  if and only if  $X$  has a divisor of degree 1 defined over  $k$ .

**Remark 8.5.** We have not actually give an example where a line bundle of degree 0 fails to descend, which is the case of interest (as  $F(k') = \text{Pic}^0(X \times_k k')$ ). I believe such an example exists if  $X$  is a genus 1 curve over a finite extension of  $\mathbf{Q}_p$  without a point.

### 8.3 The case when a rational point exists

The failure of  $F$  to satisfy descent only occurs when  $X$  has no  $k$ -rational points. To see this, suppose  $X$  has a  $k$ -rational point  $x$ . Define  $\mathcal{C}_x(T)$  to be the category

$$\mathcal{C}_x(T) := \{(\mathcal{L}, i) : \mathcal{L} \in \text{Pic}(X \times_k T) \mid \deg \mathcal{L}_t = 0, \text{ for all } t \in T, \text{ and } i : \mathcal{L}|_{\{x\} \times T} \simeq \mathcal{O}_T\}.$$

Define  $F_x(T)$  to be the set of isomorphism classes in  $\mathcal{C}_x(T)$ . The key point is that objects of  $\mathcal{C}_x(T)$  are rigid: they have no automorphisms. This means that if an isomorphism class is invariant, then it has canonical descent data. It follows that  $F_x$  is a sheaf. On the other hand, we have the following lemma:

**Lemma 8.6.** *The forgetful map  $(F_x \rightarrow F, (\mathcal{L}, i) \mapsto \mathcal{L})$  is an isomorphism.*

*Proof.* Let  $T$  be a connected scheme over  $k$ , and  $(\mathcal{L}, i)$  and  $(\mathcal{L}', i')$  two elements in  $\mathcal{C}_x(T)$  such that  $\mathcal{L} \simeq \mathcal{L}' \otimes p_T^*(\mathcal{L}'')$  for some line bundle  $\mathcal{L}''$  on  $T$ . Since  $\mathcal{L}|_{\{x\} \times T} \simeq \mathcal{O}_T \simeq \mathcal{L}'|_{\{x\} \times T}$ , we see that  $\mathcal{L}''$  is trivial, and so  $\mathcal{L} \simeq \mathcal{L}'$ . This proves injectivity.

For the surjectivity, let  $\mathcal{L}$  be a line bundle on  $X \times_k T$ , and  $\mathcal{L}_0$  its restriction to  $\{x\} \times T$ . Then  $\mathcal{L} \otimes p_T^*(\mathcal{L}_0^{-1})$  is naturally an element of  $\mathcal{C}_x(T)$  mapping to  $\mathcal{L}$  in  $F(T)$ .  $\square$

We thus see that, when  $X$  has a  $k$ -point,  $F$  is a sheaf.

**Theorem 8.7.** *Suppose  $X$  has a  $k$ -point  $x$ . Then the functor  $F$  is representable. The representing scheme is denoted by  $\text{Jac}(X)$ , and called the Jacobian variety of  $X$ .*

Theorem 8.7 implies that there exists a pair  $(\text{Jac}(X), \mathcal{M})$ , where  $\text{Jac}(X)$  is an abelian variety and a line bundle  $\mathcal{M}$  on  $X \times \text{Jac}(X)$  such that the following are true:

- (a)  $\mathcal{M}|_{X \times \{0\}} \simeq \mathcal{O}_X$  and  $\mathcal{M}|_{\{x\} \times \text{Jac}(X)} \simeq \mathcal{O}_{\text{Jac}(X)}$ ;
- (b) for any connected scheme  $T$  over  $k$ , a point  $t$  on  $T$ , and a line bundle  $\mathcal{L}$  on  $X \times T$  such that  $\mathcal{L}|_{X \times \{t\}} \simeq \mathcal{O}_X$  and  $\mathcal{L}|_{\{x\} \times T} \simeq \mathcal{O}_T$ , there exists a unique morphism  $\phi : T \rightarrow \text{Jac}(X)$  such that  $\phi(t) = 0$  and  $(1 \times \phi)^* \mathcal{M} \simeq \mathcal{L}$ .

The pair  $(\text{Jac}(X), \mathcal{M})$  is unique up to isomorphism. If  $X$  does not have a point then  $F$  is not necessarily a sheaf, and thus not necessarily representable. However, one can replace  $F$  with its sheafification, and this turns out to be representable. Thus one can define the Jacobian of  $X$  even when  $X(k) = \emptyset$ .

## 8.4 Construction of the Jacobian

We now sketch the proof of the representability of  $F$  when  $X(k)$  is non-empty. Let  $x \in X(k)$ , and  $X^{(r)}$  the  $r$ -th symmetric power of  $X$ , i.e., the quotient of  $X^r$  by the action of the symmetric group  $S_r$ . Points on  $X^{(r)}$  defined over  $k'$  can be identified with effective divisors on  $X \times_k k'$  of degree  $r$ . We will consider  $X^{(g)}$ , where  $g$  is the genus of  $X$ . Let  $U \subset X^{(g)} \times X^{(g)}$  be the subset given by

$$U := \left\{ (D, D') \in X^{(g)} \times X^{(g)} : \ell(D + D - g[x]) = 1 \right\}.$$

For any effective divisors  $D$  and  $D'$  of degree  $g$  on  $X$ , the Riemann–Roch theorem implies that  $\ell(D + D' - g[x]) \geq 1$ . So, by semi-continuity, the locus  $U$  where equality holds is open. To show  $U$  is non-empty, proceed as follows. Taking  $D' = g[x]$ , one must find an effective divisor  $D$  of degree  $g$  with  $\ell(D) = 1$ , or, equivalently  $\ell(K - D) = 0$ . Simply pick  $g$  points  $x_1, \dots, x_g$  on  $X$  such that the restriction map  $H^0(X, \Omega^1) \rightarrow \prod_{i=1}^g T_{x_i}^*$  is an isomorphism.

Given  $(D, D') \in U$ , there is a non-zero meromorphic function  $f$  on  $X$ , unique up to scaling, such that  $D'' = \text{div}(f) + D + D - g[x]$  is effective. We define a map  $U \rightarrow X^{(g)}$  by sending  $(D, D')$  to  $D''$ . By working systematically with families of divisors, one shows that this is a map of schemes. Therefore, it induces a rational map  $X^{(g)} \times X^{(g)} \dashrightarrow X^{(g)}$ . This rational map satisfies the axioms of a group (it is a group object in the category of varieties with rational maps). Weil showed that any such rational group variety can be upgraded to an actual group variety. Precisely, there exists a group variety  $J$  (unique up to isomorphism) and a unique isomorphism of rational group varieties  $X^{(g)} \dashrightarrow J$ .

Finally, we need to show that  $J$  represents  $F$ . To that end, we first show that  $J$  is proper, so that the rational map  $X^{(g)} \dashrightarrow J$  is an actual map. Then, we define a map  $\phi : \text{Div}^0(X) \rightarrow J$  as follows. If  $\deg D = 0$  is a degree 0 and  $D + g[x]$  is effective, then we view  $D + g[x]$  as an element of  $X^{(g)}$  and takes its image in  $J$ . If  $D + g[x]$  is not effective, then we find a divisor  $D'$  such that  $\deg D' = 0$ , and both  $D + D' + g[x]$  and  $D' + g[x]$  are effective; and we define  $\phi(D) = \phi(D + D') - \phi(D')$ . Working with families of divisors,  $\phi$  gives a map of functors  $F \rightarrow J$ . One then verifies that it is a bijection on  $T$ -points.

## 8.5 Basic properties

The Jacobian variety satisfies the following basic properties:

- One can show that  $T_0(\text{Jac}(X)) = H^1(X, \mathcal{O})$  using the functor of points of  $\text{Jac}(X)$  and the interpretation of the tangent space in terms of dual numbers.

- From this, one finds that  $H^0(\text{Jac}(X), \Omega^1)$  is naturally isomorphic to  $H^0(X, \Omega^1)$ .
- One again has a map  $f_x : X \rightarrow \text{Jac}(X)$  given a base point  $x \in X(k)$ . On field points, this takes a point  $y \in X(k)$  to the degree 0 divisor  $[y] - [x]$ . On  $T$ -points, it does the same thing, but one must use a relative notion of divisor.
- By definition,  $\text{Jac}(X)(k)$  is isomorphic to  $\text{Pic}^0(X)$ .

There are comparison theorems between the first (co)homology groups of  $X$  and  $\text{Jac}(X)$ , though this now involves cohomology. To see this, one can use Kummer theory. Suppose  $n$  is prime to  $\text{char}(k)$ , so that we have an exact sequence of sheaves on the étale site of  $X$ :

$$0 \rightarrow \mu_n \rightarrow \mathbf{G}_m \xrightarrow{[n]} \mathbf{G}_m \rightarrow 0.$$

Taking cohomology over  $\bar{k}$ , and using the fact that  $(\bar{k}^\times \rightarrow \bar{k}^\times, x \mapsto x^n)$  is surjective, we see that

$$H^1(X_{\bar{k}}, \mathbf{G}_m)[n] = H^1(X_{\bar{k}}, \mu_n).$$

Now, we also have

$$H^1(X_{\bar{k}}, \mathbf{G}_m) = \text{Pic}(X_{\bar{k}}).$$

Since all torsion in this group is of degree 0, we see that

$$H^1(X_{\bar{k}}, \mathbf{G}_m)[n] = \text{Jac}(X)[n](\bar{k}).$$

Replacing  $n$  with  $\ell^n$  and taking an inverse limit, we find

$$T_\ell(\text{Jac}(X)) = H^1(X_{\bar{k}}, \mathbf{Z}_\ell(1)),$$

where the (1) is a Tate twist.

## 9 Zeta functions of curves

### 9.1 Hasse–Weil–Serre theorem

**Proposition 9.1.** *Let  $X$  be a nonsingular complete curve over a finite field  $\mathbf{F}_q$ , and  $J := \text{Jac}(X)$  its Jacobian. Let  $\alpha_1, \dots, \alpha_{2g}$  be the complex roots of the polynomial  $f_J$ . Then for every positive integer  $n$  we have*

$$\#X(\mathbf{F}_{q^n}) = 1 - \text{Tr}(\pi_J^n) + q^n = 1 - \sum_{i=1}^{2g} \alpha_i^n + q^n.$$

*Proof.* It suffices to prove this for  $n = 1$ , as the assertion for arbitrary  $n$  then follows by considering  $X \times_{\mathbf{F}_q} \mathbf{F}_{q^n}$ . The number of points is given by the intersection number

$$\#X(\mathbf{F}_q) = \Delta_X \cdot \Gamma, \text{ where } \Gamma_X \subset X \times X$$

is the graph of the geometric Frobenius  $\pi_X$ . To prove the identity

$$\Delta_X \cdot \Gamma = 1 - \text{Tr}(\pi_J) + q.$$

we may work over  $k := \mathbf{F}_q$ . Choose a point  $P \in X(k)$  and let  $\phi : X \rightarrow J$  be the map given on points by  $Q \mapsto [Q - P]$ .  $\square$

**Theorem 9.2.** *Let  $X$  be a nonsingular complete curve of genus  $g$  over a finite field  $\mathbf{F}_q$ , and  $J := \text{Jac}(X)$  its Jacobian. Let  $\alpha_1, \dots, \alpha_{2g}$  be the complex roots of the characteristic polynomial  $f_J$  of the geometric Frobenius of  $J$ . Let  $P_0 := 1 - t$  and  $P_2 := 1 - qt$ , and let*

$$P_1 := \prod_{i=1}^{2g} (1 - \alpha_i \cdot t)$$

be the reciprocal of the polynomial  $f_J$ . Then we have

$$Z(X; t) = \frac{P_1}{P_0 P_2} = \frac{P_1}{(1-t)(1-qt)}.$$

All complex roots of the polynomial  $P_i$  are algebraic integers of absolute value  $q^{i/2}$ . Further,  $Z(X; t)$  satisfies the functional equation

$$Z(X; t) = q^{g-1} \cdot t^{2g-2} \cdot Z(X; \frac{1}{qt}).$$

**Theorem 9.3.** *Let  $X$  be an abelian variety of dimension  $g$  over  $\mathbf{F}_q$ . Then, we have*

$$|\text{Tr}(\pi_X)| \leq g \cdot [2\sqrt{q}].$$

This is an equality if and only if either  $\alpha_i + \bar{\alpha}_i = [2\sqrt{q}]$  for all  $i$  or  $\alpha_i + \bar{\alpha}_i = -[2\sqrt{q}]$  for all  $i$ .

