Abelian varieties over finite fields: Honda–Tate's Theorem

Lassina Dembélé
lassina.dembele@kcl.ac.uk
King's College London

Preliminary Arizona Winter School 2024

Version: October 27, 2023

Contents

1 Definition and properties of abelian varieties

We fix a field k, and let $\overline{k}$ 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. $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ 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 $m : G \times G \to G$ (the group law) and $i : G \to G$ (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:

$$\begin{tikzcd}
G \times G \times G \arrow[r, "id_{G\times G\times G}"] \arrow[d, "id_{G\times G\times G}"'] & (G \times G) \times G \arrow[r, "m \times id_G"] & G \times G \arrow[d, "m"] \\
G \times (G \times G) \arrow[r, "id_G \times m"] & G \times G \arrow[r, "m"] & G
\end{tikzcd}$$

(ii) Identity element:

$$\begin{tikzcd}
G \times \mathrm{Spec}(k) \arrow[r, "id_G \times e"] \arrow[dr, "j_1"'] & G \times G \arrow[d, "m"] & \mathrm{Spec}(k) \times G \arrow[l, "e \times id_G"'] \arrow[dl, "j_2"] \\
 & G &
\end{tikzcd}$$

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

(iii) Existence of inverse element:

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[d, "{(id_G, i)}"'] & \mathrm{Spec}(k) \arrow[d, "e"] & G \arrow[l, "\pi"'] \arrow[d, "{(i, id_G)}"] \\
G \times G \arrow[r, "m"'] & G & G \times G \arrow[l, "m"]
\end{tikzcd}$$

where $\pi : G \to \mathrm{Spec}(k)$ 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 $f : X \times Y \to Z$ 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 $f : X \to Y$ 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

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

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. □

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. □

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 $\mathscr{L}$ be a line bundle on $X \times Y \times Z$ such that the restrictions of $\mathscr{L}$ to $X \times Y \times \{z_0\}, X \times \{y_0\} \times Z$ and $\{x_0\} \times Y \times Z$ are trivial. Then $\mathscr{L}$ is trivial.*

Corollary 1.8. *Let A be an abelian variety. Let $\pi_i : A \times A \times A \to A$ 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 $\mathscr{L}$ be a line bundle on A. Then the line bundle*

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

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 $\pi_{123}^*\mathscr{L} = \pi_{12}^*\mathscr{L}$, $\pi_{13}^*\mathscr{L} = \pi_1^*\mathscr{L}$, and $\pi_3^*\mathscr{L} = 1$, so all factors cancel. □

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

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

on X is trivial.

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

1.4 Theorem of the square

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

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

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

1.5 Isogenies

Proposition 1.11. *Let $f : A \to B$ 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 $f : A \to B$ 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 $k(B) \to k(A)$, since an isogeny is surjective.)*

Definition 1.13. *Let $f : A \to B$ 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 $f : A \to C$ be an isogeny. Then, there exist*

(i) an abelian variety B;

(ii) an inseparable isogeny $g : A \to B$; and

(iii) a separable isogeny $h : B \to C$

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

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

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

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

In particular,

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

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

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

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

is trivial. In other words, we have

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

The result now follows by induction. □

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

Proof. One can show that abelian varieties are projective. Let $\mathscr{L}$ be an ample line bundle on A. Replacing $\mathscr{L}$ by $\mathscr{L} \otimes [-1]^*\mathscr{L}$, we can assume $\mathscr{L}$ is symmetric. Since $[n]^*\mathscr{L} = \mathscr{L}^{n^2}$, 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. □

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

Proof. Let $f : X \to Y$ be a finite map of complete varieties of degree d. If $D_1, \ldots, D_n$ 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^2D. We thus find

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

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

One can show that $[n] : A \to A$ 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 $(\mathrm{char}(k), n) = 1$, 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 $f : A \to B$ be an isogeny of degree n. Then there exists an isogeny $g : B \to A$ 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 $\mathrm{Pic}(A)$ to be the set of isomorphism classes of line bundles on A. Then, we let $\mathrm{Pic}^0(A)$ be the subgroup consisting of those line bundles $\mathscr{L}$ which are translation invariant, i.e., which satisfy $t_x^*(\mathscr{L}) \simeq \mathscr{L}$ for all $x \in A$. We define the following functor. For each variety T over k, let $F(T)$ be the of isomorphism classes of line bundles $\mathscr{L}$ on $A \times T$ satisfying the following two conditions:

(a) for all $t \in T$, the restriction of $\mathscr{L}$ to $A \times \{t\}$ belongs to $\mathrm{Pic}^0(A)$; and

(b) the restriction of $\mathscr{L}$ to $\{0\} \times T$ is trivial.

We see that $F(k) = \mathrm{Pic}^0(A)$. 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 $\mathscr{P}$ on $A \times A^\vee$, which is called the *Poincaré bundle.*

2.2 Construction of the dual

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

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

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

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

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

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

2.3 Polarisations

Definition 2.2. *Let A be an abelian variety. A* polarisation *on A is an isogeny $\lambda : A \to A^\vee$ such that $\lambda_{\overline{k}} : A(\overline{k}) \to \mathrm{Pic}^0(A)$ is given by $\lambda_{\overline{k}} = \phi_{\mathscr{L}}$ for some ample line bundle $\mathscr{L}$ on A over $\overline{k}$. The* degree *of the polarisation λ 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 λ has degree 1, then we say that (A, λ) 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 $B \times C \to A$ is an isogeny.*

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

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. □

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 $f : A \to B$ is an isogeny then there exists an isogeny $g : B \to A$ 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 Δ_E *of E is the discriminant Δ_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 $\Delta_E = -4a^3 - 27b^2$.

