The Tate Conjecture for Abelian Varieties over Finite Fields

Sjoerd Wijnand de Vries

Born 28 August 1997 in Schoorl, The Netherlands

05.07.2021

Master's Thesis Mathematics

Advisor: Prof. Dr. Peter Scholze

Second Advisor: Dr. Marco D'Addezio

Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Contents

Contents i

Introduction iii

I Tate's Theorem 1

1 Abelian varieties 2
1.1 Basics 2
1.2 Projectivity of abelian varieties 4
1.3 Isogenies 5
1.4 Endomorphism algebras 9
1.5 The Tate module 10
1.6 The dual abelian variety 13
1.7 Riemann-Roch for abelian varieties 17
1.8 Characteristic polynomials 21
1.9 Weil pairings 23
1.10 Polarisations 24

2 Tate's theorem 27
2.1 Statement of the theorem 27
2.2 Reduction steps 29
2.3 The proof 31
2.4 Consequences 36

II Motives and the Tate conjecture 40

3 Preliminaries 41
3.1 Affine groups 41
3.1.1 Representations 41
3.1.2 Tannakian categories 42
3.2 CM abelian varieties 45
3.2.1 Complex multiplication 45
3.2.2 Reduction of CM abelian varieties 48
3.3 Motives 49
3.3.1 Motivation 49
3.3.2 Construction of the category of motives 50
3.3.3 Realisation functors 53
3.3.4 Motives of abelian varieties 55
3.3.5 Lefschetz motives 55
3.3.6 The Frobenius endomorphism of a motive 56
3.3.7 Some fundamental groups 57
3.3.8 The Lefschetz group 59

4 Hodge implies Tate **63**

4.1 Overview . . . 63

4.2 Construction of the commutative square . . . 64

4.2.1 The categories . . . 64

4.2.2 The functors . . . 65

4.2.3 A filtration by CM fields . . . 66

4.3 Calculation of the character groups . . . 67

4.3.1 $X^*(T^K)$ . . . 68

4.3.2 $X^*(L^K)$ . . . 69

4.3.3 $X^*(S^K)$ . . . 69

4.3.4 The maps between the character groups . . . 70

4.4 $P = S \cap L$ . . . 73

4.4.1 Set-up and notation . . . 74

4.5 Proof of the main theorem . . . 78

Bibliography **82**

Introduction

Around the 1960's, a revolution was taking place in algebraic geometry, stimulated primarily by Weil's conjectures on the zeta functions of varieties over finite fields. Grothendieck's school had just developed the theory of schemes, and used this to attack the problem. It was clear to those involved that the conjectures could be proven if one could construct a cohomology theory for varieties over finite fields which behaves just like singular cohomology does in the analytic setting. Such a cohomology theory, considered as a functor $H^\bullet\colon \mathcal{V}_k \to \mathsf{Vec}_{\mathbb{K}}$, where $\mathcal{V}_k$ is the category of smooth projective varieties over k and where $\mathbb{K}$ is a field of characteristic zero, is now called a Weil cohomology theory.

The first Weil cohomology theory to be discovered was étale cohomology, and part of its power stems from the fact that it admits an action of the Galois group of the base field. For a variety X/k and any prime $l \neq \operatorname{char}(k)$, one can consider the l-adic cohomology

$$H_l^\bullet(X) := \bigoplus_{r=0}^{2\dim(X)} H^r(\bar{X}, \mathbb{Q}_l) := \bigoplus_{r=0}^{2\dim(X)} \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \varprojlim_n H^r(\bar{X}, \mathbb{Z}/l^n\mathbb{Z}),$$

where $\mathbb{Z}/l^n\mathbb{Z}$ is seen as a constant sheaf on the étale site of $\bar{X} := X \times_k \bar{k}$. Now $\operatorname{Gal}(k)$ acts on $\bar{X}$ through the second factor, which induces an action on the étale site. This is possible because, as Tate puts it [Tat65], the étale topology depends only on $\bar{X}$ and not on the arrow $\bar{X} \to \operatorname{Spec}(\bar{k})$.

Cohomology provides a link between zeta functions and algebraic cycles. Denote by $\mathcal{Z}^r(X)$ the free abelian group on the set of codimension r irreducible closed subvarieties of X. Then there is for each $0 \leq r \leq \dim(X)$ a cycle class map

$$\operatorname{cl}^r\colon \mathcal{Z}^r(X) \longrightarrow H^{2r}(\bar{X}, \mathbb{Q}_l(r)), \tag{1}$$

where the notation $\mathbb{Q}_l(r) := (\mathbb{Q}_l \otimes_{\mathbb{Z}_l} \varprojlim_n \mu_{l^n}(\bar{k}))^{\otimes r}$ denotes a Tate twist.

The theme of this thesis will be a conjecture posed by Tate in 1963 about this cycle class map.

Conjecture 0.0.1 (Tate Conjecture)**.** Let k be a field which is finitely generated over its prime field, and let X/k be a smooth projective variety. Then the kernel of the cycle class map (1) consists of the cycles numerically equivalent to zero, and induces for each r an isomorphism

$$\operatorname{CH}^r_{\text{num}}(X) \otimes \mathbb{Q}_l \xrightarrow{\sim} H^{2r}(\bar{X}, \mathbb{Q}_l(r))^{\operatorname{Gal}(k)}.$$

For the definition of numerical equivalence, see Example 3.3.2.3.

It is known that the zeta function $\zeta(X, s)$ of a d-dimensional variety X over a finite field has simple poles at $s = 1, 2, \ldots, d$. For k a finite field, the Tate conjecture is equivalent to the following statement: if the Frobenius of X acts semisimply on the l-adic cohomology, then the residue of the pole of $\zeta(X, s)$ at $s = r$ equals the dimension of $\operatorname{CH}^r_{\text{num}}(X)$. Thus, much like the Weil conjectures, the Tate conjecture seeks to answer a natural question about zeta functions.

Deligne famously proved the Weil conjectures in the early 70's. In contrast, at the time of writing, the Tate conjecture is still wide open. The first non-trivial case was proven by Tate himself in 1966: it restricts to the case where $r = 1$ and X is an abelian variety over a finite field. In this setting, the Tate conjecture can be phrased without reference to étale cohomology, and is now known as Tate's (isogeny) theorem. This result was extended by Zarhin to function fields over finite fields [Zar75], and by Faltings to number fields [Fal83], which was enough to deduce the result for all finitely generated fields. For K3 surfaces, the only non-trivial case is $r = 1$. The proof of Tate conjecture in this setting has been a major achievement and was completed only recently: the final brick was laid in 2016 in the erratum to [KMP16], after proofs in odd characteristic [MP15], [Cha13]. The proof uses a reduction to abelian varieties via the Kuga-Satake construction. Besides this, only few cases are known.

The topic of this thesis is the Tate conjecture for abelian varieties over finite fields. Aside from the proof for $r = 1$ by Tate mentioned above, we will focus on a notable result which relies on the theory of motives. Grothendieck envisioned the theory of motives as the key to proving the Weil conjectures, but it has never really gotten off the ground. The reason is that the theory of motives works well only if one assumes Grothendieck's standard conjectures, which are deep conjectures on algebraic cycles which nobody knows how to solve. However, when we work with abelian varieties over finite fields, we know that the Künneth components of the diagonal are algebraic, which gives us some room to manoeuvre. We will use the theory of motives to prove the following theorem by Milne:

Theorem 0.0.2. If the Hodge conjecture is true for CM abelian varieties over $\overline{\mathbb{Q}}$, then the Tate conjecture is true for abelian varieties over finite fields.

The outline of the thesis is as follows.

Part I revolves around Tate's theorem. We give an introduction to the theory of abelian varieties, focusing on the important concepts and theorems and leaving out most of the technical proofs, for which the reader is referred to [EvdGM] or [Mum74]. Main results include Riemann-Roch (1.7.6) and the Riemann hypothesis (1.10.6) for abelian varieties. Afterwards, we go through the proof of Tate's theorem in detail.