**Corollary 9.4** (Hasse–Weil–Serre). *Let  $X$  be a complete nonsingular curve over  $\mathbf{F}_q$ . Then for the number of  $\mathbf{F}_q$ -rational points of  $X$ , we have the inequalities*

$$q + 1 - g[2\sqrt{q}] \leq \#X(\mathbf{F}_q) \leq q + 1 + g[2\sqrt{q}].$$

## 9.2 Examples: curves of genus $\leq 3$

**Example 9.5.** Let  $X \subset \mathbf{P}^2$  be the Klein curve over  $\mathbf{F}_2$ ; this is the nonsingular quartic curve over  $\mathbf{F}_2$  given by the homogeneous equation  $X^3Y + Y^3Z + Z^3X = 0$ . The genus of  $X$  is 3 and one easily checks that  $\#X(\mathbf{F}_2) = 3$ , that  $\#X(\mathbf{F}_4) = 5$ , and  $\#X(\mathbf{F}_8) = 24$ . The characteristic polynomial of Frobenius is  $f_J = t^6 + 5t^3 + 8$  and  $X$  is ordinary. This curve reaches the Serre bound  $q + 1 + g[2\sqrt{q}]$  over  $\mathbf{F}_8$ . Note that in this case Serre's bound is better than the original Hasse–Weil bound:  $8 + 1 + 3[2\sqrt{8}] = 24$ , whereas  $8 + 1 + [6\sqrt{8}] = 25$ .

**Example 9.6.** Let  $F = \mathbf{Q}(\sqrt{53})$  and  $\mathcal{O}_F = \mathbf{Z}[w]$  the ring of integers of  $F$ , where  $w = \frac{1+\sqrt{53}}{2}$ . We let  $X$  be the curve defined over  $F$  by  $X : y^2 + Q(x)y = P(x)$ , where

$$P := -4x^6 + (w - 17)x^5 + (12w - 27)x^4 + (5w - 122)x^3 + (45w - 25)x^2 - (9w + 137)x + 14w + 9,$$

$$Q := wx^3 + wx^2 + w + 1.$$

The discriminant of this curve is  $\Delta_X = -\epsilon^7$ , where  $\epsilon = 4 - w$ . Thus  $X$  has everywhere good reduction. This means that the Jacobian  $A = \text{Jac}(X)$  has everywhere good reduction. So for each prime ideal  $\mathfrak{p} \subset \mathcal{O}_F$ ,  $A \times_{\mathcal{O}_F} \mathbf{F}_{\mathfrak{p}}$  is an abelian surface. Using Sage or Magma, compute the reduction of  $A$  modulo all the prime ideals of norm less than 100, and find the number of points on  $A \times_{\mathcal{O}_F} \mathbf{F}_{\mathfrak{p}}$ .

**Example 9.7.** Let  $S_2(61, (\frac{\cdot}{61}))$  be the space of cusp forms of weight 2, level 61 and character the quadratic character of  $F := \mathbf{Q}(\sqrt{61})$ . The space  $S_2(61, (\frac{\cdot}{61}))$  has dimension 4. The space is irreducible and has a unique conjugacy class of newforms. Let  $f$  be the newform given by

$$\begin{aligned} f &= \sum_{n=1}^{\infty} a_n q^n \\ &= q + \sqrt{4 - \sqrt{3}}q^2 + (\sqrt{3} - 1)q^3 + (\sqrt{3} - 2)q^4 - \sqrt{3}q^5 + (\sqrt{3} - 1)\sqrt{4 - \sqrt{3}}q^6 - \sqrt{3}\sqrt{4 - \sqrt{3}}q^7 + O(q^8). \end{aligned}$$

Then  $f$  corresponds to an abelian variety  $B_f$  of dimension 4 defined over  $\mathbf{Q}$ . One can show that, for each prime  $p \neq 61$ , the eigenvalues of Frobenius are given by the conjugates of  $a_p$ . So, the traces of Frobenius acting on the Tate module  $T_\ell(B_f \times_{\mathbf{Z}} \mathbf{F}_p)$  is given by  $b_p$  where the sequence  $(b_n)_{n \geq 1}$  is given by

$$\begin{aligned} \text{Tr}(f) &= \sum_{\sigma: E \rightarrow \mathbf{C}} \left( \sum_{n=1}^{\infty} a_n q^n \right) = \sum_{n=1}^{\infty} \left( \sum_{\sigma: E \rightarrow \mathbf{C}} a_n \right) q^n = \sum_{n=1}^{\infty} b_n q^n. \\ &= 4q - 4q^3 - 8q^4 + 4q^9 + 20q^{12} + 12q^{13} - 12q^{14} + O(q^{15}). \end{aligned}$$

The abelian variety  $B_f$  is  $\mathbf{Q}$ -simple. However,  $B_f \times_{\mathbf{Q}} F$  is no longer simple. One can show that there exists an abelian surface  $A_f$  defined over  $F$  such that

$$B_f \times_{\mathbf{Q}} F \sim_F A_f \times A_f^\sigma,$$

where  $A_f^\sigma$  is the  $\text{Gal}(F/\mathbf{Q})$ -conjugate of  $A_f$ . The endomorphism ring of the surface  $A_f$  is  $\text{End}_F(A_f) = \mathbf{Z}[\sqrt{3}]$ . The surface  $A_f$  has everywhere good reduction. This means that, for every prime ideal  $\mathfrak{p} \subset \mathcal{O}_F$ ,  $A_f \times_{\mathcal{O}_F} \mathbf{F}_{\mathfrak{p}}$  is an abelian surface, where  $\mathcal{O}_F$  is the ring of integers of  $F$ , and  $\mathbf{F}_{\mathfrak{p}} = \mathcal{O}_F/\mathfrak{p}$  the residue field at  $\mathfrak{p}$ . The endomorphism ring  $\text{End}_{\mathbf{F}_{\mathfrak{p}}}(A_f \times_{\mathcal{O}_F} \mathbf{F}_{\mathfrak{p}}) \supset \mathbf{Z}[\sqrt{3}]$ .

## 10 Dieudonné modules and $p$ -divisible groups

We have seen that the notion of  $\ell$ -adic Tate modules, for primes  $\ell$  away from the characteristic  $p$  of the ground field, is incredibly useful when studying abelian varieties. The analogous notion at the prime  $p$  is that of Dieudonné modules. At finite level, Dieudonné modules classify commutative finite group schemes of  $p$ -power order over a field of characteristic  $p$ . Dieudonné modules can be used to determine local Brauer invariants of the endomorphism algebra of a simple abelian variety over a finite field at  $p$ -adic places of the centre.

### 10.1 $p$ -divisible groups

**Definition 10.1.** Let  $S$  be a base scheme. A  $p$ -divisible group over  $S$ , also called a Barsotti-Tate group over  $S$ , is an inductive system

$$\{G_n : i_n : G_n \rightarrow G_{n+1}\}_{n \in \mathbf{N}} : \quad G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \xrightarrow{i_3} \dots,$$

where:

- (i) each  $G_n$  is a commutative finite locally free  $S$ -group scheme, killed by  $p^n$ , and flat when viewed as a sheaf of  $\mathbf{Z}/p^n\mathbf{Z}$ -modules;

(ii) each  $i_n : G_n \rightarrow G_{n+1}$  is a homomorphism of  $S$ -group schemes, inducing an isomorphism  $G_n \xrightarrow{\sim} G_{n+1}[p^n]$ .

Homomorphisms of  $p$ -divisible groups are defined to be the homomorphisms of inductive systems of group schemes.

Given a  $p$ -divisible group as in Definition 10.1, we may consider the  $(G_n)_{n \in \mathbf{N}}$  as fppf sheaves on  $S$  and form the limit

$$G := \varinjlim_n G_n,$$

in the category of fppf sheaves of abelian groups. We can recover  $(G_n)_{n \in \mathbf{N}}$  from  $G$  by  $G_n = G[p^n]$ . If  $\{G_n\}$  and  $\{H_n\}$  are two  $p$ -divisible groups and we form  $G := \varinjlim_n G_n$  and  $H := \varinjlim_n H_n$ , then the homomorphisms from  $\{G_n\}$  and  $\{H_n\}$  are just the homomorphisms from  $G$  to  $H$  as fppf sheaves. In other words, by passing from the inductive system  $\{G_n\}$  to the limit  $G$ , we can identify the category of  $p$ -divisible groups over  $S$  with a full subcategory of the category of fppf sheaves in abelian groups over  $S$ .

In our case, we have  $S = \text{Spec}(k)$ . If  $G = \varinjlim G_n$  is a  $p$ -divisible group over a connected base scheme  $S$  then, by definition, the group scheme  $G_1$  is locally free and killed by  $p$ . It follows that the rank of  $G_1$  equals  $p^h$  for some integer  $h$ . We call  $h(G) := h$  the height of  $G$ .

**Definition 10.2.** *Let  $A$  be an abelian variety over a field  $k$ , and  $p$  be a prime number. Then the  $p$ -divisible group associated to  $A$ , denoted by  $A[p^\infty]$ , is the inductive system  $\{A[p^n] \hookrightarrow A[p^{n+1}]\}_{n \geq 1}$  with respect to the natural inclusion homomorphisms  $A[p^n] \hookrightarrow A[p^{n+1}]$ .*

In that case, we see that the height of  $A[p^\infty]$  is  $2g$ , where  $g = \dim(A)$ . If  $f : A \rightarrow B$  is a homomorphism of abelian varieties over  $k$ , it induces a homomorphism of  $p$ -divisible groups  $f_\infty : A[p^\infty] \rightarrow B[p^\infty]$ .

When  $G$  is a  $p$ -divisible group over  $k$ , viewed as an fppf sheaf, then we define the  $p$ -adic Tate module associated to  $G$  by  $T_p G := \text{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, G(\bar{k}))$ . Concretely, we take the limit of the projective system

$$\{G_n : i_n : G_n \leftarrow G_{n+1}\}_{n \in \mathbf{N}} : \quad G_1 \xleftarrow{\pi_{1,1}} G_2 \xleftarrow{\pi_{1,2}} G_3 \xleftarrow{\pi_{1,3}} \dots$$

When  $p \neq \text{char}(k)$ , then the  $p$ -adic Tate module of an abelian variety  $A$  is  $T_p(A[p^\infty]) = T_p A$  as defined in Section 5. Similarly, the Tate module of  $\mathbf{G}_m[p^\infty]$  is  $\mathbf{Z}_p(1)$ .

## 10.2 Dieudonné modules

### 10.2.1 Commutative group schemes of $p$ -power order

Let  $k$  be a perfect field of characteristic  $p$ . (We will be mainly interested in the case when  $k$  is finite or algebraically closed.) We want to classify finite commutative group schemes over  $k$  whose orders are  $p$ -powers. For motivation, suppose  $A$  is an abelian variety of dimension  $g$  over  $k$ . To make a  $p$ -adic analogue of the Tate module, we need to begin with the  $p$ -power torsion of  $A$ . The  $p^n$ -torsion of  $A$ , for  $n$  a positive integer, is a group scheme of order  $p^{2ng}$ . So we are naturally interested in a description of such group schemes.

Finite commutative group schemes of  $p$ -power order over  $k$  are classified in terms of Dieudonné modules. See Fontaine [10] for a detailed exposition on Dieudonné theory, and [4] for a concise summary.



**Proposition 10.3.** *Let  $k$  be field with  $\text{char}(k) = p > 0$ . Let  $G$  be a flat  $k$ -group scheme. Then, there exists a homomorphism of group schemes  $V_{G/k} : G^{(p)} \rightarrow G$  such that*

$$(i) \quad V_{G/k} \circ F_{G/k} = [p]_G \text{ and } F_{G/k} \circ V_{G/k} = [p]_{G^{(p)}};$$

$$(ii) \quad (V_{G/k})^D = F_{G^D/k} \text{ and } V_{G/k} = (F_{G^D/k})^D.$$

The homomorphism  $V_{G/k}$  is called the Verschiebung map.

Given our perfect field  $k$  of characteristic  $p$ , let  $W = W(k)$  denote the ring of Witt vectors of  $k$  (as defined in [17]). When  $k$  is finite,  $W(k)$  is the ring of integers of the unique extension of  $\mathbf{Q}_p$  whose residue field is  $k$ . Let  $K_0 := W(k)[1/p]$  be the field of fraction of  $W(k)$ . Let  $\sigma$  denote the unique automorphism of  $W(k)$  lifting the absolute Frobenius  $x \mapsto x^p$  on  $k$ .

**Definition 10.4.** *The Dieudonné ring  $\mathbf{D}_k := W(k)[F, V]$  over  $k$  is the associative  $W(k)$ -algebra (non-commutative when  $k \neq \mathbf{F}_p$ ) generated by elements  $F$  and  $V$  subject to the relations*

$$FV = VF = p$$

$$F\alpha = \sigma(\alpha)F, \text{ and } \alpha V = V\sigma(\alpha), \text{ for all } \alpha \in W(k).$$

Elements of the Dieudonné ring  $\mathbf{D}_k$  have unique expressions as finite sums

$$a_0 + \sum_{j>0} a_j F^j + \sum_{j>0} b_j V^j, \text{ with } a_j, b_j \in W(k).$$

The centre of  $\mathbf{D}_k$  is  $\mathbf{Z}_p[F^n, V^n]$  when  $k = \mathbf{F}_{p^n}$ , and  $\mathbf{Z}_p$  otherwise (i.e., if  $k$  is infinite).