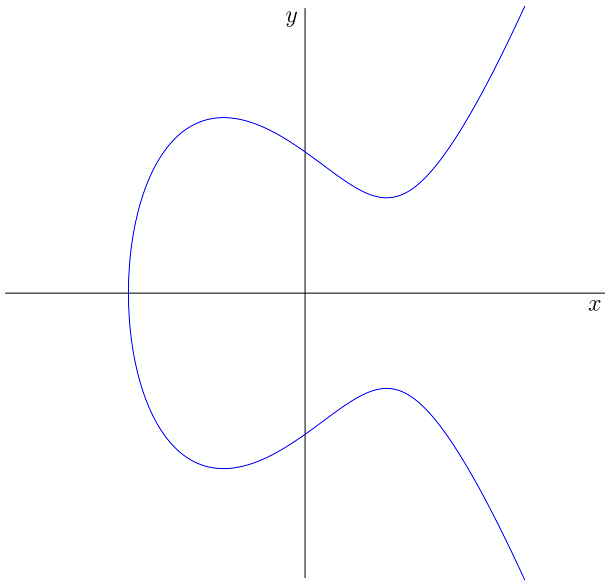

Figure 1: Real points of the elliptic curve $y^2 = x^3 - 8$

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 $\overline{k}$. 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 $f'(x) = 3x^2 + 2x = 2x$ ($\mathrm{char}(\mathbf{F}_3) = 3$). So $\gcd(f, f') = 1$, which implies that f has distinct roots.

4.2 Definition of the group law

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

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3. \tag{1}$$

The *only* point at infinity on E is $[0 : 1 : 0]$, which we denote by ∞ 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*

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

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

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

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 $\overline{k}$ is n. The following theorem can be see 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 $L \subset \mathbf{P}^1(\overline{k})$ 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 $L \cap E \subset \mathbf{P}^1(\overline{k})$, 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 ∞ 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.*

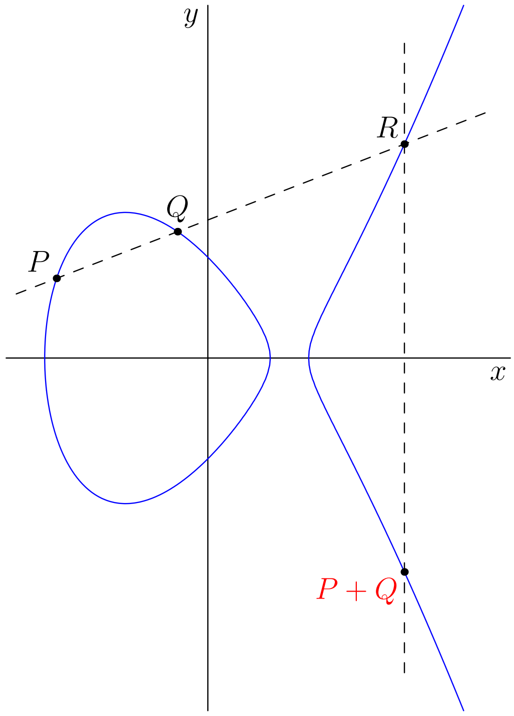

Figure 2: Group addition law

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

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

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

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

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

(i) The neutral *element is ∞;*

(ii) If $P, Q, R \in E(\overline{k})$ 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 $E(\overline{k})$. 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 ∞.

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 $Q = (0,1)$. Th 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 ∞ 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 $E(\mathbf{Q})$.

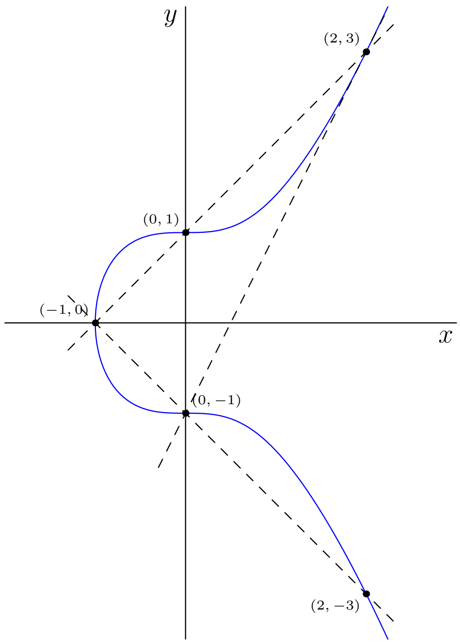

Figure 3: Euler cubic: $y^2 = x^3 + 1$

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) $P + Q = Q + P \;\; \forall P, Q \in E(\bar{k})$ *(commutativity).*

(ii) $P + \infty = P \;\; \forall P \in E(\bar{k})$ *(identity element).*

(iii) If $P = (x, y)$*, then* $-P = (x, -y)$ *(opposite element).*

(iv) $P + (Q + R) = (P + Q) + R, \;\; \forall P, Q, R \in E(\bar{k})$ *(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. □