Part II is devoted to a proof of Theorem 0.0.2. It relies on the theory of motives and the Tannakian formalism, and we again introduce the necessary theory before delving into the proof, which follows Milne's articles [Mil94], [Mil99a], and [Mil99b]. The strategy is to translate the Tate conjecture into a statement about affine groups arising as fundamental groups of Tannakian categories (4.1.3 and 4.5.2). We then try to understand these groups, both directly and by working with the categories. The theory of abelian varieties is sufficiently well-understood to describe the groups and their characters in detail. If we additionally assume the Hodge conjecture, we can make use of the category of Hodge motives. Putting these together allows us to prove the Tate conjecture.

Throughout the thesis, a good knowledge of algebraic geometry and representation theory is assumed. We will also use standard results on étale cohomology without proof. Otherwise, the thesis is intended to be as self-contained as possible, with either proofs or references provided for all results we use.

Acknowledgements

First and foremost, I would like to thank my supervisor, Dr. Marco D'Addezio, for taking on his role with such enthusiasm and dedication. I am grateful for his explanations and suggestions, his willingness to discuss anything mathematical (be it inside our outside parentheses), his insistence on understanding the smallest details, and his constant encouragement over the past months, which have influenced not only this thesis but also my general development as a mathematician.

Secondly, I would like to thank Prof. Dr. Peter Scholze, for his willingness to be involved in the thesis and in particular for agreeing to be my formal supervisor.

Lastly, I owe more than I can say to my friends and family, who have constantly supported me throughout my studies and who I can always count on when I need a break. Especially during the pandemic, it has been invaluable having them around, and I wish to thank all of them for their invisible, but not insignificant contribution to this thesis.

Notation

- Unless mentioned otherwise, a scheme will always mean an object in the category Sch_k of schemes over a field k of characteristic $p \geq 0$, not necessarily algebraically closed.
- By a variety we will mean a separated, geometrically integral scheme of finite type over k.
- The projection morphism from a product onto its i^{th} factor is denoted by pr_i.
- A vector bundle will always mean a locally free sheaf of finite rank, and line bundles will mean invertible sheaves.
- The tangent space of a scheme X at a point x will be denoted by $\text{Tgt}_x(X)$.
- In the context of abelian varieties, the letter g will denote the dimension.
- For an abelian variety A over k, the notation $\text{End}^0(A)$ will mean $\mathbb{Q} \otimes_{\mathbb{Z}} \text{End}_k(A)$.
- If G is an affine k-group, its characters will be denoted by $X(G) := \text{Hom}_k(G, \mathbb{G}_m)$. Its geometric characters are denoted by $X^*(G) := \text{Hom}_{k^{\text{sep}}}(G_{k^{\text{sep}}}, \mathbb{G}_{m,k^{\text{sep}}})$, but will often also be referred to as the characters of G.

Part I

Tate's Theorem

1. Abelian varieties

An abelian variety is a projective variety with a group structure. In this chapter, we will explore some of their properties, as preparation for Tate's theorem. We will see that just the existence of a group structure imposes heavy restrictions on the geometry of varieties. It makes abelian varieties nice objects to work with, but one should always keep in mind that they are a very special class of varieties.

1.1 Basics

We will start off with the definition of an abelian variety.

Definition 1.1.1. Let k be a field. A *group variety* is a group object in the category of varieties over k. An *abelian variety* is a complete group variety (i.e. for any variety Y, the second projection $X \times Y \to Y$ is closed). We write $e \in X(k)$ for the identity element and $m\colon X \times_k X \to X$ and $i\colon X \to X$ for the multiplication and inverse morphisms, respectively. A *homomorphism of group varieties* is a morphism of varieties respecting the group scheme structure.

Examples 1.1.2.
1. The unique zero-dimensional abelian k-variety is $\mathrm{Spec}(k)$. Extensions K/k don't work, as these don't possess any k-points, so they can't have an identity element. Another way to see it is that $\mathrm{Hom}_k(\mathrm{Spec}(k), \mathrm{Spec}(K)) = \emptyset$ and thus the functor of points for $\mathrm{Spec}(K)$ can't factor through Grp.
2. Any one-dimensional abelian variety is an elliptic curve. Let $k = \mathbb{R}$ and let E be an elliptic curve over k. The fact that it is a group object implies that $E(\mathbb{R})$ has a natural group structure. One can draw these $\mathbb{R}$-points by taking a Weierstrass equation $y^2 = x^3 + ax + b$ and drawing its solutions in the xy-plane; since we are dealing with a projective variety, one should not forget about the point at infinity.
The group law is now given as follows: given points P and Q on the curve, let Z be the point of intersection of the line through P and Q with the curve. Then $P + Q$ is the third point on the line through Z and infinity (a vertical line). Note that the point at infinity acts as the identity element.
3. For any smooth projective curve C of genus g, its Jacobian $\mathrm{Jac}(C)$ is a g-dimensional abelian variety. If C is an elliptic curve, $C \cong \mathrm{Jac}(C)$.
4. Finite products of abelian varieties are abelian varieties.

More examples of abelian varieties can be obtained through identity components of subgroup schemes of abelian varieties [EvdGM, Prop. 3.17]:

Proposition 1.1.3. Let X be an abelian variety and let $G \subset X$ be a subgroup scheme. Denote by $Y = G^0_{\mathrm{red}}$ the reduced subscheme underlying the connected component of G containing the identity element. Then Y is an abelian variety.

Lemma 1.1.4 (Rigidity lemma)**.** Let X be an abelian variety and let Y, Z be k-varieties. Suppose a morphism $f\colon X \times Y \to Z$ is constant when restricted to a fibre $X \times \{y\}$ for some $y \in Y(k)$. Then f factors through the projection $\pi_Y\colon X \times Y \to Y$.

Proof. Without loss of generality, $k = \bar{k}$ and we may check the statement on k-points.
Let $f|_{X \times \{y\}} = z$ and pick an affine open neighbourhood $U \ni z$. The pre-image $f^{-1}(Z \setminus U)$ is closed, so by completeness of X, so is the projection $\pi_Y(f^{-1}(Z \setminus U))$. Let V be its complement. Then by construction, for any closed point $y' \in V$, we have $f(X \times \{y'\}) \subset U$. But X is complete

and U is affine, so f is constant on such a fibre.
So f factors through π_Y on $X \times V$, where $V \subset Y$ is an open set. As Y is irreducible, this is enough. □

Definition 1.1.5. Let $x \in X(k)$. Define the *right translation by x* to be the morphism

$$t_x \colon X \xrightarrow{\sim} X \times_k k \xrightarrow{\mathrm{id} \times x} X \times_k X \xrightarrow{m} X.$$

It is an isomorphism with inverse $t_{i(x)}$.

Proposition 1.1.6. Let X and Y be abelian varieties. Then any morphism $X \to Y$ is a translation of a homomorphism.

Proof. Let $f : X \to Y$ be a morphism. Let $g := t_{i(f(e_X))} \circ f$. Then $g(e_X) = e_Y$, and we want to show that $g(x + x') = g(x) + g(x')$. For this, consider the morphism

$$\varphi : \; X \times X \xrightarrow{(g \circ m_X) \times (i_Y \circ m_Y \circ (g \times g))} Y \times Y \xrightarrow{m_Y} Y$$

Then $\varphi|_{X \times \{e_X\}} = e_Y = \varphi|_{\{e_X\} \times X}$. By Lemma 1.1.4, φ factors through both the first and the second projection, so $\varphi = e_Y$ is constant. So $g \circ m_X = m_Y \circ (g \times g)$, i.e. g is a homomorphism. □

Corollary 1.1.7. The group law on an abelian variety is commutative. That is, $m \circ \tau = m$, where τ is the map swapping the two factors of the product.

Proof. By Proposition 1.1.6, $i \colon X \to X$ is a homomorphism. □

Corollary 1.1.7 justifies the usage of additive notation for abelian varieties. We will follow this, and from now on write 0 for the identity element of an abelian variety, $+$ for the multiplication law, and $-$ for the inversion law.

Proposition 1.1.8. Any abelian variety X is smooth and has trivial tangent bundle.