We now state the relationship between Dieudonné modules and finite commutative group schemes of  $p$ -power order over  $k$  (see [4, Theorem 1.4.3.2]).

**Theorem 10.5.** *There is an additive anti-equivalence of categories:*

$$\boxed{\begin{array}{l} \text{Finite commutative} \\ \text{group schemes } G/k \\ \text{of order } p^h, h \in \mathbf{N} \end{array}} \xrightarrow{G \mapsto \mathbf{M}(G)} \boxed{\begin{array}{l} \text{Left } \mathbf{D}_k\text{-modules } M \\ \text{of finite length } h \in \mathbf{N} \\ \text{over } W(k) \end{array}}$$

Writing  $\mathbf{M}(G)$  for the  $\mathbf{D}_k$ -module associated to  $G$ , we have the following.

1. If  $G$  has order  $p^h$ , then  $\mathbf{M}(G)$  has  $W(k)$ -length  $h$ .
2. The functor  $\mathbf{M}$  is functorial in the base field: given an inclusion  $i : k \hookrightarrow k'$ , we have

$$\mathbf{M}(G \times_k k') = \mathbf{M}(G) \otimes_{W(k)} W(k').$$

3. The relative Frobenius morphism  $F_{G/k} : G \rightarrow G^{(p)}$  corresponds to the linearisation

$$\mathbf{M}(F_{G/k}) : \mathbf{M}(G)^{(p)} = \sigma^*(\mathbf{M}(G)) \rightarrow \mathbf{M}(G).$$

and the Verschiebung morphism  $V_{G/k} : G^{(p)} \rightarrow G$  corresponds to the linearisation

$$\mathbf{M}(V_{G/k}) : \mathbf{M}(G) \rightarrow \sigma^*(\mathbf{M}(G)) = \mathbf{M}(G)^{(p)}.$$

4. The Cartier dual of  $G$  has associated Dieudonné module naturally isomorphic to the  $K_0/W(k)$ -dual of  $\mathbf{M}(G)$  equipped with  $F$  and  $V$  operators that are semi-linear dual to the  $V$  and  $F$  operators on  $\mathbf{M}(G)$  respectively.
5. The quotient  $\mathbf{M}(G)/F\mathbf{M}(G)$  is naturally isomorphic to the dual of the tangent space to  $G$  at the identity.

### 10.3 Some basic examples

To illustrate the correspondence between commutative group schemes of  $p$ -power order and their Dieudonné modules, we compute the correspondence explicitly for some groups of small order. A Dieudonné module, i.e. a left  $\mathbf{D}_k$ -module, is a  $W(k)$ -module equipped with actions of  $F$  and  $V$  satisfying the relations in Definition 10.4. We are interested in Dieudonné modules of finite length over  $W(k)$ . For  $k$  a finite field, we know that  $W(k)$  is the ring of integers of some unramified extension of  $\mathbf{Q}_p$ . In general,  $W(k)$  is a complete discrete valuation ring with residue field  $k$  and uniformiser  $p$ , so is a PID. (See e.g. [17, Section 2.5. Theorem 3].) By the classification of modules over a PID, every Dieudonné module with finite  $W(k)$ -length has as its underlying  $W(k)$ -module a finite direct sum of modules  $W/(p^{n_i})$ .

For the examples below we assume  $k$  is algebraically closed.

#### 10.3.1 Group schemes of order $p$

We first classify the commutative finite group schemes of order  $p$  over  $k$ . These must be in bijection with left  $\mathbf{D}_k$ -modules whose underlying  $W(k)$ -module is of length 1. The only  $W(k)$ -module  $M$  of length 1 is a line over  $W/(p) = k$ . Thus, to specify our  $\mathbf{D}_k$ -module it suffices to give actions of  $F$  and  $V$  on a basis element  $e$  of a  $k$ -line such that their product acts as multiplication by  $p$ . Suppose

$$Fe = \alpha e, \quad Ve = \beta e, \quad \text{for some } \alpha, \beta \in k.$$

By semilinearity, we have

$$FVe = \alpha\beta(\sigma)e;$$

the requirement that  $FV = p$  implies that at least one of  $\alpha$  and  $\beta$  must be zero. Conversely, if at least one of  $\alpha$  and  $\beta$  is zero, then the condition  $FV = VF = p$  is satisfied. So to specify the Dieudonné module with basis we need only give values  $\alpha, \beta \in k$ , at least one equal to zero.

Under a change of basis  $e' = \lambda e$ , with  $\lambda \in k^\times$ , by semilinearity  $\alpha$  and  $\beta$  become

$$\begin{aligned} \alpha' &= \frac{\sigma(\lambda)}{\lambda} = \lambda^{p-1}\alpha \\ \beta' &= \frac{\lambda}{\sigma(\lambda)} = \lambda^{-(p-1)}\beta. \end{aligned}$$

Since  $k$  is algebraically closed, we may thereby arrange by a change of basis that if one of  $\alpha$  and  $\beta$  is nonzero then it is in fact equal to 1. Thus we obtain three possibilities for the pair  $(\alpha, \beta)$  the pair may be  $(0, 0)$ ,  $(0, 1)$ , or  $(1, 0)$ . It is clear that these represent three distinct isomorphism classes of  $\mathbf{D}_k$ -module. To what groups do they correspond?

The relative Frobenius kills a connected order- $p$  group scheme, while its action on an étale group scheme has trivial kernel. Thus, the unique étale group scheme of order  $p$  (consisting of  $p$  reduced points with the group structure of  $\mathbf{Z}/(p)$ ) corresponds to  $(\alpha, \beta) = (1, 0)$ .

There are two well-known connected group schemes of order  $p$ , namely  $\mu_p$  and  $\alpha$ . The first,  $\mu_p$ , is the kernel of the  $p$ -th power map acting on the multiplicative group  $\mathbf{G}_m$ ; specifically, the scheme is  $\text{Spec } k[x]/(x^p - 1)$ , and the group law is multiplication. The second,  $\alpha_p$ , is that subgroup of the additive group  $\mathbf{G}_a$  cut out by the equation  $x^p = 0$ . The relative Frobenius kills both these groups; we need to distinguish them by the action of the Verschiebung. We will use Cartier duality.

The Cartier dual of  $\mu_p$  is  $\mathbf{Z}/(p)$ , which is étale, so its Verschiebung is nonzero. Thus,  $\mu_p$  corresponds to the pair  $(0, 1)$ . On the other hand, one can show that  $\alpha_p$  is its own Cartier dual, which is again infinitesimal, so  $\alpha_p$  corresponds to  $(0, 0)$ . (Alternatively, via the theory of the Verschiebung homomorphism that makes sense beyond the finite case, one can show that the Verschiebung homomorphism for  $\mathbf{G}_a$  vanishes, ultimately because its Frobenius is finite at, so this gives the conclusion for the subgroup scheme  $\alpha_p$  by functoriality.)

### 10.3.2 A group scheme of order $p^2$

We move on to order  $p^2$  killed by  $p$ . It is an elementary exercise in semi-linear algebra to show that there are three possibilities for the Dieudonné module of an infinitesimal group scheme with infinitesimal dual (i.e., the module is a  $k$ -vector space of dimension 2 on which  $V$  and  $F$  are each nilpotent). We focus here on deducing the one corresponding to  $p$ -torsion  $G = E[p]$  of a supersingular elliptic curve  $E$  over  $k$ . (In particular, we get the non-obvious conclusion that its isomorphism class is independent of the elliptic curve.)

Since  $G$  has order  $p^2$ , its Dieudonné module  $\mathbf{M}(G)$  has length 2. Since  $G$  is killed by  $p$ , by functoriality  $\mathbf{M}(G)$  is also killed by  $p$ . Thus the underlying  $W(k)$ -module of  $\mathbf{M}(G)$  is  $(W(k)/(p))^2$ . Again, all we need to do now is to determine the actions of  $F$  and  $V$  on  $(W(k)/(p))^2$ . The relative Frobenius on a smooth connected commutative group scheme of dimension 1 is a finite at morphism of degree  $p$ , so its kernel has order  $p$ . Thus  $F$  acts on  $\mathbf{M}(G)$  in such a way that its kernel has  $W$ -length 1, and similarly for  $V$  since  $n$ -torsion in an elliptic curve is self-dual (see [14] for an explanation). Since  $E$  is supersingular, the action of  $F$  on  $\mathbf{M}(G)$  is nilpotent, so (by some semilinear algebra) we can find a  $k$ -basis  $e_1, e_2$  of  $\mathbf{M}(G)$  such that

$$Fe_1 = e_2, \text{ and } Fe_2 = 0.$$

By the relation  $VF = p$ , we have  $Ve_2 = VFe_1 = 0$ ; and from  $FV = p$ , we know that  $Ve_1 = \alpha e_2$  for some  $\alpha \in k$ . Since the kernel of  $V$  has  $W(k)$ -length 1, the action of  $V$  on  $\mathbf{M}(G)$  is nonzero, so  $\alpha \neq 0$ . Since  $k$  is algebraically closed, by scaling the basis element  $e_1$ , we may assume that  $\alpha = 1$ . Thus, we have determined the Dieudonné module of our group scheme.

## 10.4 Dieudonné modules associated to abelian varieties

Let  $A$  be an abelian variety over  $k$  with dimension  $g \geq 1$ , and recall that the torsion group scheme  $A[p^n]$  is commutative and has rank  $p^{2ng}$ . We define the  $p$ -divisible group  $A[p^\infty]$  associated to  $A$  the  $p$ -divisible group

$$A[p^\infty] = \varinjlim A[p^n].$$

It is a  $p$  divisible group of height  $2g$ . Generally, for any  $p$ -divisible group  $G = (G_n)_{n \geq 1}$  over  $k$  with height  $h \geq 1$ , we let  $\mathbf{M}(G)$  denote the  $\mathbf{D}_k$ -module

$$\mathbf{M}(G) := \varprojlim \mathbf{M}(G_n).$$

Then by the same style of arguments used to work out the  $\mathbf{Z}_\ell$ -module structure of Tate modules of abelian varieties in characteristic  $\ell \neq p$  (resting on knowledge of the size of the  $\ell$ -power torsion subgroups of geometric points), we use  $W(k)$ -length to replace counting to infer that  $\mathbf{M}(G)$  is a free right  $W(k)$ -module of rank  $h$  with

$$\mathbf{M}(G)/p^r \mathbf{M}(G) \simeq \mathbf{M}(G_r), \text{ for all } r \geq 1.$$

The  $p$ -divisible group  $G$  is connected if and only if  $F$  is topologically nilpotent on  $\mathbf{M}(G)$  (since this is equivalent to nilpotence of  $F$  on each  $\mathbf{M}(G_r)$ ).

In analogy with the  $\ell$ -adic case we will now write  $T_p G$  for  $\mathbf{M}(G)$  and  $T_p A$  for the case  $G = A[p^\infty]$ . The  $\mathbf{D}_k$ -module  $T_p G$  will be the replacement for the  $\ell$ -adic Tate module in the “classical” case, even though it is contravariant in  $A$ ; its  $\mathbf{D}_k$ -action is the analogue of the Galois action on  $\ell$ -adic Tate modules, though this Dieudonné structure remains non-trivial when  $k$  is algebraically closed (whereas the Galois action on Tate modules is trivial for such  $k$ ).

Let  $K_0 := W(k)[1/p]$  be the fraction field of  $W(k)$ . For any  $p$ -divisible group  $G$  over  $k$ , let  $V_p G := \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_p G$  (and write  $V_p A$  for  $G = A[p^\infty]$ ). Then  $V_p G$  is an  $K_0$ -module of rank equal to the height  $h$  of  $G$ , and it also has a left module structure over the Laurent polynomial ring  $\mathbf{D}_k[1/p] = K_0[F, 1/F]$  that is non-commutative if  $k \neq \mathbf{F}_p$ .

**Theorem 10.6.** *Let  $A$  and  $B$  be abelian varieties over  $k$ , and  $A[p^\infty]$  and  $B[p^\infty]$  their associated  $p$ -divisible groups. Then the map*

$$\mathbf{Z}_p \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A, B) \rightarrow \mathrm{Hom}_{\mathbf{D}_k}(T_p B, T_p A) \quad (4)$$

is an injective of  $\mathbf{Z}_p$ -algebras; it is an isomorphism when  $k$  is finite.

Recall that the Tate module of  $A$  is defined to be

$$T_p A = \varprojlim \mathbf{M}(A[p^n]).$$

This is naturally a module over the noncommutative ring  $\mathbf{D}_k$ . Additionally, we define

$$V_p A = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_p A.$$

As in the  $\ell$ -adic case ( $\ell \neq p$ ), we find by a computation at finite level that  $T_p A$  is, as a  $W(k)$ -module, free of rank  $2g$ . The Tate theorem holds for  $T_p A$  as well: the natural map

$$\mathbf{Z}_p \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A, B) \rightarrow \mathrm{Hom}_{\mathbf{D}_k}(T_p B, T_p A) \quad (5)$$

is an isomorphism. The proof of injectivity is essentially the same as in the  $\ell$ -adic case (see Theorem 6.6): the argument for  $\ell \neq p$  carries through with the simplification that  $\mathrm{Hom}(A, B)$  is already known to be finitely generated (by the work with  $\ell \neq p$ ).