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

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

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 $\lambda = \frac{y_2-y_1}{x_2-y_1}$ 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 $\lambda = \frac{3x_P^2+2}{2y_P} = \frac{3(-3)^2+2}{2(4)} = 5 \bmod 11$. So, we have $x_{2P} = \lambda^2 - 2x_P = (5^2) - 2(-3) = 25 + 6 = -2 \bmod 11$. So, we get that $-y_{2P} = y_P + \lambda(x_{2P} - x_P) = 4 + 5(-2 - (-3)) = -2 \bmod 11$. 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 $k \subseteq k' \subseteq \overline{k}$ is a subfield, then $E(k')$ is a subgroup of $E(\overline{k})$.*

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. □

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 $(f + g) : A \to B$ given on points by addition $x \mapsto f(x) + g(x)$. This gives the set $\mathrm{Hom}(A, B)$ of homomorphisms $A \to B$ the structure of an abelian group. For $A = B$ we see that $\mathrm{End}(A)$ has a natural ring structure, with composition of endomorphisms as the ring multiplication. We will always write $\mathrm{Hom}(A, B)$ for the group of homomorphisms from A to B, and $\mathrm{End}(A)$ for the ring of endomorphisms of A. We will use the notations $\mathrm{Hom}_k(A, B)$ and $\mathrm{End}_k(X)$ 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* $\mathrm{Hom}(A, B)$ *is* torsion-free, *i.e. for $f \in \mathrm{Hom}(A, B)$ and $n \in \mathbf{Z}$ non-zero, $n \cdot f = 0$ implies that $f = 0$.*

Proof. For $n \in \mathbf{Z}$ and $f \in \mathrm{Hom}(A, B)$, 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 $f = 0$. □

We write

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

By definition, we see that $\mathrm{End}^0(A)$ 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 $B \times C \to A$ is an isogeny.*

Proof. Let $i : B \hookrightarrow A$ be the inclusion map and $i^\vee : A^\vee \to B^\vee$ its dual. Let $\lambda : A \to A^\vee$ 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 $i^\vee \circ \lambda : A \to B^\vee$ to B is $\lambda|_B : B \to B^\vee$, whose kernel is finite since λ arises from an ample bundle $\mathscr{L}$. Therefore $B \cap C$ is finite, and so $B \times C \to A$ is an isogeny. □

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 $B_1, \ldots, B_r$, which are pairwise non k-isogenous, and positive integers $n_1, \ldots, n_r$ such that A is k-isogenous to $B_1^{n_1} \times \cdots \times B_r^{n_r}$, which we denote by $A \sim_k B_1^{n_1} \times \cdots \times B_r^{n_r}$. 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. □

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

(i) if A is k-simple, then $\mathrm{End}_k^0(A)$ is a division algebra;

(ii) If $A \sim_k B_1^{n_1} \times \cdots \times B_r^{n_r}$, where the B_i are k-simple abelian varieties, then we have

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

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

(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 $\mathrm{End}_k^0(A)$. So if A is k-simple $\mathrm{End}_k^0(A)$ is a division algebra. For the second part of the statement, note that $\mathrm{Hom}(B_i, B_j) = 0$ if $i \neq j$ since B_i and B_j are simple and non-isogenous. □

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 $(\mathrm{char} k, n) = 1$. From Proposition 1.17, we know that $[n]$ is a separable map of degree n^{2g}. Furthermore, all fibers of the map $[n] : A(\overline{k}) \to A(\overline{k})$ have cardinality n^{2g}; in other words, $A[n](\overline{k})$ has cardinality n^{2g}, where $A[n] = \ker[n]$. By Corollary 1.18 we have an isomorphism

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

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

Let ℓ be a prime number different from the $\mathrm{char} k$. The ℓ-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 $A[n](\overline{k})$, where the transition maps are multiplication by ℓ. Explicitly, an element of $T_\ell(E)$ is a sequence $(x_0, x_1, \ldots)$ of $\overline{k}$-points of E, 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 $G_k = \mathrm{Gal}(\overline{k}/k)$ 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 $\rho : G_k \to \mathrm{GL}_{2g}(\mathbf{Z}_\ell)$, i.e., an ℓ-adic representation of the Galois group. This perspective has proved to be very useful.

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

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

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

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

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

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

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

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

is injective and has a torsion-free cokernel.

Proof. □

5.3 The Tate module of the multiplicative group

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

The construction of the Tate module in the previous section can be applied equally well to G_m. If n is prime to $\mathrm{char} k$ then the n-torsion $G_m[n]$ is just the group of n-th roots of unity; its $\overline{k}$-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 $\chi : G_k \to \mathrm{GL}_1(\mathbf{Z}_\ell) = \mathbf{Z}_\ell^\times$. 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 5.8. *Let A/k be an abelian variety and $n > 0$ an integer such that $(n, \mathrm{char} k) = 1$. Then there exists a pairing*

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

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* μ_n *is written multiplicatively.)*

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

$$\begin{aligned} e_n^\lambda : A[n] \times A[n] &\to \mu_n \\ (x,y) &\mapsto e_n(x, \lambda(y)). \end{aligned}$$

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

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

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

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* μ_n *is written multiplicatively.)*

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

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

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

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

The pairing e^λ satisfies the same properties as in Proposition 5.8.