Proof. Because X is a variety, it contains an open dense smooth subscheme, which we can move around by the translation isomorphisms, showing that X is smooth at every geometric point. In a similar way, by translating tangent vectors one can show that $\pi^* \mathrm{Tgt}_0(X) \xrightarrow{\sim} \mathcal{T}_{X/k}$, where $\pi : X \to k$ is the structure morphism [EvdGM, Prop. 1.5]. □

The next statements are classical results that will allow us to understand the behaviour of line bundles on abelian varieties. See [EvdGM, Chapter II] for proofs.

Proposition 1.1.9 (See-Saw Principle)**.** Let X be a complete variety and Y any other variety. Let $\mathcal{L}$ be a line bundle on $X \times Y$ such that $\mathcal{L}|_{X \times \{y\}} \cong \mathcal{O}_X$ for all $y \in Y(k)$ and that $\mathcal{L}|_{\{x\} \times Y} \cong \mathcal{O}_Y$ for one $x \in X(k)$. Then $\mathcal{L}$ is trivial.

Theorem 1.1.10 (Theorem of the Cube)**.** Let $\mathcal{L}$ be a line bundle on an abelian variety X, and let $f, g, h \colon Y \to X$ be morphisms. Then the bundle

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

is trivial.

Corollary 1.1.11 (Theorem of the Square)**.** Let $\mathcal{L}$ be a line bundle on an abelian variety X. Then for all $x, y \in X(k)$,

$$t_{x+y}^* \mathcal{L} \otimes \mathcal{L} = t_x^* \mathcal{L} \otimes t_y^* \mathcal{L}.$$

Proof. Apply the Theorem of the Cube with $Y = X$, $f = x$, $g = y$, and $h = \mathrm{id}_X$. Indeed, $t_x = x + \mathrm{id}_X$, and the pullback of a line bundle under a constant map is just $\mathcal{O}_X$. □

1.2 Projectivity of abelian varieties

As alluded to before, any abelian variety is in fact projective. The goal of this section is to prove this. We will quickly recall some generalities on line bundles and their interplay with projectivity. All the statements quoted without proof can be found in standard texts on algebraic geometry, e.g. [Har77].

Since abelian varieties are smooth, noetherian, integral and separated, there is an isomorphism $\operatorname{Pic}(X) \xrightarrow{\sim} \operatorname{Cl}(X)$, so we can identify line bundles with divisors. This allows us to speak of the degree of a line bundle and to associate adjectives to it normally related to divisors, such as effective.

Definition 1.2.1. Let X be a scheme and let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. We say $\mathcal{F}$ is *globally generated* if there is an indexing set I and a surjective map $\bigoplus_I \mathcal{O}_X \to \mathcal{F}$.
Let now $\mathcal{L}$ be a line bundle on a quasi-compact scheme X. We say $\mathcal{L}$ is *very ample* if there exist sections $s_0, \dots, s_n \in \Gamma(X, \mathcal{L})$ such that each $D(s_i) = \{x \in X \mid (s_i)_x \notin \mathfrak{m}_x \mathcal{L}_x\}$ is affine and $X = \bigcup_i D(s_i)$. We say $\mathcal{L}$ is *ample* if some power of it is very ample. If X is noetherian, equivalently $\mathcal{L}$ is ample if for all coherent sheaves $\mathcal{M}$, there exists $m > 0$ s.t. $\mathcal{M} \otimes \mathcal{L}^{\otimes m}$ is globally generated, or equivalently if this holds for all coherent ideal sheaves $\mathcal{M}$.

Proposition 1.2.2. A finite type k-scheme X admits an ample line bundle if and only if it is quasi-projective. More precisely, if $i \colon X \to \mathbb{P}^n_k$ is a locally closed immersion, then $i^*\mathcal{O}(1)$ is ample. Conversely if $\mathcal{L}$ is an ample line bundle, one may take a very ample power of it. Then the non-vanishing sections $s_0, \dots, s_n$ define a locally closed immersion $X \to \mathbb{P}^n_k$.

Corollary 1.2.3. A proper and finite type k-scheme is projective if and only if it admits an ample line bundle.

Since abelian varieties are proper by definition, we can show they are projective by finding an ample line bundle. Our proof of projectivity will rely on the following lemma, which is preceded by a definition.

Definition 1.2.4. Let D be a divisor on a smooth proper k-scheme X. The *complete linear system defined by* D is defined as the set of divisors linearly equivalent to D, and denoted $|D|$. Say $|D|$ is *basepoint-free* if the common support of $|D|$ is empty, i.e. if and only if $\mathcal{O}(D)$ is globally generated.

Note that a base-point free linear system defines a morphism to $\mathbb{P}^n$, where $n+1 = \dim_k \Gamma(X, \mathcal{O}(D))$. The following lemma gives criteria for this to be a closed immersion.

Lemma 1.2.5. Suppose D is a divisor such that $|D|$ is base-point free. Then D is very ample if and only if it separates points and it separates tangent vectors, i.e.

1) For all $x, y \in X$ there exists $s \in \Gamma(X, \mathcal{O}(D))$ such that $s(x) = 0$ and $s(y) \neq 0$;

2) For all $x \in X$ there exists $s \in \Gamma(X, \mathcal{O}(D))$ such that $s_x \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$.

We can now give a geometric proof that abelian varieties are projective.

Theorem 1.2.6. Any abelian variety is projective.

Proof. Since $\operatorname{Spec}(k)$ is projective, we may assume $\dim X > 0$. Take D to be a finite sum of distinct prime divisors whose common support is $\{0\}$ and write $D = \sum_i D_i$, defined over k. Since a line bundle is ample if and only if it is ample after a base change to an algebraic closure, we may now assume $k = \bar{k}$.

Recall that by the Theorem of the Square, $t_x^*\mathcal{L} \otimes t_y^*\mathcal{L} \cong t_{x+y}^*\mathcal{L} \otimes \mathcal{L}$. Thus for any divisor D', we have $nD' \sim \sum_{i=1}^n t_{x_i}^* D'$ whenever $\sum x_i = 0$. In particular, for any $a, b \in X(k)$, we have $t_a^* D + t_b^* D + t_{-a-b}^* D \sim 3D$.

We use this to show that $3D$ separates points. Let $x \neq y \in X$; we need to show that there is some $D' \sim 3D$ with $x \in \operatorname{supp}(D')$ but $y \notin \operatorname{supp}(D')$. Since $y - x \neq 0$, there is some D_i such that $y - x \notin \operatorname{supp}(D_i)$, so $y \notin \operatorname{supp}(t_x^* D_i)$. On the other hand, $x \in \operatorname{supp}(t_x^* D_i)$ since $0 \in \operatorname{supp}(D_i)$.

By dimension arguments we can find b such that $y \notin \operatorname{supp}(t_b^* D_i) \cup \operatorname{supp}(t_{-x-b}^* D_i)$. Now for the $j \neq i$, choose a_j and b_j such that

$$y \notin \operatorname{supp}(t_{a_j}^* D) \cup \operatorname{supp}(t_{b_j}^* D) \cup \operatorname{supp}(t_{-a_j-b_j}^* D);$$

then for $a_i = -x$ and $b_i = b$, we get

$$3D \sim \sum_{j=1}^n t_{a_j}^* D_j + t_{b_j}^* D_j + t_{-a_j-b_j}^* D_j,$$

which is a divisor separating x from y.

Next we need to separate tangent vectors. For this, let $0 \neq \tau \in \operatorname{Tgt}_x(X)$ be a tangent vector at x; so $t_{-x}^* \tau \in \operatorname{Tgt}_0(X)$. If $t_{-x}^* \tau$ were tangent to all the D_i at 0, the intersection multiplicity of the D_i at 0 would be greater than 1, contradicting our assumption. So some D_i is not tangent to $t_{-x}^* \tau$. Then choose $a_i = -x$, and let the other a_j and b_j be such that x does not lie in the support of each of the other terms in the sum which will be linearly equivalent to $3D$; then this gives a divisor which contains x in its support, but such that τ is not tangent to it. □

Remark 1.2.7. In fact, something even stronger is true: if $\mathcal{L}$ is any ample line bundle on an abelian variety, then $\mathcal{L}^{\otimes 3}$ is very ample. The proof of this surprising fact is more technical than our given proof because we can make no choices for the D we start with, but the general idea is the same. It can be found in [Mum74, §17, p. 163]. There is also a more arithmetic proof of projectivity of abelian varieties, which uses properties of the Mumford bundle (cf. Remark 1.6.11).