For the proof of surjectivity, we reduce to the case when  $A$  is  $k$ -simple by an argument similar to the one in the proof of Theorem 6.6. So, it is enough to prove that the map

$$\mathbf{Q}_p \otimes_{\mathbf{Z}} \mathrm{End}_k(A) \rightarrow \mathrm{End}_{\mathbf{D}_k[1/p]}(V_p(A))^{\mathrm{opp}} \quad (6)$$

is surjective for any  $k$ -simple abelian variety  $A$ . We start with the following result.

**Lemma 10.7.** *Let  $g \in K_0[x]$  be monic polynomial such that  $\deg(g) = d > 0$  and  $g(0) \neq 0$ . Let  $M := \mathbf{D}_k[1/p]/\mathbf{D}_k[1/p]g(F)$ . Then  $M$  is a left  $\mathbf{D}_k[1/p]$ -module which has dimension  $d$  as a left  $K_0$ -vector space.*

*Proof.* Working as in the commutative case, one can show that every element  $h \in \mathbf{D}_k[1/p]$  can be uniquely written as

$$h = \alpha \cdot g(F) + (c_0 + c_1 F + \cdots + c_{d-1} F^{d-1}), \text{ with } c_0, \dots, c_{d-1} \in K_0 \text{ and } \alpha \in \mathbf{D}_k[1/p].$$

The result then follows.  $\square$

**Exercise 10.8.** Show that  $I \subset \mathbf{D}_k[1/p]$  is a two-sided ideal if and only if there exists a polynomial  $g \in \mathbf{Q}_p[x]$  such that  $I = \mathbf{D}_k[1/p]g(F^n) = g(F^n)\mathbf{D}_k[1/p] = (g(F^n))$ .

**Lemma 10.9.** Let  $g(x) \in \mathbf{Q}_p[x]$  be an irreducible polynomial of degree  $m$  such that the field  $E := \mathbf{Q}[x]/(g)$  is a subfield of  $K_0$ . Let  $\pi \in E$  be a root of  $g$ ,  $r = n/m$  and  $\text{Gal}(K_0/\mathbf{Q}_p) = \langle \sigma \rangle$ , where  $\sigma$  is the automorphism lifting the arithmetic Frobenius. Let  $\Delta := \mathbf{D}_k[1/p]/(g(F^n))$ . Then, there is an isomorphism between  $\Delta$  and the cyclic  $E$ -algebra  $(K_0/E, \sigma^r, \pi)$ .

*Proof.* Since the degree of the residue field  $K_0 := W(k)[1/p]$  is  $n$ , the centre of  $\mathbf{D}_k[1/p]$  is  $\mathbf{Q}_p[F^n]$ . Therefore,  $\Delta := \mathbf{D}_k[1/p]/(g(F^n))$  is an algebra over  $\mathbf{Q}_p[F^n]/(g(F^n))$ . Writing

$$\mathbf{Q}_p[F^n]/(g(F^n)) = \mathbf{Q}_p[((F^r)^m)]/(g((F^r)^m)) = \mathbf{Q}_p[F'^m]/(g(F'^m)),$$

We see that the map

$$(E \rightarrow \mathbf{Q}_p[F'^m]/(g(F'^m)), \pi \mapsto F'^m)$$

is an isomorphism. This makes  $\Delta$  into a cyclic  $E$ -algebra, i.e.  $\Delta$  satisfies the relations

$$F'^m = \pi, F' \cdot x = \sigma^r(x) \cdot F', \text{ for } x \in K_0.$$

□

**Theorem 10.10.** Let  $h \in \mathbf{Q}_p[x]$  be a monic irreducible polynomial of degree  $n$  such that  $h(0) \neq 0$ . Let  $L := \mathbf{Q}_p[x]/(h)$  and  $D' := \mathbf{D}_k[1/p]/(h(F^n))$ . Then  $D'$  is a central simple  $L$ -algebra. More precisely, let  $E := \mathbf{Q}[x]/(g) = K_0 \cap L$ , where  $g(x) \in \mathbf{Q}_p[x]$  is an irreducible polynomial of degree  $m$ . Let  $\pi \in E$  be a root of  $g$ ,  $r = n/m$  and  $\text{Gal}(K_0/\mathbf{Q}_p) = \langle \sigma \rangle$ , where  $\sigma$  is the automorphism lifting the arithmetic Frobenius. Then,  $D'$  is isomorphic to  $M_r(\Delta)$ , where  $\Delta$  is the cyclic  $L$ -algebra  $\Delta := (K_0L/L, \sigma^r, \pi)$ .

*Proof.* Let  $\sigma : K_0 \rightarrow K_0$  is the cyclic automorphism lifting the geometric Frobenius on  $k = \mathbf{F}_q$ . Let  $E = K_0 \cap L$ , and denote by  $g$  the minimal polynomial of  $E$ . Let  $m = \deg(g)$  and  $r = n/m$ . Since the centre of  $D' := \mathbf{D}_k[F]/(h(F^n))$  is  $Z(D') := \mathbf{Q}_p[F^n]/(h(F^n))$ , which is isomorphic to  $L$ , we see that  $D'$  is indeed a central  $L$ -algebra. By Exercise 10.8, it is also simple since  $h$  is irreducible. By construction, we have  $E \subset L$ ; so the cyclic algebra  $\Delta_0 := (K_0/E, \sigma^r, \pi)$  is contained in  $D'$ . The field  $E$  is the maximal unramified subfield of  $L$  contained in  $K_0$ . So, since  $K_0$  and  $L$  have the same degree (over  $\mathbf{Q}_p$ ),  $L/E$  must be ramified. Therefore  $L/E$  doesn't split  $\Delta := \Delta_0 \otimes_E L$ , the base change of  $\Delta_0$  to  $L$ . So  $\Delta$  is the cyclic  $L$ -algebra  $\Delta = (LK_0/L, \sigma^r, \pi) \subseteq D'$ . By Wedderburn's theorem  $D' \simeq M_r(\Delta)$ . □

**Corollary 10.11.** Let  $h \in \mathbf{Q}_p[x]$  be a monic irreducible polynomial of degree  $n$  such that  $h(0) \neq 0$ . Let  $L := \mathbf{Q}_p[x]/(h)$ ,  $D' := \mathbf{D}_k[1/p]/(h(F^n))$ , and  $M$  a finite  $D'$ -module. Then, we have

$$\dim_{K_0} \text{End}_{K_0[F^n]}(M) = \dim_{\mathbf{Q}_p} \text{End}_{D'}(M),$$

*Proof.* Since  $D'$  is a simple  $L$ -algebra, it is enough to prove the statement for  $M$  a simple  $D'$ -module. So, from now on, assume that  $M$  is a simple  $D'$ -module. Then, the commutant of  $M$  is  $C = \text{End}_{D'}(M)$  and the bi-commutant of  $C$  is  $D' := \text{End}_C(M)$ . Now, observe that since  $\mathbf{D}_k[1/p] = K_0[F, 1/F] = K_0[F]$  and the centre of  $Z(\mathbf{D}_k[1/p]) = \mathbf{Q}_p[F^n]$ , the result follows from general properties of semi-simple modules. □

*Proof of Theorem 10.6.* Let  $D := \text{End}_k^0(A)$ , and recall that, by Albert classification theorem, the centre of  $D$  is  $Z = \mathbf{Q}[\pi_A]$ . To show that the map in (6) is surjective, we will make use of Corollary 10.11 and Proposition C.13. First, consider the algebra

$$D' := \text{End}_{\mathbf{D}_k[1/p]}(V_p(A))^{\text{opp}},$$

and recall that  $f_A \in \mathbf{Z}[x]$ , the characteristic polynomial of  $V_\ell(\pi_A)$ , is independent of  $\ell \neq p$ , and is the same for  $\ell = p$ . Also, since  $A$  is  $k$ -simple, we have  $f_A = g_A^r$ , where  $g_A$  is the minimal polynomial of  $\pi_A$  and  $r \geq 1$  an integer.

By functoriality of Dieudonné modules,  $V_p(\pi_A) = F^n$ . Therefore, the centre of  $D'$  is

$$Z(D') := \mathbf{Q}_p[F^n]/(g_A(F^n)) \simeq Z \otimes_{\mathbf{Q}} \mathbf{Q}_p.$$

We have the decomposition

$$\mathbf{Q}_p \otimes_{\mathbf{Q}} Z = \mathbf{Q}_p[x]/(g_A) = \prod_{v|p} \mathbf{Q}_p[x]/(g_{A,v}) = \prod_{v|p} Z_v,$$

where  $g_{A,v}$  is the minimal polynomial of  $Z_v$  over  $\mathbf{Q}_p$ . Up to isogeny, the group  $G := A[p^\infty]$  decomposes accordingly into a product  $G = \prod_{v|p} G_v$ , where  $G_v$  corresponds to the idempotent of  $Z_v$ . The module  $V_p(A)$  also decomposes accordingly as a sum of  $\mathbf{D}_k[1/p]$ -modules

$$V_p(A) \simeq \bigoplus_{v|p} V_p(G_v).$$

It follows that  $V_p(G_v)$  is a left module over the quotient algebra

$$D'_v = \mathbf{D}_k[1/p]/(g_{A,v}(F^n)).$$

There is a similar decomposition for the algebra  $\mathbf{Q}_p \otimes_{\mathbf{Q}} \text{End}_k^0(G)$ :

$$\mathbf{Q}_p \otimes_{\mathbf{Q}} \text{End}_k^0(G) = \prod_{v|p} \mathbf{Q}_p \otimes_{\mathbf{Q}} \text{End}_k^0(G_v).$$

So, it is enough to show that

$$\dim_{\mathbf{Q}_p} \mathbf{Q}_p \otimes_{\mathbf{Q}} \text{End}_k^0(G_v) = \dim_{\mathbf{Q}_p} \text{End}_{D'_v}(V_p(G_v)), \text{ for all } v | p.$$

However, by construction the field

$$L_v = K_0[x]/(g_{A,v}(x)) \simeq K_0[F^n]/(g_{A,v}(F^n)),$$

is a commutative sub-algebra of both algebras of dimension  $[D'_v : F_v]^{1/2}$ . So it is enough to prove that

$$\dim_{L_v} \mathbf{Q}_p \otimes_{\mathbf{Q}} \text{End}_k^0(G_v) = \dim_{L_v} \text{End}_{D'_v}(V_p(G_v)), \text{ for all } v | p.$$

Since  $L_v$  is maximal commutative, the result now follows from Corollary 10.11 and Proposition C.13.  $\square$

### 10.5 Local invariants associated to abelian varieties

Let  $k$  to be finite of size  $q$ , and  $A$  a  $k$ -simple abelian variety, and set  $D := \text{End}_k^0(A)$ . By Albert's classification,  $D$  is a division algebra with centre  $Z := \mathbf{Q}[\pi_A]$ .

Since the Dieudonné functor is fully faithful and contravariant, and the map in (4) is an isomorphism for finite fields  $k$ , as  $Z \otimes_{\mathbf{Q}} \mathbf{Q}_p$ -algebras, we have

$$D \otimes_{\mathbf{Q}} \mathbf{Q}_p = \text{End}_{\mathbf{D}_k[1/p]}(V_p A)^{\text{opp}}.$$

Now, recall the natural the decomposition

$$D \otimes_{\mathbf{Q}} \mathbf{Q}_p = \prod_{v|p} D \otimes_F F_v = \prod_{v|p} D_v.$$

It yields a corresponding decomposition of  $G := A[p^\infty]$  (up to isogeny) into a product of  $p$ -divisible groups over  $k$

$$G = \prod_{v|p} G_v,$$

where  $G_v$  is defined over  $Z_v$ . So, for each  $v | p$ , we have

$$D_v \simeq \text{End}_k^0(G_v) = \text{End}_{\mathbf{D}_k[1/p]}(V_p G_v)^{\text{opp}}.$$

Consequently, the right handside is a central simple  $Z_v$ -algebra. We now determine its invariant. Since the action of  $\pi_A$  decomposes accordingly to

$$V_p G = \bigoplus_{v|p} V_p G_v,$$

its characteristic polynomial factors as

$$g_A(x) = \prod_{v|p} g_{A,v}(x).$$

Since  $Z \otimes_F \mathbf{Q}_p$  maps to the centre  $Z(\mathbf{D}_k[1/p]) = \mathbf{Z}_p[F^n]/(g_A(F^n))$ , we see that, for all  $v | p$ ,

$$D_v := \mathbf{D}_k[1/p]/(g_{A,v}(F^n)).$$

By Theorem 10.10 and Theorem C.24, the class of  $D_v$  in  $\text{Br}(Z_v)$  is the same as that of the cyclic  $Z_v$ -algebra

$$\Delta_v = (K_0 Z_v / Z_v, \sigma', \pi^{f_v/g_v}),$$

where  $\sigma' \in \text{Gal}(K_0 Z_v / Z_v)$  is the arithmetic Frobenius and the element  $\pi^{f_v/g_v} \in Z_v^\times$  where  $f_v = f(v | p)$  and  $g_v = \text{gcd}(f_v, n)$ . Since  $[K_0 Z_v : Z_v] = n/g_v$ , the formula in Theorem C.24 gives

$$\text{inv}_v(D_v) = \frac{1}{n/g_v} \cdot v(\pi^{f_v/g_v}) = \frac{f_v}{n} v(\pi) \in \mathbf{Q}/\mathbf{Z}.$$

Let  $e_v = e(v | p)$ , so that  $e_v f_v = [Z_v : \mathbf{Q}_p]$ , we have

$$v(q) = n \cdot v(p) = n \cdot e_v,$$

so  $a = v(q)/e_v$ . This implies that

$$\text{inv}_v(D_v) = \frac{f_v}{n} v(\pi) = \frac{e_v f_v}{v(q)} v(\pi) = \frac{v(\pi)}{v(q)} \cdot [Z_v : \mathbf{Q}_p] \in \mathbf{Q}/\mathbf{Z}.$$



## 11 Honda–Tate’s theorem

### 11.1 Statement of main result

**Definition 11.1.** Let  $q = p^n$  with  $n \geq 1$  and integer and  $p$  prime number. Let  $F$  be a field of characteristic 0.