Proposition 5.11. *Let* A *be an abelian variety over* k. *The degree map*

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

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

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

Corollary 5.12. *Let A be an abelian variety over k. Then, for each $\phi \in \mathrm{End}^0(A)$, 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_ϕ is monic and that it has integer coefficients when $\phi \in \mathrm{End}(A)$. We call P_ϕ the *characteristic polynomial* of ϕ and we define the *trace* of ϕ by the equation

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

Proposition 5.13. *Let A be an abelian variety over k and $\phi \in \mathrm{End}(A)$. For each prime number ℓ such that $\ell \neq \mathrm{char}(k)$, $P_\phi(X)$ is the characteristic polynomial of ϕ acting on $V_\ell A$; hence the trace and degree of ϕ are the trace and determinant of ϕ acting $V_\ell A$.*

5.5 Semi-simple modules

In this subsection, all rings have an identity element. A ring homomorphism is a map $f : A \to B$ 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^{opp} denotes the opposite ring and $Z(A)$ the center of A. For a integer $r \geq 0$, we le $M_r(A)$ 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 5.14. *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 5.15. *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 $A_1, \ldots, A_r \subset A$. Each ideal A_i is also a ring, with an identity element making it a simple ring. Thus A is isomorphic to the product $A_1 \times \cdots \times A_r$. So every semisimple ring is a product of finitely many simple rings. Conversely, every finite product of simple rings is semisimple.

Proposition 5.16. *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. □

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

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

Lemma 5.17. *Let A be a simple ring, M a simple A-module and $D = \mathrm{End}_A(M)$. Then, the map $a \mapsto a_M$ is an isomorphism of A onto its bi-commutant $End_D(M)$.*

Corollary 5.18 (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 isomorphic to M^r as A-modules. From this and the lemma above, it follows that $A \simeq M_r(D)$. □

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^{opp}.

Theorem 5.19 (Bi-commutant)**.** *Let A be a semisimple ring, and let M be an A-module of finite type. Let $C := \mathrm{End}_A(M)$, and consider M as a left module over C by the rule*

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

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

Theorem 5.20 (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 $\varphi : B \to B'$ of K-algebras there is an inner automorphism ψ 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 $\mathrm{Aut}_K(A) = \mathrm{Inn}(A) \simeq A^\times / K^\times$.

6 Tate's theorem

6.1 Frobenius endomorphism

We le $k := \mathbf{F}_q$ 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* $\pi_V : V \to V$ is defined to be the map which is the identity on the underlying topological space of V and is the map $\mathcal{O}_V \to \mathcal{O}_V, f \mapsto f^q$ on the structure sheaves. When $V := \mathbf{P}^n(\mathbf{F}) = \mathrm{Proj}(k[x_0, \ldots, x_n])$, then π_V is given by the ring homomorphism

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

On points, this induces the map

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

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

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

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

Let A be an abelian variety over $\mathbf{F}_q$. Then π_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 π_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 5.12 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 ℓ 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 $\mathbf{Q}[\pi_A] \subset \mathrm{End}^0(A)$ is a field, and f_A is a power of the minimum polynomial $f_{\mathbf{Q}}^{\pi_A}$ of π_A over $\mathbf{Q}$.

Proof. (i) As observed above, π_A lies in the centre of $\mathrm{End}^0(A)$, which is a product of number fields. Hence $\mathbf{Q}[\pi_A] \subset \mathrm{End}^0(A)$ is a product of (number) fields, too. It follows that also $\mathbf{Q}_\ell[\pi_A] \subset \mathbf{Q}_\ell \otimes \mathrm{End}^0(A)$ 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 π_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 $\mathrm{End}^0(A)$ is a field, so also $\mathbf{Q}[\pi_A]$ is a field. Let $g := f_A$ be the minimum polynomial of π_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. □

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 ℓ be a prime number such that $\ell \neq \mathrm{char}(k)$.*

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

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

is an isomorphism if and only if the map

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

is an isomorphism.

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

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

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 5.7, the map T_ℓ is injective and $\mathrm{coker}(T_\ell)$ is torsion-free (hence free). Hence T_ℓ 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_ℓ 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

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

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

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

□

Lemma 6.4. *Let A an abelian variety over a field k, and let ℓ 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 ℓ be a prime number such that $\ell \neq \mathrm{char}(k)$. Then the representation*

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

is semisimple and the map

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

is an isomorphism.

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

The map $\mathbf{Q}_\ell \, \mathrm{End}(A) \to \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell A)$ is injective by Theorem 5.7. Letting $C = \mathrm{End}_{\mathbf{Q}_\ell \mathrm{End}(A)}(V_\ell A)$, Theorem 5.19 implies that $\mathbf{Q}_\ell \, \mathrm{End}(A) = \mathrm{End}_C(V_\ell A)$. Hence it suffices to show that for every $\varphi \in \mathrm{End}_{\mathrm{Gal}(k_s/k)}(V_\ell A)$ 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 $u \in \mathbf{Q}_\ell \, \mathrm{End}(A^2) = M_2(\mathbf{Q}_\ell \, \mathrm{End}(A))$ such that $\Gamma_\varphi = u \cdot V_\ell A^2$. But $\gamma := \left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) \in M_2(\mathbf{Q}_\ell \, \mathrm{End}(A)$ 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. □

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

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

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

is semisimple.