1.3 Isogenies

To prepare for the notion of an isogeny between abelian varieties, we review some facts about finite group schemes. A finite group scheme over a base S is a group object in Sch_S whose structure morphism is finite. When dealing with abelian varieties, finite group schemes naturally appear, for instance as kernels of morphisms.

Definition 1.3.1. Let $f\colon X \to Y$ be a homomorphism of abelian varieties. The kernel of f is the fibre over $0 \in Y$, i.e. the pullback

$$\begin{tikzcd}
\ker f \arrow[r, hook] \arrow[d] & X \arrow[d, "f"] \\
\operatorname{Spec}(k) \arrow[r, hook, "0"] & Y
\end{tikzcd}$$

Kernels are projective, since abelian varieties are, but they are in general no longer reduced or irreducible. Note also that for any $y \in Y(k)$, the pre-image $f^{-1}(y)$ is isomorphic to $\ker f$ via a translation.

The following general proposition shows that kernels are indeed group schemes:

Proposition 1.3.2. Let G be a group scheme over some base S, and let $S' \to S$ be a morphism. Then the base change $G' = G \times_S S'$ is a group scheme over S'.

Proof. The Yoneda point of view tells us that being a group object in a category is equivalent to the functor of points factoring through Grp. Thus, it suffices to show that $\operatorname{Hom}_{S'}(X, G')$ has a group structure functorial in X. To see this, note that for any S'-scheme X, we have a natural isomorphism $\operatorname{Hom}_{S'}(X, G') \xrightarrow{\sim} \operatorname{Hom}_S(X, G)$ induced by composition with the morphism $G' \to G$, using the universal property of the fibre product. Since any S'-morphism $X \to Y$ is also an S-morphism, the functoriality of the group structure is inherited as well. □

Explicitly, the multiplication $m' \colon G' \times_{S'} G' \to G'$ is induced by $m \circ (\varphi \times \varphi)$ and the structure morphism, where $\varphi : G' \to G$ is the canonical map. In particular, a subgroup scheme of an abelian variety is commutative.

Affine group schemes (that is, group schemes of the form $\operatorname{Spec}(H)$) are always represented by commutative Hopf algebras. A Hopf algebra over k is a ring H (in general not assumed to be commutative) with unit $\eta \colon k \to H$, multiplication $m \colon H \otimes H \to H$, co-unit $\epsilon \colon H \to k$, comultiplication $\Delta \colon H \to H \otimes H$, and antipode $I \colon H \to H$ such that $(H, m, \Delta, \eta, \epsilon)$ is a bialgebra and such that the following diagram commutes:

$$\begin{tikzcd}
& H \otimes H \arrow[r, "I \otimes \mathrm{id}"] & H \otimes H \arrow[dr, "m"] & \\
H \arrow[ur, "\Delta"] \arrow[rr, "\epsilon"] \arrow[dr, "\Delta"'] & & k \arrow[r, "\eta"] & H \\
& H \otimes H \arrow[r, "\mathrm{id} \otimes I"] & H \otimes H \arrow[ur, "m"'] &
\end{tikzcd}$$

If H is also cocommutative, $\operatorname{Spec}(H)$ is a commutative group scheme.
Finite group schemes over affine bases are examples of affine group schemes. In this case we have the following definition:

Definition 1.3.3. Let G be an affine k-group scheme whose structure morphism is finite. The *rank* of G is the dimension of its global sections:

$$\operatorname{rk} G := \dim_k H^0(G, \mathcal{O}_G).$$

Let now $G = \operatorname{Spec}(H)$ for a commutative Hopf algebra H which is finite-dimensional over k. Then we define the *Cartier dual* of G to be $G^D := \operatorname{Spec}(H^\vee)$, where $H^\vee = \operatorname{Hom}_k(H, k)$ naturally inherits a Hopf algebra structure from H; the multiplication and comultiplication get swapped after dualising, and so do the unit and co-unit. Dualising defines an endofunctor $(-)^D$ on the category of finite-dimensional affine commutative k-group schemes, and we have a natural isomorphism $(G^D)^D \cong G$.

The Hopf algebra $H^\vee$ represents the group functor $\mathcal{H}om(G, \mathbb{G}_m)$, which is defined through

$$T \longmapsto \operatorname{Hom}_T(G_T, \mathbb{G}_{m,T}).$$

Cartier duality exists for general commutative group schemes which are finite locally free over their base, but we won't need this amount of generality.

In some ways, finite group schemes behave just like finite groups [Sti09, Thm. 6]:

Proposition 1.3.4 (Deligne)**.** Let G be a commutative k-group scheme of rank n. Then

$$G = \ker(G \xrightarrow{n} G).$$

In other ways, though, finite group schemes are more complicated than finite groups. For instance, it is an open question whether the above result holds for finite non-commutative group schemes. Another way that group schemes are different is that there exist at least three non-isomorphic group schemes of order p^2, at least when $\operatorname{char}(k) = p$:

Examples 1.3.5.
1. There is the constant group scheme associated to $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. As a scheme, it is isomorphic to $\coprod_G \operatorname{Spec}(k)$, and the group structure is induced by permuting the components according to the group law on G.
2. The multiplicative group $\mathbb{G}_m$ is the affine group scheme $\operatorname{Spec}(k[T^{\pm 1}])$ whose Hopf algebra is isomorphic to the group algebra $k[\mathbb{Z}]$. For any integer n, it has an endomorphism given by $T \mapsto T^n$ on global sections. This has kernel is $\mu_n \cong \operatorname{Spec}(k[T]/(T^n - 1))$. If $n = p^2$, this has order p.
3. Suppose $\operatorname{char}(k) = p > 0$. Then the map $f \mapsto f^{p^n} : k[T] \to k[T]$ is a morphism of algebras for every n, and induces an endomorphism of the additive group $\mathbb{G}_a = \operatorname{Spec}(k[T])$. For $n = 2$, its kernel is $\alpha_{p^2} \cong \operatorname{Spec}(k[T]/(T^{p^2}))$ and has order p^2. It is clearly non-reduced.

We can always decompose a finite group scheme as follows [EvdGM, Prop. 4.45]:

Proposition 1.3.6. Let G be a finite k-group scheme. Then there is an exact sequence

$$0 \to G^0 \to G \to G_{\text{ét}} \to 0,$$

where G^0 is the connected component of G containing the identity element, and $G_{\text{ét}}$ is the étale group scheme $\pi_0(G)$ of connected components of G.

We will now move on to studying isogenies.

Definition 1.3.7. A homomorphism $f : X \to Y$ is said to be an *isogeny* if $\dim X = \dim Y$ and $\ker f$ is finite. The *degree* of an isogeny is the degree $[k(X) : k(Y)]$ of the field extension induced by f.

We can give equivalent definitions using the following lemma:

Lemma 1.3.8. Let $f : X \to Y$ be a flat morphism of k-varieties. Let X' be the fibre of f over a closed point $y \in Y$. Then X' is equidimensional and $\dim X = \dim Y + \dim X'$.

Proof. See [Har77, III.9.5]. □

Proposition 1.3.9. Let $f \colon X \to Y$ be a homomorphism of abelian varieties. The following are equivalent:

(i) f is an isogeny.

(ii) $\dim X = \dim Y$ and f is surjective.

(iii) f is finite, flat, and surjective.

Proof. (i) $\implies$ (ii): Since f is proper and all fibres are translates of $\ker f$, which is finite, it follows that f is finite. Moreover, $f(X)$ is closed in Y, and $\dim f(X) = \dim X = \dim Y$, so f is surjective because Y is irreducible.
(ii) $\implies$ (iii): By generic flatness, f is flat over a non-empty open subset $U \subseteq Y$. Applying Lemma 1.3.8 to the restriction of f to this locus and using that all fibres are all isomorphic to $\ker f$ via translation, we see that $\ker f$ is a finite group scheme. As above, f is finite, so in particular quasi-finite. In general, a quasi-finite morphism between regular, irreducible noetherian schemes of the same dimension is flat, which shows (iii).
(iii) $\implies$ (i): Since f is finite, the fibre $\ker f$ is finite. By Lemma 1.3.8, $\dim X = \dim Y$. □

An isogeny f induces an isomorphism $X/\ker f \xrightarrow{\sim} Y$; for a rigorous treatment of quotients by finite group schemes, see [EvdGM, Chapter IV]. If one is willing to accept that the category of commutative group schemes of finite type over a field is abelian, one can simply take the quotient in this category.