- (i) A Weil  $q$ -integer in  $F$  (or a Weil  $q$ -integer of weight 1) is an algebraic integer  $\alpha \in F$  whose  $\mathbf{Q}$ -conjugates in  $\mathbf{C}$  have absolute value  $q^{1/2}$ .
- (ii) Let  $w$  be an integer. A Weil  $q$ -number of weight  $w$  is an algebraic number  $\alpha$  such that  $\text{ord}_v(\alpha) = 0$  for all finite places  $v$  of  $\mathbf{Q}(\alpha)$  prime to  $q$  and  $|\tau(\alpha)| = q^{w/2}$  for all injective ring homomorphisms  $\tau : \mathbf{Q}(\alpha) \rightarrow \mathbf{C}$ .

We will denote by  $W(q)$  the set of conjugacy classes of all Weil  $q$ -numbers.

**Theorem 11.2** (Honda–Tate). Let  $k$  be a finite field of size  $q = p^n$ .

- (i) The following map is a bijection:

$$\boxed{\begin{array}{c} \text{Isogeny classes of} \\ \text{simple abelian} \\ \text{varieties } A/k \end{array}} \xrightarrow{A \mapsto \pi_A} \boxed{\begin{array}{c} \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\text{-conjugacy} \\ \text{classes of } q\text{-Weil} \\ \text{numbers } \pi \in \overline{\mathbf{Q}} \end{array}}$$

- (ii) Let  $A$  be a  $k$ -simple abelian variety, and set  $D := \text{End}_k^0(A)$  and  $F := \mathbf{Q}[\pi_A]$ , where  $\pi_A$  is the Frobenius endomorphism. Then, we have the following:

- (a)  $D$  is a totally definite algebra of centre of  $D$  is  $F = \mathbf{Q}(\pi_A)$ ;
- (b) We have  $2 \cdot \dim A = [D : F]^{1/2} [F : \mathbf{Q}]$ ;
- (c) For every finite place  $v \nmid p$  of  $F$ ,  $D$  splits at  $v$ ;
- (d) For every finite place  $v \mid p$  of  $F$ , we have

$$\text{inv}_v(D) = \frac{v(\pi_A)}{v(q)} [F_v : \mathbf{Q}_p] \pmod{1}, \quad (7)$$

where  $F_v$  denotes the completion of  $F$  at  $v$ .

We set

$$W_{\text{AV}}(q) := \{ \pi \in W(q) \mid [\pi] = [\pi_A] \text{ for some simple abelian variety } A/k \}.$$

Our goal is to show that  $W_{\text{AV}}(q) = W(q)$ .

### 11.2 Examples

Let  $\pi \in W(q)$  be a Weil  $q$ -integer, where  $q = p^n$ , with  $n \in \mathbf{Z}_{\geq 1}$ .



### 11.2.1 The totally real case

Assume  $F = \mathbf{Q}[\pi]$  has a real embedding. Then by Albert’s classification (Theorem 7.1),  $F$  is totally real. Therefore, by Theorem 7.2, we have  $\pi = \sqrt{q}$  or  $\pi = -\sqrt{q}$ , in which case it appears with even multiplicity. There are two possible cases to consider.

- (1) **Case:  $n$  is even.** In that case, we have  $F = \mathbf{Q}$ . By (7), we have  $\text{inv}_p(D) = 1/2$ . So  $D$  is a division quaternion algebra over  $\mathbf{Q}$  ramified at  $p$  and  $\infty$ . The formula

$$2 \dim A = [D : F]^{1/2} [F : \mathbf{Q}]$$

implies that  $\dim A = 1$ . Since  $D = \text{End}_k^0(A)$ ,  $A$  is a supersingular elliptic curve. Clearly, the characteristic polynomial of  $f_A \in \mathbf{Z}[x]$  is of the form  $f_A = (x - p^{n/2})^2$ .

- (2) **Case:  $n$  is odd.** In that case, we have  $F = \mathbf{Q}(\pi) = \mathbf{Q}(p^{1/2})$ . In other words,  $F$  is a real quadratic field. Hence, it has two real places at which  $\text{inv}_v(D) = 1/2$  ( $v \mid \infty$ ). Since there is only one place  $v$  of  $F$  dividing  $p$ , and

$$\sum_v \text{inv}_v(D) = 0 \in \text{Br}(F),$$

we must have  $\text{inv}_v(D) = 0$ , for  $v \mid p$ , meaning that  $D$  is a definite quaternion algebra ramified at  $v \mid \infty$  only. From this, we see that  $\dim A = 2$ . By Theorem 7.2, the characteristic polynomial  $f_A$  of  $\pi_A \in \mathbf{Z}[x]$  is of the form

$$f_A(x) = ((x - p^{n/2})(x + p^{n/2}))^2 = (x^2 - p^n)^2 = g(x^2),$$

where  $g(x) = (x - p^n)^2$ . Let  $k'$  be the quadratic extension of  $k$ . By Case (1), there exists a supersingular elliptic curve  $A'/k'$  such that  $f_{A'} = g$ . By Corollary A.3, we see that  $A$  is  $k'$ -isogenous to  $\text{Res}_{k'/k}(A')$ .

### 11.2.2 Totally imaginary case

By Theorem 7.2, both  $\pi$  and  $\bar{\pi} = \pi/q$  are roots of  $f_A$ . In that case,  $F_0 = \mathbf{Q}(\pi + \pi/q)$  is a totally real field, and  $F/F_0$  is a CM extension. Let  $\alpha \mapsto \bar{\alpha}$  the complex conjugation of  $F/F_0$ . Since  $F$  is CM, the division algebra  $D$  splits at all the places  $v \nmid p$  of  $F$ . For each place  $v \mid p$  of  $F$ , since  $\pi\bar{\pi} = q$ , we have  $v(\pi) + v(\bar{\pi}) = v(q)$ . Therefore, since  $[F_v : \mathbf{Q}_p] = [F_{\bar{v}} : \mathbf{Q}_p]$ , we have

$$\text{inv}_v(D) + \text{inv}_{\bar{v}}(D) = 0 \pmod{1}, \text{ if } v \neq \bar{v}, \quad (8)$$

$$\text{inv}_v(D) = 0 \pmod{1}, \text{ if } v = \bar{v}. \quad (9)$$

Let  $e_v$  and  $f_v$  be the inertia and residue degrees of  $F$  at  $v \mid p$ , respectively. Then, we have

$$\text{inv}_v(D) = \frac{v(\pi_A)}{v(q)} [F_v : \mathbf{Q}_p] = \frac{v(\pi_A)e_v f_v}{n} \pmod{1}.$$

Therefore, if  $n \mid v(\pi_A)e_v$  for all  $v \mid p$ ,  $D$  splits at all places of  $F$ , meaning that  $D = F = \text{End}_k^0(A)$  is commutative. This is the case when  $k = \mathbf{F}_p$  is the prime field.

*Proof of Theorem 11.2. Uniqueness:* Let  $A$  and  $B$  be two  $k$ -simple abelian varieties such that  $\pi_A$  and  $\pi_B$  are  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ -conjugate. Then,  $\pi_A$  and  $\pi_B$  have the same minimal polynomial  $h \in \mathbf{Z}[x]$ . Let  $f_A$  and  $f_B$  be the characteristic polynomials of  $\pi_A$  and  $\pi_B$ , respectively. Since  $A$  and  $B$  are simple, there exist integers  $r, s \geq 1$  such that  $f_A = h^r$  and  $f_B = h^s$ . Without loss of generality, we may assume that  $r \leq s$ . This means that  $f_A$  divides  $f_B$ . Therefore, by [14, Theorems 2 and 3, Appendix I], we see that  $B$  is isogenous to an abelian subvariety of  $A$  over  $k$ . Since  $A$  and  $B$  are  $k$ -simple, this inclusion must be an isogeny.

**Structure of  $D := \text{End}_k^0(A)$ :** Let  $G_k := \text{Gal}(\overline{k}/k)$ . Tate’s isogeny theorem implies that

$$\begin{aligned} D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell &\simeq \mathbf{Q}_\ell \otimes_{\mathbf{Q}} \text{End}_{G_k}(V_\ell A), & \text{if } \ell \neq p; \\ D \otimes_{\mathbf{Q}} \mathbf{Q}_p &\simeq \mathbf{Q}_p \otimes_{\mathbf{Q}} \text{End}_{\mathbf{D}_k[1/p]}(V_p A)^{\text{opp}}, & \text{if } \ell = p. \end{aligned}$$

By Theorem C.21,  $D$  is determined by its local structures. Therefore,  $D$  is also determined by  $f_A$ . We compute these local structures using the results of Section 10.5.  $\square$

### 11.3 Proof of Theorem 11.2: Existence

**Lemma 11.3.** *Let  $\pi \in W(q)$ , and  $m \geq 1$  an integer. If  $\pi^m \in W_{\text{AV}}(q^m)$ , then  $\pi \in W_{\text{AV}}(q)$ .*

*Proof.* Let  $k'$  be an extension of  $k$  of degree  $m$ , and  $A'/k'$  an abelian variety such that  $[\pi^m] = [\pi_{A'}]$ . Let  $A$  be the abelian variety over  $k$  which is the restriction of scalars of  $A'$ . Let  $\ell$  be a prime,  $\ell \neq p$ . By Theorem A.2, we have as  $\mathbf{Q}_\ell[G_k]$ -modules (with  $G_k = \text{Gal}(\overline{k}/k)$  for a separable closure  $\overline{k}/k'$ ) we have

$$V_\ell A = \text{Ind}_{G_{k'}}^{G_k} V_\ell A'.$$

So by Corollary A.3, we see that  $f_A(x) = f_{A'}(x^m)$ . Since  $\pi$  is a root of  $f_A$ , this implies that  $[\pi] = [\pi_{A_1}]$ , where  $\pi_{A_1}$  is the Frobenius of some  $k$ -simple factor  $A_1$  of  $A$ .  $\square$

Let  $\pi$  be a Weil  $q$ -integer, and  $D$  be the division algebra obtained from  $\pi$  and the local information in Theorem 11.2. Note that, by Theorem C.21, such a  $D$  indeed exists and is unique up to isomorphism.

**Lemma 11.4.** *There exists a CM field  $E$  containing  $F = \mathbf{Q}(\pi)$  such that  $E$  splits  $D$  and such that  $[E : F] = [D : F]^{1/2}$ .*

*Proof.* Let  $E \subset D$  be a maximal commutative sub-algebra of  $D$  given in Proposition C.13. Then  $[E : F] = [D : F]^{1/2}$  and  $E$  splits  $D$ . Since  $D$  is totally definite,  $E$  must be a CM field.  $\square$

*Proof of existence in Theorem 11.2.* by using Lemma 11.4, choose a CM extension  $E/F$  contained in  $D$ . By Theorem B.2, let  $K/\mathbf{Q}_p$  be a finite extension, and  $B/K$  an abelian variety with CM by  $E$  such that the reduction  $B_0$  of  $B$  at the maximal ideal in  $\mathcal{O}_K$  has Frobenius endomorphism  $[\pi_0] = [\pi_A^m]$ , for some integer  $m \geq 1$ . Then apply Lemma 11.3 to conclude the proof of Theorem 11.2.  $\square$

## A Weil restriction of an abelian variety

Let  $k$  be a field and  $k'$  a finite Galois extension of  $k$ .

Let  $V/k'$  be an variety. Then for any  $k$ -algebra  $R$ , set

$$F_V(R) := V(k' \otimes_k R) = \text{Hom}(\text{Spec}(R \otimes_k k'), V).$$

In particular, we see that

$$F_V(k) = V(k' \otimes_k k) = V(k').$$

One can see that

$$\begin{aligned} F_V : k\text{-Alg} &\rightarrow \mathbf{Sets} \\ R &\mapsto F_V(R). \end{aligned}$$

is a functor.