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

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

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 $D = \mathrm{End}_k^0(A)$ 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 $(D \to D,\, x \mapsto x^\dagger)$ be the Rosati involution on A. This is a positive involution. So, its fixed field $F^\dagger := \{x \in D \,|\, x^\dagger = x\}$ 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 $D = \mathrm{End}_k^0(A)$ 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 † 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* $\mathrm{char}(k) = 0$, *and $e^\dagger d \mid g$ if* $\mathrm{char}(k) > 0$.

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 α of f_A has absolute value $|\alpha| = \sqrt{q}$.

(ii) If α is a complex root of f_A then so is $\overline{\alpha} = q/\alpha$, 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

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

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

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

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

Let λ be any polarisation on A, and † the associated Rosati involution on $\mathrm{End}^0(A)$. 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 Verschibung map $V_{A/\mathbf{F}_q}$ (see next section), we have $\pi_A^\vee = V_{A^\vee/\mathbf{F}_q}$, and

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

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 Propostion 6.1, f_A is a power of the minimum polynomial of g of π_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 $\iota : \mathbf{Q}[\pi_A] \to \mathbf{C}$. The relation $\pi_A^\dagger = q/\pi_A$ shows that $\mathbf{Q}[\pi_A] \subset \mathrm{End}^0(A)$ 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 † is the identity on $\mathbf{Q}[\pi_A]$.

(b) CM case: $\mathbf{Q}[\pi_A]$ is a CM-field and for every complex embedding $\iota : \mathbf{Q}[\pi_A] \to \mathbf{C}$ we have $\iota(x^\dagger) = \overline{\iota(x)}$, 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 $\overline{\alpha} \cdot \alpha = q$. 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. □

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

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

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 ℓ 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

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

(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 π_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 $\bigwedge^k V_\ell(\pi_A^n)$ are the numbers the products

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

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

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

(ii)We use the general fact (see Hartshorne [4, Appendix C, Lemma 4.1]) that for $\phi \in \mathrm{End}(V)$, where V is a finite dimensional vector space V over a field K, we have an identity of formal power series

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

Applying (i) then gives

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

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

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

Therefore

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

Since $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts naturally on the set of sequences $(\alpha_{i_j})_{1\le j\le k}$, $P_k \in \mathbf{Q}[x]$. 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 $\mathrm{Div}(X)$ is the set formal sums

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

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

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

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

$$\mathrm{Pic}^0(X) := \left\{ \mathscr{L} \in \mathrm{Pic}(X) \,\middle|\, \deg \mathscr{L} = 0 \right\}.$$

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

$$F(T) = \left\{ \mathscr{L} \in \mathrm{Pic}(X \times T) \,\middle|\, \deg(\mathscr{L}_t) = 0, \text{ for all } t \in T \right\} / p_T^* \mathrm{Pic}(T),$$

where $p_T : X \times_k T \to T$ 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 $\mathscr{M} \in \mathrm{Pic}(T)$, $(p_T^*\mathscr{M})_t$ is isomorphic to $\mathcal{O}_{X_t}$ and so $\deg(p_T^*\mathscr{M})_t = 0$. The Jacobian attempts to represent the functor F.

Theorem 8.1. *There is an abelian variety* $\mathrm{Jac}(X)$ *over* k *and a morphism of functors* $\iota : F \to \mathrm{Jac}(X)$ *such that* $\iota : F(T) \to \mathrm{Jac}(X)(T)$ *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 Γ. Then the natural map $F(k) \to F(k')^\Gamma$ need not be a bijection, which is a requirement for representability.

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

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

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

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

Now, let $\mathscr{L} \in \mathrm{Pic}(X \times_k k')^\Gamma$. We will construct an element of $\mathrm{Br}(k)$ measuring the obstruction that $\mathscr{L}$ comes from $\mathrm{Pic}(X)$. Since $\mathscr{L} \in \mathrm{Pic}(X \times_k k')^\Gamma$, we see that, for all $\sigma \in \Gamma$, there exists an isomorphism $i_\sigma : \mathscr{L} \simeq \sigma^*\mathscr{L}$. 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 $\mathscr{L} \simeq (\sigma\tau)^*\mathscr{L}$; thus they differ by an element $c_{\sigma,\tau} \in \mathrm{Aut}(\mathscr{L}) = k'^\times$. It is easy to see that c satisfies the 2-cocycle condition, and thus defines an element of $\mathrm{H}^2(\mathrm{Gal}(k'/k), k'^\times) \subset \mathrm{Br}(k)$. If this 2-cocycle is a coboundary, then the choice of i's can be modified to give descent data on $\mathscr{L}$, and $\mathscr{L}$ belongs to $\mathrm{Pic}(X)$. This completes the proof. □

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, $\mathrm{Pic}(X \times_k k')$ is isomorphic to $\mathbf{Z}$. Since $\Gamma = \mathbf{Z}/2\mathbf{Z}$, $\mathrm{Pic}(X)$ has index at most 2 inside $\mathrm{Pic}(X \times_k k')$. But the bundle $\mathcal{O}(1)$ on $X \times_k k'$ does not descend to X, as this would give an isomorphism $X \to \mathbf{P}^1$ over k. Therefore Γ acts trivially on $\mathrm{Pic}(X \times_k k')$ given the exact sequence