Since the identity morphism is an isogeny and compositions of isogenies are isogenies, we see that the relation "$A \sim B \iff$ there exists an isogeny $A \to B$" is reflexive and transitive. The following proposition shows that it is an equivalence relation:

Proposition 1.3.10. Let $f \colon X \to Y$ be an isogeny. Then there exists an isogeny $g \colon Y \to X$.

Proof. Write $Y \cong X/\ker f$, and let $n := \operatorname{rk} \ker f$. Then $n(\ker f) = 0$ (Proposition 1.3.4), so $[n]_X$ factors through a morphism $g : Y \to X$:

$$\begin{tikzcd}
X \arrow[r, "{[n]_X}"] \arrow[d, two heads, "f"'] & X \\
X/\ker f \arrow[r, "\sim"] \arrow[ur, dotted] & Y \arrow[u, dotted, "g"']
\end{tikzcd}$$

We will see in Theorem 1.5.5 that $[n]_X$ is surjective, so g is surjective. Since $\dim X = \dim Y$, it is an isogeny by Proposition 1.3.9, so we are done. □

Hence isogenies induce an equivalence relation on the category of abelian varieties. Whenever we talk about isogeny classes, we mean equivalence classes with respect to this relation.

Lemma 1.3.11. Let $f : X \to Y$ be an isogeny. Then $\deg(f) = \operatorname{rk} \ker f$.

Proof. If f is an isogeny, $\ker f$ is a finite group scheme, so in particular affine; hence it makes sense to talk about its rank. Consider the sheaf $f_*\mathcal{O}_X$; it is coherent since f is finite, and locally free since the fibres are all translates of $\ker f$. The rank can be computed as the dimension of the fibre at any point. In particular, taking the generic point gives $\dim_{K(Y)} K(X) = \deg f$, and taking the point $0 \in Y$ gives $\dim_k H^0(\ker(f), \mathcal{O}_{\ker f}) = \operatorname{rk}\ker f$. □

We distinguish two special kinds of isogenies:

Definition 1.3.12. An isogeny $X \to Y$ is said to be *separable*, resp. *purely inseparable* if the extension $k(Y) \hookrightarrow k(X)$ is separable, resp. purely inseparable.

Proposition 1.3.13. *Let $f\colon X \to Y$ be an isogeny.*

1) *f is separable if and only if $\ker f$ is étale over k.*

2) *f is purely inseparable if and only if $\ker f$ is connected.*

Proof. See [EvdGM, Prop. 5.6]. □

Proposition 1.3.14. *Any isogeny $f\colon X \to Y$ can be written as a composition $g \circ h$ with g separable and h purely inseparable.*

Proof. By Proposition 1.3.6, any finite k-group scheme is an extension of an étale group scheme by a connected group scheme (the connected component containing 0). Applying this to $K := \ker f$, we can factor f as

$$X \longrightarrow X/K^0 \longrightarrow X/K \xrightarrow{\sim} Y,$$

which has the desired properties. □

1.4 Endomorphism algebras

Now that we have introduced isogenies, the study of the endomorphism ring of an abelian variety becomes rather interesting. The results in this section are of major importance in the study of abelian varieties.

Definition 1.4.1. An abelian variety A is *simple* if its only abelian subvarieties are 0 and itself.

Theorem 1.4.2 (Poincaré Splitting Theorem)**.** *Let A be an abelian variety. Then A is isogenous to a product $A_1^{n_1} \times \ldots \times A_m^{n_m}$, where each of the A_i are pairwise non-isogenous simple abelian varieties.*

Proof. We give the rough idea of the proof; for details, see [EvdGM, Thm. 12.2].
Given an abelian subvariety $A_1 \hookrightarrow A$, we want to construct another abelian subvariety A_2 such that the induced map $A_1 \times A_2 \to A$ is an isogeny. We do this by considering a composition $A \to A^t \to A_1^t$ of a polarisation with the transpose of the inclusion and taking its kernel K. Then K^0_{red} is an abelian subvariety of A, which is the right choice for A_2. □

Thus, if we consider abelian varieties up to isogeny, every object decomposes as a product of simples. If one is only interested in isogeny classes, this reduces most problems to the case of simple abelian varieties.

The second interesting thing about endomorphism rings is what happens to them after we tensor with $\mathbb{Q}$. This process kills torsion, so we have to be careful, but luckily $\operatorname{Hom}_k(X, Y)$ is torsion-free. Indeed, Suppose $nf = 0$. Then $\operatorname{im}(f) \subseteq Y[n]$, a finite group scheme, and since the image is an integral subscheme of Y we get $\mathrm{im}(f) = 0$, i.e. $f = 0$.

So we may consider now the category AV_k^0 of abelian varieties over k with morphisms given by $\mathrm{Hom}^0(X,Y) := \mathbb{Q} \otimes \mathrm{Hom}_k(X,Y)$, without fear of killing anything off. When we do this, something interesting happens:

Proposition 1.4.3. Let $f\colon X \to Y$ be an isogeny. Then f is invertible in AV_k^0.

Proof. This is similar to Proposition 1.3.10. Say f has degree n. Then $n(\ker f) = 0$, so $[n]_X$ factors through a map $g\colon Y \to X$:

$$\begin{tikzcd}
X \arrow[r, "{[n]_X}"] \arrow[d, two heads, "f"'] & X \\
X/\ker f \arrow[r, "\sim"] \arrow[ur, dotted] & Y \arrow[u, dotted, "g"']
\end{tikzcd}$$

Then $\frac{1}{n} \otimes g \in \mathrm{Hom}^0(Y,X)$ is the inverse of f. Indeed, $gf = [n]_X$ by the above diagram, and since $f[n]_X = [n]_Y f$, we see $fgf = [n]_Y f$. Since f is surjective, also $fg = [n]_Y$. □

The first consequence of these facts is the following:

Proposition 1.4.4. For any abelian variety A, $\mathrm{End}^0(A) = \mathbb{Q} \otimes \mathrm{End}_k(A)$ is a semisimple algebra.

Proof. By Proposition 1.4.3, we may replace A by any variety in its isogeny class. Using the Poincaré splitting theorem, we can write $A \sim A_1^{m_1} \times \ldots \times A_n^{m_n}$ for pairwise non-isogenous A_i. By simplicity, we have

$$\mathrm{Hom}_k(A_i^{m_i}, A_j^{m_j}) = \begin{cases} \mathrm{Mat}_{m_i}(\mathrm{End}_k(A_i)) & i = j; \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $\mathrm{End}_k(\prod_i A_i^{m_i})$ is a product of matrix algebras over rings of the form $\mathrm{End}_k(A_i)$ with A_i simple, and $\mathbb{Q} \otimes \mathrm{End}_k(A) \cong \prod \mathrm{Mat}_{m_i}(\mathbb{Q} \otimes \mathrm{End}_k(A_i))$. Again by general theory, a matrix algebra over a division ring is semisimple, so it suffices to show that the $\mathbb{Q} \otimes \mathrm{End}_k(A_i)$ are division algebras. But this is again the statement that isogenies become invertible after tensoring with $\mathbb{Q}$, so we are done. □

After proving Tate's theorem, we will see that we one can say much more about the structure of endomorphism algebras of abelian varieties when the base field is finite.

1.5 The Tate module

Now let n be a natural number and A an abelian variety. The multiplication-by-n-map is defined as

$$[n]_A : A \xrightarrow{\Delta_{A/k}^{(n-1)}} A \times A \times \ldots \times A \xrightarrow{m^{(n-1)}} A.$$

We will also write the map $[n]_A$ as simply n or (n), e.g. for a sheaf of $\mathcal{O}_A$-modules $\mathcal{F}$, $(-1)^*\mathcal{F} := [-1]_A^*\mathcal{F}$.

Definition 1.5.1. Let A be an abelian variety. The *n-torsion* of A is the subgroup scheme $A[n] := \ker[n]_A$.