**Theorem A.1.** *The functor  $F_V$  is representable by a variety defined over  $k$ , denoted by  $\text{Res}_{k'/k}(V)$ , and called the Weil restriction of  $V$  from  $k'$  to  $k$ . It has the universal property that, for any  $k$ -algebra  $R$ , we have*

$$\text{Res}_{k'/k}(V)(R) = V(R \otimes_k k').$$

If  $V$  is an abelian variety over  $k'$ , then  $\text{Res}_{k'/k}(V)$  is an abelian variety defined over  $k$ .

*Proof.* See Weil [24, Chapter I, Section 1.3]. □

**Theorem A.2.** *Let  $k$  be a field and  $k'$  a finite extension of  $k$ . Let  $G_k := \text{Gal}(\bar{k}/k)$  and  $G_{k'} := \text{Gal}(\bar{k}/k')$  be the absolute Galois groups of  $k$  and  $k'$ , respectively. Let  $A$  be an abelian variety defined over  $k'$  and  $\ell \neq \text{char}(k)$ . Then, we have*

$$T_\ell(\text{Res}_{k'/k}(A)) = \text{Ind}_{G_{k'}}^{G_k} T_\ell(A).$$

*Proof.* This follows from the functorial properties of Weil restriction. □

**Corollary A.3.** *Let  $k$  be a finite field of size  $q = p^n$ , where  $p$  is prime and  $n \geq 1$  an integer. Let  $k'$  a finite extension of  $k$  of degree  $r$ . Let  $A$  be an abelian variety defined over  $k'$ , and  $B := \text{Res}_{k'/k}(A)$ . Let  $\pi_A$  and  $\pi_B$  be the Frobenius endomorphisms of  $A$  and  $B$ , respectively. Let  $g_A$  and  $g_B$  be the minimal polynomial of  $\pi_A$  and  $\pi_B$ , respectively. Then, we have  $\pi_B = \pi_A^r$  so that  $g_B(x) = g_A(x^r)$ .*

Moreover, let  $F \subset \text{End}_{k'}^0(A)$  and  $E \subset \text{End}_k^0(B)$  be their respective centres. Then, under the extension of scalar ( $F \rightarrow E, \pi_A \mapsto \pi_B^r$ ), we have an isomorphism

$$E \otimes_F \text{End}_{k'}^0(A) \simeq \text{End}_k^0(B).$$

*Proof.* This follows from Theorem A.2. □

## B CM lifting of abelian varieties

**Lemma B.1.** *Let  $F$  be a totally real field and  $E/F$  a CM extension. Let  $\pi$  be a Weil  $q$ -integer in  $E$  and  $\pi_0$  a Weil  $q_0$ -integer in  $E$  which satisfy*

$$\frac{w(\pi)}{w(q)} = \frac{w(\pi_0)}{w(q_0)}, \text{ for all places } w \text{ of } E.$$

*Then there exist positive integers  $m$  and  $m_0$  such that  $\pi^m = \pi_0^{m_0}$ .*

*Proof.* Replacing  $\pi$  and  $\pi_0$  by appropriate powers, if necessary, we may assume that  $q = q_0$ , so that

$$w(\pi) = w(\pi_0), \text{ for each place } w \mid p \text{ of } E.$$

For each finite place  $w \nmid p$  of  $E$ , it then follows that both  $\pi$  and  $\pi_0$  are units since they divide a power of  $p$ . At the infinite places,  $\pi$  and  $\pi_0$  have the same absolute value  $|\pi| = |\pi_0| = q^{1/2}$ . Therefore, we have

$$\left| \frac{\pi}{\pi_0} \right|_w = 1, \text{ for each place } w \text{ of } E.$$

This means that  $\pi/\pi_0$  is a root of unity. So there exists an integer  $s \geq 1$  such that  $(\pi/\pi_0)^s = 1$ , and the lemma follows.  $\square$

**Theorem B.2.** *Let  $E$  be a CM field containing  $F = \mathbf{Q}(\pi)$  which splits  $D$ . Then there exist a finite extension  $K/\mathbf{Q}_p$  and an abelian variety  $A$  defined over  $K$  such that*

- (i)  $A$  has good ordinary reduction;
- (ii) The geometric Frobenius of the reduction of  $A$  is conjugate to a power  $\pi^m$  of  $\pi$ ;
- (iii)  $[E : \mathbf{Q}] = 2 \dim A$ .

The proof of Theorem B.2 requires some preparation. We start by recall the results need from the theory of complex multiplication.

Let  $E$  be a CM field with  $[E : \mathbf{Q}] = 2g$ . Let  $\tau$  be the automorphism of  $E$  of order 2 which is induced by complex conjugation for each embedding  $E \hookrightarrow \mathbf{C}$ . Intrinsically,  $\tau$  is the unique nontrivial automorphism of  $E$  over its maximal totally real subfield. Let  $\Phi$  be a CM type for  $E$ , i.e.  $\Phi$  is a subset of  $\text{Hom}_{\mathbf{Q}\text{-alg}}(E, \mathbf{C})$  such that

$$\Phi \cap \Phi\tau = \emptyset, \text{ and } \Phi \sqcup \Phi\tau = \text{Hom}(E, \mathbf{C}). \quad (10)$$

**Definition B.3.** *An abelian variety  $A$  over a subfield  $F \subset \mathbf{C}$  is of type  $(E, \Phi)$ , if  $A$  satisfies the conditions of Theorem B.2 over  $F$ , and the action of  $\mathbf{C} \otimes_{\mathbf{Q}} E$  on the tangent space  $\text{Lie}(A \times_F \mathbf{C})$  is through the decomposition*

$$\mathbf{C} \otimes_{\mathbf{Q}} E = \prod_{\phi \in \Phi} \mathbf{C}$$

(where  $E$  acts on  $\phi$ -th component of the product through the embedding  $\phi : E \hookrightarrow \mathbf{C}$ ).

**Theorem B.4.** *There exist a number field  $K/\mathbf{Q}$ , and an abelian scheme  $A$  defined over the ring of integers  $\mathcal{O}_K$  of  $K$ , which is of type  $(E, \Phi)$ .*

*Proof.* The proof of this result is explained in Tate [21, Lemma 4]. It combines results from Serre–Tate [18, §§6.2 and 12.4] and Shimura–Taniyama [19, Theorem 7].  $\square$

From now, we fix an identification  $\overline{\mathbf{Q}}_p \simeq \mathbf{C}$ . For each place  $w \mid p$  of  $E$ , we let  $E_w$  be the completion of  $E$  with respect to  $w$ . We identify  $\text{Hom}_{\mathbf{Q}_p}(E_w, \mathbf{C})$  with its image in  $\text{Hom}(E, \mathbf{C})$  which we denote by  $H_w$ . Let  $\Phi_w := \Phi \cap H_w$ . We have a decomposition

$$\mathbf{Q}_p \otimes_{\mathbf{Q}} E = \prod_{w \mid p} E_w$$

and the disjoint unions

$$\text{Hom}(E, \mathbf{C}) = \bigsqcup_{w \mid p} H_w \text{ and } H_w = \bigsqcup_{w \mid p} \Phi_w. \quad (11)$$

**Lemma B.5.** *Let  $K/\mathbf{Q}_p$  be a finite extension, with ring of integers  $\mathcal{O}_K$ , and  $A$  an abelian scheme of type  $(E, \Phi)$  defined over  $\mathcal{O}_K$ . Let  $k_0$  be the residue field of  $\mathcal{O}_K$ , with  $q_0 = \#k_0$ . Let  $A_0$  be the reduction of  $A$  modulo the maximal ideal of  $\mathcal{O}_K$ . Then there exists an element  $\pi_0 \in E$  such that  $i(\pi_0) \in \text{End}(A)$  induces the Frobenius  $\pi_{A_0} \in \text{End}_k^0(A_0)$ , and we have*

$$\frac{w(\pi_0)}{w(q_0)} = \frac{\#\Phi_w}{\#H_w}, \text{ for all } w \mid p.$$

*Proof.* See Shimura and Taniyama [19].  $\square$

*Proof of Theorem B.2.* Keeping the above notations, assume that  $\pi$ ,  $q$ ,  $F$ ,  $D$  and  $E$  satisfy the hypotheses of Theorem B.2. Let  $z \mapsto z^\tau$  be the complex conjugation on  $E$ . We will now show how we can choose the set  $\Phi$  such that we have

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#H_w}, \text{ for each place } w \text{ of } E \text{ with } w \mid p.$$

Let  $w \mid p$  be a place of  $E$ ,  $v$  be the place of  $F$  below  $w$ , and define  $n_w \in \mathbf{Q}_{\geq 0}$  by

$$n_w = \frac{w(\pi)}{w(q)} \#H_w = \frac{w(\pi)}{w(q)} [E_w : \mathbf{Q}_p] = \frac{v(\pi)}{v(q)} [E_w : F_v][F_v : \mathbf{Q}_p].$$

Since  $E$  splits  $D$ , we see that  $\text{inv}_w(D \otimes_F E) = 0$ . By properties of local invariants and (7), we also have

$$\text{inv}_w(E \otimes_F D) = [E_w : F_v] \frac{v(\pi)}{v(q)} [F_v : \mathbf{Q}_p] = n_w \in \mathbf{Q}/\mathbf{Z}.$$

Therefore,  $n_w$  must be a non-negative integer. Since  $\pi\pi^\tau = q$ , we see that

$$n_w + n_{\tau w} = \#H_w = \#H_{\tau w}. \quad (12)$$

Since  $\tau$  is the CM involution of  $E/F$ , it acts without a fixed point on the partition in (11) and such that  $H_{\tau w} = \tau \cdot H_w$ . Therefore, for any sequence of non-negative integers  $n_w$  satisfying (12), we can choose a CM type  $\Phi = \bigsqcup_w \Phi_w$  such that  $\#\Phi_w = n_w$  which satisfies (11) as follows: First,

we consider the places  $w \mid p$  fixed by  $\tau$ , then we consider the pairs of places  $(w, \tau w)$  where  $w \neq \tau w$ . Given such a CM type  $\Phi$ , the condition

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#H_w}$$

is satisfied by construction.

By Theorem B.4, there exists an abelian scheme of type  $(E, \Phi)$  defined over  $\mathcal{O}_K$ . By Lemma B.5, there exists a Weil  $q_0$ -number  $\pi_0 \in E$  which is conjugate to the Frobenius  $\pi_{A_0}$  of the reduction  $A_0$  of  $A$  such that

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#H_w} = \frac{w(\pi_0)}{w(q_0)}.$$

Replacing  $K/\mathbf{Q}$  by an unramified extension of degree  $m$  leads to  $\pi_0$  being replaced by  $\pi_0^m$ . We then conclude the proof of Theorem B.2 by using Lemma B.1.  $\square$

## C Background on non-commutative algebra

### C.1 Semi-simple modules

In this subsection, all rings have an identity element. A ring homomorphism is a map  $f : A \rightarrow B$  such that

1.  $f(x + y) = f(x) + f(y)$ , for all  $x, y \in A$ ;
2.  $f(x \cdot y) = f(x) \cdot f(y)$ , for all  $x, y \in A$ ;
3.  $f(1_A) = 1_B$ .

If  $A$  is a ring then, we let  $A^{\text{opp}}$  denotes the opposite ring and  $Z(A)$  the center of  $A$ . For a integer  $r \geq 0$ , we let  $M_r(A)$  be the ring of  $r \times r$  matrices with coefficients in  $A$ .

Let  $A$  be a ring, and  $M$  a non-zero left (resp. right)  $A$ -module.

- a) We say that  $M$  is an *irreducible* (or *simple*)  $A$ -module if the only left (resp. right)  $A$ -submodules of  $M$  are  $\{0\}$  and  $M$  itself.
- b) We say that  $M$  is a *semisimple* left (resp. right)  $A$ -module if every left (resp. right)  $A$ -submodule of  $M$  is a direct summand.

**Lemma C.1.** *Let  $A$  be a ring, and  $M$  a non-zero left (resp. right)  $A$ -module. Then  $M$  is semisimple if and only if there exists an finite set of simple  $A$ -modules  $(M_i)_{i \in I}$  such that  $M$  a direct sum*

$$M = \bigoplus_{i \in I} M_i.$$

Note that the zero module is semisimple but not simple; by convention it is the direct sum of the empty collection of  $A$ -modules.

Let  $A$  be nonzero ring.

- a) We say that  $A$  is *simple* (as a ring) if the only two-sided ideals of  $A$  are  $\{0\}$  and  $A$  itself.
- b) A ring  $A$  is called *semisimple* if every left (resp. right)  $A$ -module is semisimple.