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

Remark 8.4. Suppose k is a finite extension of $\mathbf{Q}_p$. Then $\mathrm{Br}(k) = \mathbf{Q}/\mathbf{Z}$, and Lichtenbaum showed that the image of the the map $\mathrm{Pic}(X \times_k \overline{k})^\Gamma \to \mathrm{Br}(k)$ is $N^{-1}\mathbf{Z}/\mathbf{Z}$, where N is the gcd of the degrees of divisors on X. Thus $\mathrm{Pic}(X) = \mathrm{Pic}(X \times_k \overline{k})^\Gamma$ 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 $F(k') = \mathrm{Pic}^0(X \times_k k')$). 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

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

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* $(F_x \to F, (\mathscr{L}, i) \mapsto \mathscr{L})$ *is an isomorphism.*

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

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

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* $\operatorname{Jac}(X)$, *and called the* Jacobian variety *of X.*

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

(a) $\mathscr{M}|_{X\times\{0\}} \simeq \mathcal{O}_X$ and $\mathscr{M}|_{\{x\}\times \operatorname{Jac}(X)} \simeq \mathcal{O}_{\operatorname{Jac}(X)}$;

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

The pair $(\operatorname{Jac}(X), \mathscr{M})$ 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 $X(k) = \varnothing$.

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 $x_1, \ldots, x_g$ on X such that the restriction map $\mathrm{H}^0(X, \Omega^1) \to \prod_{i=1}^g T_{x_i}^*$ is an isomorphism.

Given $(D, D') \in U$, there is a non-zero meromorphic function f on X, unique up to scaling, such that $D'' = \operatorname{div}(f) + D + D - g[x]$ is effective. We define a map $U \to X^{(g)}$ 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 groupg (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 $\phi : \operatorname{Div}^0(X) \to J$ 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 finds 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, ϕ gives a map of functors $F \to J$. 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 $T_0(\operatorname{Jac}(X)) = \mathrm{H}^1(X, \mathcal{O})$ using the functor of points of $\operatorname{Jac}(X)$ and the interpretation of the tangent space in terms of dual numbers.
- From this, one finds that $\mathrm{H}^0(\operatorname{Jac}(X), \Omega^1)$ is naturally isomorphic to $\mathrm{H}^0(X, \Omega^1)$.
- One again has a map $f_x : X \to \operatorname{Jac}(X)$ 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, $\operatorname{Jac}(X)(k)$ is isomorphic to $\operatorname{Pic}^0(X)$.

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

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

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

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

Now, we also have

$$\mathrm{H}^1(X_{\overline{k}}, \mathbf{G}_m) = \operatorname{Pic}(X_{\overline{k}}).$$

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

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

Replacing n with ℓ^n and taking an inverse limit, we find

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

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 $J := \mathrm{Jac}(X)$ 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*

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

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 π_X. To prove the identity

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

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

Theorem 9.2. *Let X be a nonsingular complete curve of genus g over a finite field $\mathbf{F}_q$, and $J := \mathrm{Jac}(X)$ 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*

$$|\,\mathrm{Tr}(\pi_X)| \le g \cdot \lfloor 2\sqrt{q} \rfloor.$$

This is an equality if and only if either $\alpha_i + \overline{\alpha}_i = \lfloor 2\sqrt{q} \rfloor$ for all i or $\alpha_i + \overline{\alpha}_i = -\lfloor 2\sqrt{q} \rfloor$ 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*

$$q + 1 - g\lfloor 2\sqrt{q} \rfloor \le \#X(\mathbf{F}_q) \le q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

9.2 Examples: curves of genus ≤ 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 $q + 1 + g\lfloor 2\sqrt{q}\rfloor$ over $\mathbf{F}_8$. Note that in this case Serre's bound is better than the original Hasse–Weil bound: $8 + 1 + 3\lfloor 2\sqrt{8}\rfloor = 24$, whereas $8 + 1 + \lfloor 6\sqrt{8}\rfloor = 25$.

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 $A = \mathrm{Jac}(X)$ 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 primes 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

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

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^σ is the $\mathrm{Gal}(F/\mathbf{Q})$-conjugate of A_f. The endomorphism ring of the surface A_f is $\mathrm{End}_F(A_f) = \mathbf{Z}[\sqrt{3}]$. 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 $\mathrm{End}_{\mathbf{F}_\mathfrak{p}}(A_f \times_{\mathcal{O}_F} \mathbf{F}_\mathfrak{p}) \supset \mathbf{Z}[\sqrt{3}]$.

10 Dieudonné modules and p-divisible groups

We have seen that the notion of ℓ-adic Tate modules, for primes ℓ 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*

$$\{G_n : i_n : G_n \to G_{n+1}\}_{n\in\mathbf{N}} : \qquad G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \xrightarrow{i_3} \cdots,$$

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 $i_n : G_n \to G_{n+1}$ 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 $S = \operatorname{Spec}(k)$. 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 $f : A \to B$ is a homomorphism of abelian varieties over k, it induces a homomorphism of p-divisible groups $f_\infty : A[p^\infty] \to B[p^\infty]$.

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 $T_pG := \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, G(\overline{k}))$. Concretely, we take the limit of the projective system

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

When $p \neq \mathrm{char}(k)$, then the p-adic Tate module of an abelian variety A is $T_p(A[p^\infty]) = T_pA$ 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 [6] for a detailed exposition on Dieudonné theory, and [1] for a concise summary.