The torsion points of an abelian variety form an interesting object of study. We begin with a useful proposition.

Proposition 1.5.2. Let $\mathcal{L}$ be a line bundle on an abelian variety A, and let $n \in \mathbb{Z}$. Then

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

Proof. We use induction. Clearly the formula is correct for $n = 0, 1$, and -1. Applying the Theorem of the Cube (1.1.10) with $f = n-1$, $g = 1 = \mathrm{id}_A$, and $h = -1$, gives the formulas

$$(n+1)^*\mathcal{L} \cong n^*\mathcal{L}^2 \otimes (n-1)^*\mathcal{L}^{-1} \otimes \mathcal{L} \otimes (-1)^*\mathcal{L}, \tag{1.1}$$

$$(n-1)^*\mathcal{L} \cong n^*\mathcal{L}^2 \otimes (n+1)^*\mathcal{L}^{-1} \otimes \mathcal{L} \otimes (-1)^*\mathcal{L}, \tag{1.2}$$

If we know the formula is true for n and $n-1$, then (1.1) simplifies to $\mathcal{L}^{(n+2)(n+1)/2} \otimes (-1)^*\mathcal{L}^{n(n+1)/2}$. Similarly, if we know the statement is true for n and $n+1$, (1.2) simplifies to the desired expression. Thus we get the result for all n. □

Definition 1.5.3. A line bundle on an abelian variety is said to be *symmetric* if $\mathcal{L} \cong (-1)^*\mathcal{L}$, and *antisymmetric* if $\mathcal{L}^{-1} \cong (-1)^*\mathcal{L}$.

To justify the terminology, consider an elliptic curve over $\mathbb{R}$ with equation $y^2 = x^3+ax+b$. Then a line bundle is symmetric precisely when the corresponding divisor satisfies $\mathrm{ord}_P(D) = \mathrm{ord}_{-P}(D)$ for every prime divisor $[P]$; and $-P$ is the point P reflected through the x-axis.

Corollary 1.5.4. Let $\mathcal{L}$ be a symmetric line bundle on A. Then $n^*\mathcal{L} \cong \mathcal{L}^{n^2}$.

Any abelian variety carries a symmetric line bundle: for instance $\mathcal{L} \otimes (-1)^*\mathcal{L}$ is always symmetric.

With these tools under our belt, we can show that the n-torsion is a finite subgroup scheme.

Theorem 1.5.5. Let A be an abelian variety of dimension g over a field of characteristic p. For $n \neq 0$, the endomorphism $[n]_A$ is an isogeny of degree n^{2g}; moreover, if $p \nmid n$, it is separable.

Proof. Since A is projective (Theorem 1.2.6), it admits an ample and symmetric divisor D. Thus $n^*\mathcal{O}(D) \cong \mathcal{O}(n^2D)$ is ample if $n \neq 0$, and so restricts to an ample line bundle on $\ker[n]_A$. But this restriction is trivial, as we can see by considering the pullback square

$$\begin{tikzcd}
\ker[n]_A \arrow[r] \arrow[d, hook] & \mathrm{Spec}(k) \arrow[d, hook, "0"] \\
A \arrow[r, "{[n]_A}"] & A
\end{tikzcd}$$

Hence the kernel is finite, so $[n]_A$ is an isogeny.
To calculate the degree, we consider the g-fold self-intersection of D:

$$(D)^g = (D_1 \cdot \ldots \cdot D_g) = \sum_{p \in |D_1| \cap \cdots \cap |D_g|} (D_1 \cdot \ldots \cdot D_g)_p,$$

where $D_i \sim D$ (linear equivalence) and $D_1, \ldots, D_g$ intersect properly. This is well-defined [Mil15b, 12.7, 12.8], and since A is smooth, we have

$$\deg[n]_A \cdot (D)^g = (n^* D)^g = (n^2 D)^g = n^{2g}(D)^g,$$

where the first equality is [Mil15b, Thm. 12.10], and the second equality was explained above. Since D is ample, $(D)^g > 0$ and hence the degree of $[n]_A$ equals n^{2g}.

Finally, if $p \nmid n$ then $p \nmid n^{2g} = [K(A) : K(nA)]$, so the field extension $K(nA) \hookrightarrow K(A)$ is separable. □

Theorem 1.5.5 leads to the definition of Tate modules.

Definition 1.5.6. Let A be an abelian variety over a field k of characteristic $p \geq 0$, and $l \neq p$ a prime number. The *Tate-l-module* of A is defined as

$$T_l(A) := \varprojlim A[l^n](k_s),$$

where k_s is a separable closure of k. In positive characteristic, we define

$$T_p(A) := \varprojlim A[p^n](\bar{k}).$$

Note that for any n, we have a (right) $\mathrm{Gal}(k_s/k)$-action on $A[l^n](k_s)$, and the multiplication-by-l-maps are equivariant with respect to this action. Hence $T_l(A)$ inherits a $\mathrm{Gal}(k_s/k)$-action, and moreover this action is continuous.

We will usually consider T_l as a functor $\mathsf{AV}_k \to \mathsf{Rep}_{\mathbb{Z}_l}(\mathrm{Gal}(k))$: a homomorphism of abelian varieties respects the l^n-torsion, so induces a $\mathbb{Z}_l$-linear map which is equivariant with respect to the Galois action.

Theorem 1.5.7. For $(p, n) = 1$, we have $A[n](k_s) = A[n](\bar{k}) = (\mathbb{Z}/n\mathbb{Z})^{2g}$, where $g = \dim A$.

Proof. If $(p, n) = 1$, the isogeny $[n]_A$ is separable. Therefore, Proposition 1.3.13 tells us that $\ker[n]_A$ is an étale group scheme of rank $\deg[n]_A = n^{2g}$. Hence $A[n](k_s) = A[n](\bar{k})$ is an abelian group of order n^{2g}. For any $d \mid n$, we have that the d-torsion of this group is $A[d](k_s)$ which has order d^{2g} by the same argument, so we must have $A[n](k_s) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. □

Corollary 1.5.8. If $l \neq p$, we have $T_l(A) \cong \mathbb{Z}_l^{2g}$ (non-canonically).

It will often be useful to consider the l-adic representation obtained from the Tate module:

Definition 1.5.9. Denote by $V_l(A) := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(A)$. If $l \neq p$, this is a $2g$-dimensional l-adic representation of $\mathrm{Gal}(k_s/k)$.

The story of the rank of $T_p(A)$ is more complicated. The result will be that $T_p(A) \cong \mathbb{Z}_p^n$ for some $0 \leq n \leq g$ called the *p-rank* of A. We will not study this phenomenon, although it gives examples of abelian varieties with interesting properties. For example, an elliptic curve with p-rank zero is called supersingular, and over a finite field, this is the only example of a simple abelian variety whose endomorphism algebra has a one-dimensional centre.

One can view the Tate module as an l-adic analogue of the singular homology group $H_1(A(\mathbb{C}), \mathbb{Z})$ in the analytic setting. We will explore this analogy further when talking about the Tate conjecture.

1.6 The dual abelian variety

Let C be a genus g Riemann surface. Then for any choice of a point $Q \in C$, there is the famous Abel-Jacobi map,

$$AJ_Q \colon C \longrightarrow \mathrm{Jac}(C), \qquad P \longmapsto \mathcal{O}_X(Q - P).$$

In genus 1, the Abel-Jacobi theorem implies that this map is an isomorphism.

This demonstrates a much more general phenomenon. A genus 1 Riemann surface is nothing but a complex elliptic curve (up to the choice of a base point), and Abel-Jacobi says that such a curve is always isomorphic to its Jacobian variety. For general abelian varieties, we will have a similar statement: any abelian variety is isogenous to its dual. In the language that we will develop, the Abel-Jacobi theorem says that any complex elliptic curve is principally polarised.

As in the case of Riemann surfaces, it will turn out that there is a space parameterizing line bundles on an abelian variety A, and the connected component containing $\mathcal{O}_A$ is itself an abelian variety of the same dimension. The space we want to consider is the representing object of the relative Picard functor.