**Lemma C.2.** *Let  $A$  be nonzero ring. Then  $A$  is semisimple if and only if  $A$  is semisimple as a left (resp. right)  $A$ -module.*

Let  $A$  be a semisimple ring. Then, there exists has finitely many minimal nonzero ideals  $A_1, \dots, A_r \subset A$ . Each ideal  $A_i$  is also a ring, with an identity element making it a simple ring. Thus  $A$  is isomorphic to the product  $A_1 \times \dots \times A_r$ . So every semisimple ring is a product of finitely many simple rings. Conversely, every finite product of simple rings is semisimple.

**Proposition C.3.** *Let  $A$  be a semisimple ring. Then, up to isomorphism, there are finitely many simple  $A$ -modules.*

*Proof.* Since  $A$  is a semisimple ring, every left ideal  $I \subset A$  (resp. right ideal  $J \subset A$ ) is generated by an idempotent, i.e., there is an idempotent  $e \in A$  with  $I = Ae$  (resp.  $J = eA$ ). Indeed, because  $A$  is semisimple as a left (resp. right) module over itself there exists a left ideal  $I'$  (resp. right ideal  $J'$ ) such that  $A = I \oplus I'$  as left  $A$ -modules (resp.  $A = J \oplus J'$  as right  $A$ -modules); writing  $1 = e + e'$  one easily finds that  $e$  is an idempotent and  $I = Ae$  (resp.  $J = eA$ ). If  $A$  is a simple ring then up to isomorphism there is a unique simple  $A$ -module. It follows that, up to isomorphism, there are finitely many simple modules over  $A$ ; one corresponding to each simple factor  $A_i$ .  $\square$

Let  $A$  be a simple ring, and  $M$  a simple  $A$ -module. The ring  $D := \text{End}_A(M)$  is a division algebra. We called  $D$  the *commutant* of  $A$ , and  $\text{End}_D(M)$  its *bi-commutant*. For  $a \in A$ , let  $a_M \in \text{End}_D(M)$  be the map ( $M \rightarrow M, m \mapsto am$ ). Then, we have a map

$$\begin{aligned} A &\rightarrow \text{End}_D(M) \\ a &\mapsto a_M. \end{aligned}$$

**Lemma C.4.** *Let  $A$  be a simple ring,  $M$  a simple  $A$ -module and  $D = \text{End}_A(M)$ . Then, the map  $a \mapsto a_M$  is an isomorphism of  $A$  onto its bi-commutant  $\text{End}_D(M)$ .*

**Corollary C.5** (Wedderburn). *Let  $A$  be a simple ring. Then, there exist an integer  $r \geq 1$  and a division algebra  $D$  such that  $A \simeq M_r(D)$ , where  $M_r(D)$  is the ring of  $r \times r$  matrices over  $D$ . In particular,  $Z(A) = Z(D)$  is a field.*

*Proof.* Let  $M$  be a simple  $A$ -module. Then we see that  $A$  has finite length  $r$  as a left module over itself. So,  $A$  is isomorphic to  $M^r$  as  $A$ -modules. From this and the lemma above, it follows that  $A \simeq M_r(D)$ .  $\square$

Conversely, if  $D$  is a division algebra and  $r$  is a positive integer,  $M_r(D)$  is a simple ring. The unique simple module over this ring is given by  $D^r$  with its natural structure of a left  $M_r(D)$ -module. It follows from the discussion that if  $A$  is a simple ring, so is  $A^{\text{opp}}$ .

**Theorem C.6** (Bi-commutant). *Let  $A$  be a semisimple ring, and let  $M$  be an  $A$ -module of finite type. Let  $C := \text{End}_A(M)$ , and consider  $M$  as a left module over  $C$  by the rule*

$$c \cdot m = c(m), \text{ for } c \in C \text{ and } m \in M.$$

*Then the map ( $A \rightarrow \text{End}_C(M), a \mapsto a_M$ ) is an isomorphism.*

**Theorem C.7** (Skolem-Noether). *Let  $A$  be a simple algebra with center  $K$ . Let  $B$  and  $B'$  be simple  $K$ -subalgebras of  $A$  of finite dimension over  $K$ . Then for every isomorphism  $\varphi : B \rightarrow B'$  of  $K$ -algebras there is an inner automorphism  $\psi$  of  $A$  with  $\varphi = \psi|_B$ .*

In particular, if  $A$  is a simple algebra of finite dimension over its centre  $K$  then all automorphisms of  $A$  over  $K$  are inner, so  $\text{Aut}_K(A) = \text{Inn}(A) \simeq A^\times / K^\times$ .

## C.2 Brauer group

We let  $K$  be a field.

**Definition C.8.** A central simple algebra over  $K$  is a  $K$ -algebra  $A$  such that

- (a)  $A$  is finite dimensional over  $K$ .
- (b)  $K$  is the centre of  $A$ .
- (c)  $A$  is a simple ring.

If in addition  $A$  is a division algebra, we call it a central division algebra over  $K$ .

**Theorem C.9.** Let  $A$  be a  $K$ -algebra of finite dimension. Then, the following are equivalent

- (i)  $A$  is a simple central;
- (ii) There is a canonical homomorphism of  $K$ -algebras

$$\begin{aligned} A \otimes_K A^{\text{opp}} &\rightarrow \text{End}_K(A) \\ a \otimes a' &\mapsto (x \mapsto axa') \end{aligned}$$

is a bijection;

- (iii) There exist a field extension  $L/K$  and an integer  $n \geq 1$  such that  $A \otimes_K L$  is isomorphic to  $M_n(L)$ ;
- (iv) For any separable closure  $K_s$  of  $K$ , there exists an integer  $n \geq 1$  such that the  $K_s$ -algebras  $A \otimes_K K_s$  and  $M_n(K_s)$  are isomorphic;
- (v) There exists a finite Galois extension  $L$  of  $K$  and an integer  $n \geq 1$  such that  $A \otimes_K L$  and  $M_n(L)$  are isomorphic;
- (vi) There exists a division  $K$ -algebra  $D$  of finite dimension and an integer  $n \geq 1$  such that  $A$  is isomorphic to the matrix algebra  $M_n(D)$ .

*Proof.* See Bourbaki [2, §14, Theorem 1]. □

**Corollary C.10.** Let  $A$  be a central simple algebra of finite dimension over an algebraically closed field  $K$ . Then, there exists an integer  $n \geq 1$  such that  $A$  is isomorphic to the matrix algebra  $M_n(K)$ .

**Corollary C.11.** Let  $A$  be a central simple  $K$ -algebra of finite dimension. Then, there exists an integer  $n \geq 1$  such that  $[A : K] = n^2$ .

*Proof.* By Theorem C.9, there exist an extension  $L$  of  $K$  and an integer  $n \geq 1$  such that the algebra  $A \otimes_K L$  and  $M_n(L)$  are isomorphic. Therefore, we have

$$[A : K] = [A \otimes_K L : L] = [M_n(L) : L] = n^2.$$

□

**Corollary C.12.** Let  $A$  be a central simple algebra over  $F$ .

- (a) For any field extension  $K/F$ ,  $A \otimes_F K$  is a central  $K$ -algebra.



(b) If  $B$  is another  $F$  central simple algebra, then  $A \otimes_F B$  is a central simple  $F$ -algebra.

*Proof.* □

**Proposition C.13.** *Let  $A$  be a simple central  $K$ -algebra of finite degree, and  $L$  a semi-simple commutative sub-algebra. Then, the following conditions are equivalent:*

(i)  $L$  is a maximal commutative sub-algebra of  $A$ ;

(ii) The  $L$ -module  $A$  is free of dimension  $[L : K]$ ;

(iii) We have  $[A : K] = [L : K]^2$ .

Suppose that, in addition,  $A$  is the algebra  $\text{End}_K(V)$ , where  $V$  is a vector space of finite dimension  $n \geq 1$  over  $K$ . Then, the conditions (i)–(iii) are also equivalent to

(iv)  $V$  est un  $L$ -module libre de dimension 1.

*Proof.* See Bourbaki [2, §14, Proposition 3]. □

**Proposition C.14.** *Let  $A$  and  $B$  be central simple  $K$ -algebras of finite dimension. Then, the following are equivalent:*

(i) There exists an integer  $t \geq 1$  such that the  $K$ -algebra  $A \otimes_K B^{\text{opp}}$  is isomorphic to the matrix algebra  $M_t(K)$ ;

(ii) There exist integers  $r, s \geq 1$  such that the  $K$ -algebras  $A \otimes_K M_r(K)$  and  $B \otimes_K M_s(K)$  are isomorphic;

(iii) There exists a division algebra  $D$  over  $K$  and integers  $m, n \geq 1$  such that  $A$  is isomorphic to  $M_m(D)$  and  $B$  to  $M_n(D)$ .

*Proof.* See Bourbaki [2, §15, Proposition 3]. □

Let  $A$  and  $B$  be finite dimensional central simple  $K$ -algebras. We say that  $A$  and  $B$  are *equivalent*, and write  $A \sim B$ , if one of the equivalent conditions in Theorem C.9 is satisfied. We write  $[A]$  for the equivalence class of  $A$ .

**Lemma C.15.** *Let  $A, A'$  and  $B$  be central simple  $K$ -algebras of finite dimension. Then,  $[A] = [A']$  implies that  $[A \otimes_K B] = [A' \otimes_K B]$ .*

*Proof.* This follows from Proposition C.14 (ii). □

By Lemma C.15, setting

$$[A][B] := [A \otimes_F B].$$

gives a well-defined composition law on the set of equivalent classes of simple central  $K$ -algebras of finite dimension.

**Definition C.16.** *The Brauer group of  $F$ , denoted by  $\text{Br}(F)$ , is the set of equivalence classes of central simple  $K$ -algebras. It is an abelian group, where  $-[A] = A^{\text{opp}}$ . (We recall that  $A^{\text{opp}}$  is the opposite algebra.)*

Let  $K'/K$  be a field extension. Then, by Proposition C.14, by extension of scalars, one obtains a group homomorphism

$$\mathrm{Br}(K) \rightarrow \mathrm{Br}(K').$$

As a result, the map  $K \mapsto \mathrm{Br}(K)$  is a covariant functor in  $K$ . We have

$$\mathrm{Br}(K) = \coprod_{K'/K \text{ Galois}} \mathrm{Br}(K'/K),$$

where we set  $\mathrm{Br}(K'/K) := \ker(\mathrm{Br}(K) \rightarrow \mathrm{Br}(K'))$ .

**Proposition C.17.** *Let  $K'/K$  be a finite Galois extension. Then, we have an isomorphism  $\mathrm{Br}(K'/K) \simeq \mathrm{H}^2(K'/K)$ .*

*Proof.* We will use a descent argument which follows [17, Chapter X, §5, Proposition 9]. Let  $K'/K$  be a Galois extension, and set

$$\mathrm{Br}(K'/K) := \{[A] \in \mathrm{Br}(K) : [A \otimes_K K'] = 0 \in \mathrm{Br}(K')\}.$$

Let  $[A], [B] \in \mathrm{Br}(K'/K)$  be such that  $[A \otimes_K K'] = [B \otimes_K K'] = 0 \in \mathrm{Br}(K')$ . This means that precisely that  $[A] = [B]$  by the equivalence relation in Theorem C.9 which defines  $\mathrm{Br}(K)$ . We will show that these are compatible with the definition of  $\mathrm{H}^2(K'/K)$ . Let  $[A : K] = n^2$ . By definition, there exists an isomorphism of  $K'$ -algebras  $\phi : A \otimes_K K' \rightarrow B \otimes_K K'$ . For any  $\sigma \in \Gamma := \mathrm{Gal}(K'/K)$ , let  $\sigma : A \otimes_K K' \rightarrow A \otimes_K K'$  be the automorphism induced by the action of  $\sigma$  on  $K'$ . Then, by composition, we get another isomorphism  $\phi^\sigma : A \otimes_K K' \rightarrow B \otimes_K K'$ . Setting  $c_\sigma := \phi^\sigma \circ \phi^{-1}$ , we get an automorphism  $c_\sigma \in \mathrm{Aut}_K(A \otimes_K K') = \mathrm{Aut}_K(M_n(K'))$ . However, every automorphism of  $M_n(K')$  is an inner automorphism by Skolem-Noether theorem. So, we have  $\mathrm{Aut}_K(M_n(K')) = \mathrm{GL}_n(K')$  and the map  $\sigma \mapsto c_\sigma$  determines a 1-cocycle in  $Z^1(\Gamma, \mathrm{GL}_n(K'))$ . By [17, Chapter X, §1, Proposition 3], we have  $\mathrm{H}^1(\Gamma, \mathrm{GL}_n(K')) = 1$ . So,  $[A] = [B]$  as expected.