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

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

(ii) $(V_{G/k})^D = F_{G^D/k}$ *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 [12]). 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 σ 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*

$$\begin{aligned} &FV = VF = p \\ &F\alpha = \sigma(\alpha)F, \ \textit{and}\ \alpha V = V\sigma(\alpha), \ \textit{for all}\ \alpha \in W(k). \end{aligned}$$

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 [1, Theorem 1.4.3.2]).

Theorem 10.5. *There is an additive anti-equivalence of categories between the category of finite commutative group schemes of p-power order over k and left $\mathbf{D}_k$-modules of finite $W(k)$-length. Writing $\mathbf{M}(G)$ for the $\mathbf{D}_k$-module associated to G, we have the following.*

1. *G has order p^r, where r is the $W(k)$-length of $\mathbf{M}(G)$.*

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 $F_{G/k} : G \to G^{(p)}$ corresponds to the linearisation*

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

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

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

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. [12, 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

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

By semilinearity, we have

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

the requirement that $FV = p$ implies that at least one of α and β must be zero. Conversely, if at least one of α and β 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 α and β become

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

Since k is algebraically closed, we may thereby arrange by a change of basis that if one of α and β is nonzero then it is in fact equal to 1. Thus we obtain three possibilities for the pair (α, β) 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 μ_p and α. The first, μ_p, is the kernel of the p-th power map acting on the multiplicative group $\mathbf{G}_m$; specifically, the scheme is $\operatorname{Spec} k[x]/(x^p - 1)$, and the group law is multiplication. The second, α_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 μ_p is $\mathbf{Z}/(p)$, which is étale, so its Verschiebung is nonzero. Thus, μ_p corresponds to the pair $(0,1)$. On the other hand, one can show that α_p is its own Cartier dual, which is again infinitesimal, so α_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 α_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 [10] 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 ℓ-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 ℓ-adic case we will now write T_pG for $\mathbf{M}(G)$ and T_pA for the case $G = A[p^\infty]$. The $\mathbf{D}_k$-module T_pG will be the replacement for the ℓ-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 ℓ-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 $V_pG := \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_pG$ (and write V_pA for $G = A[p^\infty]$). Then V_pG 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 an abelian varieties over k, and $A[p^\infty]$ and $B[p^\infty]$ their associated p-divisible groups. Then the map*

$$\mathbf{Z}_p \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A, B) \to \mathrm{Hom}_{\mathbf{D}_k}(T_pB, T_pA) \tag{4}$$

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

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

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

$$V_pA = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_pA.$$

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

$$\mathbf{Z}_p \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A,B) \to \mathrm{Hom}_{\mathbf{D}_k}(T_pB, T_pA) \tag{5}$$

is an isomorphism. The proof of injectivity is essentially the same as in the ℓ-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

$$\mathbf{Q}_p \otimes_{\mathbf{Z}} \mathrm{End}_k^0(A) \to \mathrm{End}_{\mathbf{D}_k[1/p]}(V_p(A))$$

is surjective for A k-simple. 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

$$h = \alpha \cdot g(F) + (c_0 + c_1F + \dots + c_{d-1}F^{d-1}), \text{ with } c_0, \dots c_{d-1} \in K_0 \text{ and } \alpha \in \mathbf{D}_k[1/p].$$

The result then follows. □

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 $\mathrm{Gal}(K_0/\mathbf{Q}_p) = \langle\sigma\rangle$, where σ is the automorphism lifting the arithmetic Frobenius. Let $\Delta := \mathbf{D}_k[1/p]/(g(F^n))$. Then, there is an isomorphism between Δ 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 tha the map

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

is an isomorphism. This makes Δ into a cyclic E-algebra, i.e. Δ 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.*

Proof. Let $\sigma : K_0 \to K_0$ 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 isomorphism 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 a contained in D'. Since L/E is ramified, it doesn't split $\Delta := \Delta_0 \otimes_E L$, the base change of the Δ_0 to L. So Δ 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 such that $h(0) \neq 0$. Let $L := \mathbf{Q}_p[x]/(h)$ and $D' := \mathbf{D}_k[1/p]/(h(F^n))$, M a finite D'-module. Then, we have*

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

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 $C = \mathrm{End}_{D'}(M)$ and the bi-commutant of C is $D' := \mathrm{End}_C(M)$. 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 $D := \mathrm{End}_k^0(A)$, and recall that, by Albert classification theorem, the centre of D is $Z = \mathbf{Q}[\pi_A]$. The geometric Frobenius π_A acts on V_pA simply. By functoriality of Dieudonné modules, we have $V_p(\pi_A) = F^n$. Therefore, it is enough to show that

$$\dim_{K_0} \mathbf{Q}_p \otimes_{\mathbf{Z}} \mathrm{End}_k^0(A[p^\infty]) = \dim_{K_0} \mathrm{End}_{\mathbf{D}_k[1/p]}(V_p(A))^{\mathrm{opp}}.$$

Since the centre $Z(\mathbf{D}_k[1/p]) = \mathbf{Q}_p[F^n]$ and π_A maps to $V_p(\pi_A)$, the actions of Z and $\mathbf{D}_k[1/p]$ on $V_p(A)$ commute.