Definition 1.6.1. Let X be an S-scheme. Define the contravariant functor $\mathrm{Pic}_{X/S} : \mathsf{Sch}_S \to \mathsf{Set}$ on objects via

$$\mathrm{Pic}_{X/S}(T) := \frac{\mathrm{Pic}(X \times_S T)}{\mathrm{pr}_T^* \mathrm{Pic}(T)}$$

and on morphisms via the pullback of line bundles.

Theorem 1.6.2. *Suppose X is a proper k-variety. Then the relative Picard functor $\mathrm{Pic}_{X/k}$ is representable by a separated, locally of finite type k-scheme, denoted by $\mathbf{Pic}_{X/k}$. Its universal family is called the Poincaré bundle, and denoted by $\mathcal{P}_X$.*

For a discussion, see e.g. [EvdGM, Chapter VI, §1]. Since the Picard functor factors through the category of abelian groups, so does the functor of points of its representing object, so tautologically, $\mathbf{Pic}_{X/k}$ is a commutative group scheme. Under our assumptions, it is in general true that the connected components of such a representing object are projective, but it does not a priori need to be reduced. However, we have the following result (ibid. Theorem 6.6):

Theorem 1.6.3. *The dimension of the tangent space of $\mathbf{Pic}_{X/k}$ at the identity element equals $\dim_k H^1(X, \mathcal{O}_X)$. In particular, the connected component $X^t := \mathbf{Pic}^0_{X/k}$ of $\mathbf{Pic}_{X/k}$ containing the identity element is smooth if and only if its dimension equals $\dim_k H^1(X, \mathcal{O}_X)$.*

In particular, if we can show that $\dim X^t = \dim_k H^1(X, \mathcal{O}_X)$, this group scheme is reduced. Combining it with the other properties, this means it is an abelian variety, and this is what we will call the dual abelian variety. The results we want to obtain are summarised in the following theorem:

Theorem 1.6.4. *For an abelian variety X of dimension g, we have that X^t is reduced, hence an abelian variety. Moreover, for any ample line bundle $\mathcal{L}$, the homomorphism $\varphi_{\mathcal{L}} \colon X \to X^t$ given by $x \mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ is an isogeny, and $\dim X = \dim X^t = \dim_k H^1(X, \mathcal{O}_X)$.*

The morphism $\varphi_{\mathcal{L}}$ appearing in the theorem is part of a very important class of homomorphisms, which we will now define.

Lemma 1.6.5. *Let $\mathcal{L}$ be a line bundle on an abelian variety X. Then there exists a morphism $\varphi_{\mathcal{L}} \colon X \to X^t$ which on points sends $x \mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$.*

Proof. To define the map, note that for any $x \in X(T)$, one can construct a right translation $t_x \colon X_T \to X_T$ extending Definition 1.1.5. Thus $\varphi_{\mathcal{L}}$ defines a map of schemes $X \to \mathbf{Pic}_{X/k}$. It is a homomorphism by the Theorem of the Square, and its image is contained in $\mathbf{Pic}^0_{X/k}$ since $\varphi_{\mathcal{L}}(0) = \mathcal{O}_X$ and X is connected. □

One can alternatively describe the Picard functor by considering only line bundles with a certain rigidification. Doing so leads to the following description of the universal property of the Poincaré bundle: for every k-scheme T and for every line bundle $\mathcal{L}$ on $X \times T$ such that $\mathcal{L}|_{\{0\}\times T}$ is trivial, there is a unique morphism $f : T \to \mathbf{Pic}_{X/k}$ such that $\mathcal{L} = (\mathrm{id} \times f)^*\mathcal{P}_X$. We call such a line bundle $\mathcal{L}$ a *family of line bundles on X parameterized by T.*

The morphism $\varphi_{\mathcal{L}}$ from Lemma 1.6.5 thus gives rise to a family of line bundles on A parameterized by A. We can describe it explicitly as follows:

Lemma 1.6.6. Let $\mathcal{L}$ be a line bundle on X, and let $\varphi_{\mathcal{L}}$ be the corresponding morphism $X \to X^t$. Then the pullback of the Poincaré bundle under $\varphi_{\mathcal{L}}$ is the *Mumford bundle* $\Lambda(\mathcal{L})$ on $X \times X$, described by

$$\Lambda(\mathcal{L}) := m^*\mathcal{L} \otimes \mathrm{pr}_1^*\mathcal{L}^{-1} \otimes \mathrm{pr}_2^*\mathcal{L}^{-1}.$$

Note that $\Lambda(\mathcal{L})|_{\{x\}\times X} \cong t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$.

Proof. We can view $\Lambda(L)$ as a line bundle on X parameterized by X. Hence it is the pullback of the Poincaré bundle under a morphism $f : X \to X^t$. Now let $x \in X(k)$ and consider

$$X \times \{x\} \hookrightarrow X \times X \xrightarrow{\mathrm{id}\times f} X \times X^t.$$

Considering the pullback of $\mathcal{P}_X$ under this morphism gives

$$(\mathrm{id} \times f(x))^*\mathcal{P}_X = \Lambda(L)|_{X\times\{x\}} = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}.$$

But this means precisely that $f(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. Indeed, this is how one obtains the natural isomorphism $\mathrm{Hom}(-, \mathbf{Pic}_{X/k}) \xrightarrow{\sim} \mathrm{Pic}_{X/k}(-)$: it sends $f \colon T \to \mathbf{Pic}_{X/k}$ to a family of bundles $\mathcal{L}$ on $X \times T$ such that $\mathcal{L}|_{X\times\{t\}} \cong f(t)$. Hence $f = \varphi_{\mathcal{L}}$, which is what we wanted. □

Definition 1.6.7. For a line bundle $\mathcal{L}$ on an abelian variety X, we define $K(\mathcal{L}) \subseteq X$ to be the maximal closed subscheme of X such that $\Lambda(\mathcal{L})$ restricted to $X \times K(\mathcal{L})$ is isomorphic to the pullback $\mathrm{pr}_2^*\mathcal{M}$ of some line bundle on $K(\mathcal{L})$.

Lemma 1.6.8. The scheme $K(\mathcal{L})$ is well-defined and equal to the fibre of $\varphi_{\mathcal{L}} \colon X \to X^t$ over the trivial bundle. Moreover, $\Lambda(\mathcal{L})|_{X\times K(\mathcal{L})} \cong \mathcal{O}_{X\times K(\mathcal{L})}$.

Proof. Lemma 1.6.6 implies that $\Lambda(\mathcal{L})|_{X\times\{x\}}$ is trivial if and only if $\varphi_{\mathcal{L}}(x) = 0 := \mathcal{O}_X$. Hence $K(\mathcal{L})$ is contained in the kernel of $\varphi_{\mathcal{L}}$, and in fact equality holds: by definition of the Picard functor, the induced morphism $S := \ker(\varphi_{\mathcal{L}}) \to \mathbf{Pic}_{X/k}$ gives a bundle $(\mathrm{id} \times 0)^*\mathcal{P}_X$ on $X \times S$. This is the restriction of the Mumford bundle to $X \times S$. It restricts to the trivial bundle on horizontal fibres $X \times \{x\}$ since $x \in \ker(\varphi_{\mathcal{L}})$, and to the trivial bundle on the vertical fibre $\{0\} \times K(\mathcal{L})$. By the See-Saw Principle (1.1.9), this implies $\Lambda(\mathcal{L})|_{X\times K(\mathcal{L})} \cong \mathcal{O}_{X\times K(\mathcal{L})}$. □

Note that $\varphi_{\mathcal{L}}(x) = 0$ if and only if $\mathcal{L}$ is invariant under translation by x. The following theorem can be interpreted as follows: ample line bundles on abelian varieties are invariant under few translations.

Theorem 1.6.9. If $\mathcal{L}$ is ample, $K(\mathcal{L})$ is a finite group scheme.