Keeping the notations above, for any  $\sigma \in \Gamma$ ,  $\phi^\sigma : A \otimes_K K' \rightarrow M_n(K')$  be isomorphism such that the following diagram commutes:

$$\begin{array}{ccc} A \otimes_K K' & \xrightarrow{\phi} & M_n(K') \\ & \searrow \phi^\sigma & \downarrow \sigma \\ & & M_n(K') \end{array}$$

Using Skolem-Noether's theorem, choose  $u_\sigma \in \mathrm{GL}_n(K')$  such that  $\phi^\sigma = u_\sigma^{-1} \cdot \phi \cdot u_\sigma$ . If  $\tau \in \Gamma$  is another element, we must have  $\phi^{\sigma\tau} = u_{\sigma\tau}^{-1} \cdot \phi \cdot u_{\sigma\tau}$ . We must also have

$$\phi^{\sigma\tau} = (\phi^\sigma)^\tau = u_\tau^{-1} \cdot u_\sigma^{-1} \cdot \phi \cdot u_\sigma \cdot u_\tau.$$

Set

$$c(\sigma, \tau) := u_\sigma \cdot u_\tau \cdot u_{\sigma\tau}^{-1}, \text{ for all } \sigma, \tau \in \Gamma.$$

Since  $A$  is simple and  $c(\sigma, \tau)$  commutes with  $\phi$ , we see that  $c(\sigma, \tau)$  must be a scalar matrix. This gives rise to a 2-cocycle  $c \in Z^2(\Gamma, K'^\times)$ . We let  $[c] \in \mathrm{H}^2(K'/K)$  be the class of  $c$ ...

□

**Theorem C.18.** *Let  $K_s$  be a separable closure of  $K$ . Then, there exists an isomorphism*

$$\mathrm{Br}(F) \simeq \mathrm{H}^2(F_s/F, F_s^\times).$$

*Proof.* It remains to show that the isomorphisms  $\mathrm{Br}(K'/K) \simeq \mathrm{H}^2(K'/K)$  in Proposition C.17 are compatible with the injections

$$\mathrm{Br}(K'/K) \rightarrow \mathrm{Br}(L/K) \text{ and } \mathrm{H}^2(K'/K) \rightarrow \mathrm{H}^2(L/K) \text{ for all } L \supset K'.$$

But that is not too hard to prove. □

Now, let  $K$  be a non-archimedean local field, and  $K^{\mathrm{unr}}$  the maximal unramified subextension of  $K_s$ . Let  $\kappa$  and  $\bar{\kappa}$  be the residue fields of  $K$  and  $K^{\mathrm{unr}}$ , respectively. Let  $\mathrm{Frob} \in \mathrm{Gal}(\bar{\kappa}/\kappa)$  be the arithmetic Frobenius; this is a topological generator. By local class field theory, there is a canonical isomorphism

$$\mathrm{H}^2(K^{\mathrm{unr}}/K, K^{\mathrm{unr}\times}) \simeq \mathrm{H}^2(K_s/K, K_s^\times).$$

The normalised valuation  $v : K^{\mathrm{unr}\times} \rightarrow \mathbf{Z}$  also induces an isomorphism

$$\mathrm{H}^2(K^{\mathrm{unr}}/K, K^{\mathrm{unr}\times}) \simeq \mathrm{H}^2(K^{\mathrm{unr}}/K, \mathbf{Z}) \stackrel{\delta}{\simeq} \mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbf{Q}/\mathbf{Z}).$$

**Theorem C.19.** *Let  $K$  be a non-archimedean local field. Then, the map*

$$\mathrm{inv}_K : \mathrm{Br}(K) \simeq \mathbf{Q}/\mathbf{Z}$$

*is a group homomorphism.*

*Proof.*

Give proof or reference!!

□

**Remark C.20.** Since  $\mathrm{Br}(\mathbf{R})$  is cyclic of order 2 and  $\mathrm{Br}(\mathbf{C})$  is trivial, for archimedean local fields  $F$  there is a unique injective homomorphism  $\mathrm{inv}_F : \mathrm{Br}(F) \hookrightarrow \mathbf{Q}/\mathbf{Z}$ . By [3, Thm. 3, p. 131], for a finite extension  $F'/F$  of nonarchimedean local fields, composition with the natural map  $\mathrm{Br}(F) \rightarrow \mathrm{Br}(F')$  carries  $\mathrm{inv}_{F'}$  to  $[F' : F] \cdot \mathrm{inv}_F$ . By [17, p. 194, Cor. 3],  $\mathrm{inv}_F(D)$  has order  $[D : F]^{1/2}$  for any central division algebra  $D$  over  $F$ . These assertions are trivially verified to also hold for archimedean local fields  $F$ .

**Theorem C.21.** *Let  $F$  be a global field. There is an exact sequence*

$$0 \rightarrow \mathrm{Br}(F) \rightarrow \bigoplus_{v \in M_F} \mathrm{Br}(F_v) \xrightarrow{\Sigma} \mathbf{Q}/\mathbf{Z} \rightarrow 0,$$

where  $M_F$  denotes the set of nonequivalent nontrivial absolute values of  $F$  and  $F_v$  denotes the completion of  $F$  at  $v$ . The first map is defined via the maps  $\mathrm{Br}(F) \rightarrow \mathrm{Br}(F_v)$  given by extension of scalars, and the second map is given by summing the local invariants.

*Proof.* This is [3, §§9.7, 11.2]. □

For a global field  $F$  and a central division  $F$ -algebra  $D$ , write  $\text{inv}_v(D)$  for  $\text{inv}_{F_v}(D \otimes_F F_v)$  for a place  $v$  of  $F$ . Theorem C.21 asserts that a central division algebra  $D$  over a global field  $F$  is uniquely determined by its local invariants  $\text{inv}_v(D)$ , up to isomorphism. These local invariant may be arbitrarily assigned subject to the condition  $\text{inv}_v(D) = 0$  for all but finitely many  $v$  and  $\sum_v \text{inv}_v(D) = 0$ . Moreover, the order of  $[D]$  in  $\text{Br}(F)$  is the least common “denominator” of the  $\text{inv}_v(D) \in \mathbf{Q}/\mathbf{Z}$ .

We need one more theorem that gives such a result over global fields:

**Theorem C.22.** *Let  $F$  be a global field, and  $D$  a central division algebra over  $F$ . Then, the order of  $[D]$  in  $\text{Br}(F)$  is  $[D : F]^{1/2}$ .*

*Proof.* Let  $[D : F] = n^2$ , and let  $d$  be the order of  $[D]$  in  $\text{Br}(F)$ , so that  $d \mid n$ . For a place  $v$  of  $F$ , let  $D_v = D \otimes_F F_v$  and  $d_v$  the order of  $[D_v]$  in  $\text{Br}(F_v)$ . Note that

$$d = \text{lcm}\{d_v : v \text{ a place of } F\},$$

where  $d_v = 1$  for complex  $v$ ,  $d_v \mid 2$  for real  $v$ , and  $d_v = 1$  for all but finitely many  $v$ . We recall that  $d_v = [L_v : F_v]$ , where  $L_v \subset D_v$  is the maximal commutative sub-algebra of  $D_v$  (that splits  $D_v$ ). By Proposition C.13,

$$[D_v : F_v] = [L_v : F_v]^2 = d_v^2.$$

By global class field theory [1, Chapter X, Theorem 5], there exists an abelian extension  $L/F$  of degree  $d$  such that  $d_v \mid [L_w : F_v]$ , for every  $v$  of  $F$  and  $w \mid v$  of  $L$ . Since the map  $\text{Br}(F_v) \rightarrow \text{Br}(L_w)$  sends  $\text{inv}_{F_v}$  to  $[L_w : F_v] \text{inv}_{L_w}$ , we see that  $D \otimes_F L$  splits at all the places  $w$  of  $L$ . It follows that  $L$  necessarily splits  $D$ . Since  $[L : F] = d \mid n$  and  $L$  splits  $D$ , we must have  $[D : F] = [L : F]^2$  by Proposition C.13.  $\square$

### C.3 Local invariants of division algebras

**Lemma C.23.** *Let  $F$  be a field and  $E/F$  a cyclic extension. Fix a generator  $\sigma$  of  $\Gamma := \text{Gal}(E/F)$ , and let  $\chi_\sigma : \Gamma \rightarrow \mathbf{Q}/\mathbf{Z}$  be the unique homomorphism given by*

$$(\chi_\sigma : \Gamma \rightarrow \mathbf{Q}/\mathbf{Z}, \sigma \mapsto 1/[E : F]).$$

*Let  $\theta_\sigma := \delta(\chi_\sigma) \in \text{H}^2(\Gamma, \mathbf{Z})$ , where  $\delta : \text{H}^1(\Gamma, \mathbf{Q}/\mathbf{Z}) \rightarrow \text{H}^2(\Gamma, \mathbf{Z})$  is the connecting map arising from  $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Q} \rightarrow \mathbf{Q}/\mathbf{Z} \rightarrow 0$ . Recall the Tate isomorphism induced by the cap product*

$$\widehat{\text{H}}^0(\Gamma, E^\times) \xrightarrow{\cup \theta_\sigma} \text{H}^2(\Gamma, E^\times).$$

*Then, we have the following.*

1. *For  $c \in E^\times$ , the class of the cyclic algebra  $(E/F, \sigma, c) \in \text{Br}(F)$  is the image of  $c \bmod \text{Nm}_{E/F}(E^\times)$  under the map*

$$E^\times / \text{Nm}_{E/F}(E^\times) \rightarrow \text{Br}(F).$$

2. *If  $E_0/F$  is a sub-extension of  $E/F$  and  $\sigma' = \sigma|_{E_0}$  then*

$$[(E_0/F, \sigma', c)] = [(E/F, \sigma, c^{[E:E_0]})] \in \text{Br}(F).$$

*Proof.* See [4, Appendix A] or Serre [17, Chapter V, Section 4].  $\square$

**Theorem C.24.** *Let  $F$  be a non-archimedean local field and  $E/F$  an unramified finite extension. Let  $\phi \in \text{Gal}(E/F)$  be the arithmetic Frobenius element. For any  $c \in F^\times$ , the cyclic  $F$ -algebra  $(E/F, \phi, c)$  has local invariant in  $\mathbf{Q}/\mathbf{Z}$  represented by  $\text{ord}_F(c)/[E : F]$ .*

*Proof.* See [4, Appendix A] or Serre [17, Chapter V, Section 4].  $\square$

## References

- [1] E. Artin and J. Tate. *Class field theory*. Addison-Wesley, New York, 1968.
- [2] Nicolas Bourbaki, *Éléments de mathématique. Algèbre. Chapitre 8. Modules et anneaux semi-simples*. Second revised edition of the 1958 edition Springer, Berlin, 2012. x+489 pp.
- [3] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. Reprint of the 1967 original.
- [4] C-L. Chai, B. Conrad, and F. Oort, *Complex Multiplication and Lifting Problems*, American Mathematical Society, 2014.
- [5] Ching-Li Chai and Frans Oort, *Moduli of abelian varieties and  $p$ -divisible groups*, Arithmetic geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, pp. 441–536. MR 2498069
- [6] Ching-Li Chai and Frans Oort, *An algebraic construction of an abelian variety with a given Weil number*, *Algebr. Geom.* 2 (2015), no. 5, 654–663. MR 3421786
- [7] Kirsten Eisenträger, *The theorem of Honda and Tate*. Available at <http://math.stanford.edu/~conrad/vigregroup/vigre04/hondatate.pdf>.
- [8] Robin Hartshorne, *Algebraic geometry*, Grad. Texts in Math., No. 52 Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp.
- [9] B. Edixhoven, B Moonen and G. van der Geer, *Abelian varieties*. Available at <http://van-der-geer.nl/~gerard/AV.pdf>.
- [10] J.-M. Fontaine, *Groupes  $p$ -divisibles sur les corps locaux*, Société Mathématique de France, in Astérisque, 1977.
- [11] B. Lawrence, *Dieudonné modules and  $p$ -divisible Groups*. Available at <http://virtualmath1.stanford.edu/~conrad/JLseminar/Notes/L17I.pdf>.
- [12] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR 861974
- [13] J. S. Milne and W. C. Waterhouse, *Abelian varieties over finite fields*, Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64. MR 0314847

- [14] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008, With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR 2514037
- [15] Frans Oort, *Abelian varieties over finite fields*, Higher-dimensional geometry over finite fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, pp. 123–188. MR 2484079
- [16] I. Reiner. *Maximal orders*, Volume **28** of London Mathematical Society Monographs. New Series. The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, with a foreword by M. J. Taylor.
- [17] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.
- [18] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*. Ann. of Math. (2) **88** (1968), 492–517.
- [19] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*. Publ. Math. Soc. Japan, 6 Mathematical Society of Japan, Tokyo, 1961. xi+159 pp.
- [20] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, Grad. Texts in Math., 106 Springer, Dordrecht, 2009. xx+513 pp.
- [21] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 13400144. MR 206004
- [22] John Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini* (d'après T. Honda), Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 352, 95–110. MR 3077121
- [23] W. Trappe and L. C. Washington, *Introduction to cryptography with coding theory*, Pearson Prentice Hall, Upper Saddle River, NJ, 2006, xiv+577 pp.
- [24] , André Weil, *Adèles and algebraic groups*. With appendices by M. Demazure and Takashi Ono Progr. Math., **23** Birkhäuser, Boston, MA, 1982. iii+126 pp.
- [25] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969), 521–560. MR 265369
- [26] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer, 1979.