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 π_A and $r \geq 1$ an integer. So, we have

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

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

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

Since $g_{A,v}$ is the minimal polynomial of Z_v over $\mathbf{Q}_p$, we see that $g_{A,v}(F^n) \in \mathbf{D}_k$ acts on G_v through the element $g_{A,v}(\pi_A) = 0$. So $V_p(G_v)$ is a left module over the quotient algebra

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

From this, we get the following decompositions, which are compatible:

$$\mathrm{End}_{K_0[F^n]}(V_p(A)) \simeq \prod_{v|p} \mathrm{End}_{K_0[F^n]}(V_p(G_v)) \text{ and } \mathrm{End}_{\mathbf{D}_k[1/p]}(V_p(A)) \simeq \prod_{v|p} \mathrm{End}_{D_v}(V_p(G_v)).$$

So, we are reduced to proving

$$\dim_{K_0} \mathrm{End}_{K_0[F^n]}(V_p(G_v)) = \dim_{\mathbf{Q}_p} \mathrm{End}_{D_v}(V_p(G_v)), \text{ for all } v \mid p.$$

The result now follows from Corollary 10.11. □

10.5 Local invariants for abelian varieties

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

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

This yields a corresponding decomposition of $G := A[p^\infty] = \prod_{v|p} G_v$ (up to isogeny) into a product of p-divisible groups over k, where G_v is defined over Z_v. Since the Dieudonné functor is fully faithful and contravariant, and the map in Theorem 10.6 is an isomorphism for finite k, we may identify the central $Z \otimes_{\mathbf{Q}} \mathbf{Q}_p$-algebra $D \otimes_{\mathbf{Q}} \mathbf{Q}_p$ with the opposite $Z \otimes_{\mathbf{Q}} \mathbf{Q}_p$-algebra to $\mathrm{End}_{\mathbf{D}_k[1/p]}(V_p A)$. In particular, $V_p(\pi_A)$ acts as $F^n \in \mathbf{D}_k[1/p]$, and so we get

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

We conclude that the right side is a central simple Z_v-algebra, and our goal is to compute its invariant. By functoriality, we know that π_A acts on $V_p G_v$ as $V_p(\pi_A) = F^n$, and we have

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

For each $v \mid p$, the Z_v-action on the nonzero $V_p(G_v)$ commutes with the $\mathbf{D}_k[1/p]$-action (as it arises from an action of Z_v on the p-divisible group G_v in the isogeny category over k), and the central element $g_{A,v}(F^n) \in \mathbf{D}_k[1/p]$ acts as multiplication by the element $g_{A,v}(\pi_A) \in Z_v$ that is zero. In other words, $V_p(G_v)$ is a nonzero module over the ring

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

We want to compute local invariants $\mathrm{inv}_v(D_v)$ for all place $v \mid p$ of Z. By Theorems 10.10 and 11.2, the class of D_v in $\mathrm{Br}(Z_v)$ 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 $\sigma' \in \mathrm{Gal}(K_0 Z_v/Z_v)$ is the arithmetic Frobenius and the element $\pi^{f_v/g_v} \in Z_v^\times$ where $f_v = f(v \mid p)$ and $g_v = \gcd(f_v, n)$. Since $[K_0 Z_v : Z_v] = n/g_v$, the formula in Theorem 11.2 gives

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

Let $e_v = e(v \mid p)$, 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

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

11 Brauer group and local invariants of division algebras

Lemma 11.1. *Let F be a field and E/F a cyclic extension. Fix a generator σ of $\Gamma := \mathrm{Gal}(E/F)$, and let $\chi_\sigma : \Gamma \to \mathbf{Q}/\mathbf{Z}$ be the unique homomorphism given by*

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

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

$$\widehat{\mathrm{H}}^0(\Gamma, E^\times) \overset{\cup\theta_\sigma}{\simeq} \mathrm{H}^2(\Gamma, E^\times).$$

Then, we have the following.

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

$$E^\times / \mathrm{Nm}_{E/F}(E^\times) \to \mathrm{Br}(F).$$

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

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

Proof. See [1, Appendix A] or Serre [12, Chapter V, Section 4]. □

Theorem 11.2. *Let F be a non-archimedean local field and E/F an unramified finite extension. Let $\phi \in \mathrm{Gal}(E/F)$ 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 $\mathrm{ord}_F(c)/[E:F]$.*

Proof. See [1, Appendix A] or Serre [12, Chapter V, Section 4]. □

References

[1] C-L. Chai, B. Conrad, and F. Oort, *Complex Multiplication and Lifting Problems*, American Mathematical Society, 2014.

[2] 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

[3] 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

[4] Robin Hartshorne, *Algebraic geometry*, Grad. Texts in Math., No. **52** Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp.

[5] B. Edixhoven, B Moonen and G. van der Geer, *Abelian varieties*. Available at http://van-der-geer.nl/~gerard/AV.pdf.

[6] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Société Mathématique de France, in Astérisque, 1977.

[7] B. Lawrence, *Dieudonné modules and p-divisible Groups*. Available at http://virtualmath1.stanford.edu/~conrad/JLseminar/Notes/L17I.pdf.

[8] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR 861974

[9] 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

[10] 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

[11] 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

[12] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

[13] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, Grad. Texts in Math., 106 Springer, Dordrecht, 2009. xx+513 pp.

[14] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 13400144. MR 206004

[15] 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

[16] W. Trappe and L. C. Washington, *Introduction to cryptography with coding theory*, Pearson Prentice Hall, Upper Saddle River, NJ, 2006, xiv+577 pp.

[17] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969), 521–560. MR 265369

[18] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer, 1979.