Proof. We may assume $k = \bar{k}$. We first show that $K(\mathcal{L})$ is a group scheme. Suppose $t_x^*\mathcal{L} \cong \mathcal{L} \cong t_y^*\mathcal{L}$. Then by the Theorem of the Square (1.1.11), $t_{x+y}^*\mathcal{L} \cong \mathcal{L} \otimes \mathcal{L} \otimes \mathcal{L}^{-1} \cong \mathcal{L}$.
Next, consider the abelian subvariety $Y := K(\mathcal{L})^0_{\text{red}}$ (Proposition 1.1.3). The restriction $\mathcal{L}_Y$ of $\mathcal{L}$ to Y gives an ample line bundle on Y. By Lemma 1.6.8, $\Lambda(\mathcal{L}_Y)$ is trivial on $Y \times Y$, and hence

$$(1, -1)^*\Lambda(\mathcal{L}_Y) = \mathcal{L}_Y \otimes (-1)^*\mathcal{L}_Y \cong \mathcal{O}_Y.$$

On the other hand, since $\mathcal{L}_Y$ is ample, so is the above bundle. Hence $Y = \operatorname{Spec}(k)$ and $K(\mathcal{L})$ is finite. □

Definition 1.6.10. A line bundle $\mathcal{L}$ on X is *non-degenerate* if $K(\mathcal{L})$ is finite.

Note that $K(\mathcal{L})$ is the kernel of $\varphi_{\mathcal{L}}$, so $\mathcal{L}$ is non-degenerate if and only if $\varphi_{\mathcal{L}}$ is an isogeny. Moreover, Lemma 1.3.11 says that the rank of $K(\mathcal{L})$ equals $\deg \varphi(\mathcal{L})$.

Remark 1.6.11. The theorem says that ample line bundles are non-degenerate. One can prove that abelian varieties are projective based on a converse to this statement. The converse does not hold on the nose, but we have the following statement: any *effective* non-degenerate line bundle is ample. Thus projectivity follows once one constructs such an effective line bundle, which is possible via a clever construction reminiscent of, but simpler than, the proof of projectivity from the previous section. See [EvdGM, Thm. 2.25] for the details.

We will need one more structural result to prove Theorem 1.6.4.

Theorem 1.6.12 (Borel-Hopf Structure Theorem)**.** Let $H^\bullet$ be a graded-commutative bialgebra over a perfect field k such that $H^n = 0$ for all $n < 0$ and $H^0 \cong k$. Then we have an isomorphism of bialgebras

$$H^\bullet \cong H_1^\bullet \otimes_k \ldots \otimes_k H_n^\bullet$$

where each $H_i^\bullet$ is a graded bialgebra generated by a single element of degree $d_i > 0$.

Note that the tensor product of graded algebras has a graded commutative multiplication by definition. A reference for the case where $H^\bullet$ is commutative is [MM65, Thm. 7.11], and the same argument extends to the graded-commutative case.

Proof of 1.6.4. It remains to show that $\dim X = \dim X^t = \dim_k H^1(X, \mathcal{O}_X)$.
Let $\mathcal{L}$ be an ample line bundle on X, which exists by Theorem 1.2.6. By Theorem 1.6.9, $\varphi_{\mathcal{L}} : X \to X^t$ has finite fibres, so $\dim X \leq \dim X^t$.
Next, note that the cohomology ring $H^\bullet(X, \mathcal{O}_X)$ of X obtains a comultiplication via

$$H^\bullet := H^\bullet(X, \mathcal{O}_X) \xrightarrow{m^*} H^\bullet(X \times X, \mathcal{O}_{X\times X}) \xrightarrow{\sim} H^\bullet \otimes H^\bullet.$$

Similarly, the identity $e : \operatorname{Spec}(k) \to X$ induces a co-unit. Thus, possibly after making a base change to the perfect field $\bar{k}$, $H^\bullet$ is a graded bialgebra satisfying the criteria of the Borel-Hopf Structure Theorem, and we may write

$$H^\bullet = H_1^\bullet \otimes \ldots \otimes H_n^\bullet$$

where each $H_i^\bullet$ is generated by one element x_i of degree d_i. Now we have $\dim H^1 \leq n \leq \sum d_i \leq g$, where the last inequality follows because $x_1 \otimes \ldots \otimes x_n$ is a non-zero element of $H^\bullet$, hence must have degree at most g. But by Theorem 1.6.3, $\dim X^t \leq \dim H^1(X, \mathcal{O}_X) \leq g = \dim X$, so we have equality everywhere. In particular, X^t is smooth, hence reduced and an abelian variety. □

We also obtain the following nice corollary about the cohomology of abelian varieties:

Corollary 1.6.13. If X is an abelian variety, then $H^\bullet(X, \mathcal{O}_X) \cong \bigwedge^\bullet H^1(X, \mathcal{O}_X)$.

Proof. We have seen that $H^\bullet := H^\bullet(X, \mathcal{O}_X)$ is a graded bialgebra with $\dim H^1 = g$. Write again $H^\bullet \cong H_1^\bullet \otimes \ldots H_n^\bullet$, generated by elements x_i of degree d_i. Since $H^n = 0$ for $n > g$, the equality $\dim H^1 = g$ implies that $n = g$ and $d_i = 1$ for all i. Moreover, we must have $x_i^2 = 0$ for all i, since otherwise the element $x_1 \otimes \ldots \otimes x_i^2 \otimes \ldots \otimes x_g$ would have degree $g + 1$. Thus the map $\bigwedge^\bullet H^1 \to H^\bullet$ is an isomorphism. □

We can now officially define the dual abelian variety.

Definition 1.6.14. Let X be an abelian variety of dimension g. The *dual* of X is $X^t := \mathbf{Pic}^0_{X/k}$. From now on, we will denote by $\mathcal{P}_X$ the Poincaré bundle on $X \times X^t$, i.e. the restriction of the universal family of the relative Picard functor to $X \times X^t$.

Since X^t represents the degree 0 part of the Picard functor, we can also describe $\mathcal{P}_X$ directly: it is the image of id_{X^t} under the natural isomorphism $\mathrm{Hom}_k(X^t, X^t) \xrightarrow{\sim} \mathrm{Pic}^0_{X/k}(X^t)$. We call this bundle the *Poincaré bundle*. The universal property can be described as follows.

Definition 1.6.15. Let X be an abelian variety and T a k-scheme. A *family of degree 0 line bundles on X parameterized by T* is a line bundle $\mathcal{L}$ on $X \times T$ such that

1) For any $t \in T(k)$, we have $\mathcal{L}|_{X \times \{t\}} \in \mathrm{Pic}^0(X)$;

2) $\mathcal{L}|_{\{0\} \times T} \cong \mathcal{O}_T$.

Then for every family of degree zero line bundles on X parameterized by T, there is a unique morphism $f\colon T \to X^t$ such that $\mathcal{L} = (\mathrm{id} \times f)^* \mathcal{P}_X$. Explicitly, $f(x) = \mathcal{L}|_{X \times \{x\}}$.

An application of this is the following. For a morphism $f\colon A \to B$ between abelian varieties, we can construct a transpose map $f^t\colon B^t \to A^t$, which is the unique map induced by the family of degree 0 line bundles $(f \times \mathrm{id}_{B^t})^* \mathcal{P}_B$ on A parameterized by B^t. Thus we have by definition

$$(f \times \mathrm{id})^* \mathcal{P}_B \cong (\mathrm{id} \times f^t)^* \mathcal{P}_A.$$

The term "dual" suggests that the functor $(-)^t$ is an auto-equivalence on the category of abelian varieties. This is indeed true [EvdGM, Chapter VII]:

Theorem 1.6.16. Let X be an abelian variety. Consider the Poincaré bundle $\mathcal{P}_X$ as a family of degree 0 line bundles on X^t parameterised by X. It induces an isomorphism

$$\kappa_X\colon X \xrightarrow{\sim} (X^t)^t,$$

which induces for any $f\colon X \to Y$ a commutative diagram

$$\begin{tikzcd}
(X^t)^t \arrow[r, "\kappa_X"] \arrow[d, "(f^t)^t"'] & X \arrow[d, "f"] \\
(Y^t)^t \arrow[r, "\kappa_Y"] & Y
\end{tikzcd}$$

Moreover, the duality preserves isogenies, cf. Theorem 1.9.1.

We will regard κ_X as the canonical way to identify X with $(X^t)^t$.

1.7 Riemann-Roch for abelian varieties

The main source for the following section is [Jav10], which is a good reference for more background material and proofs of the quoted results. Another option is [Ful98].

Let X be an n-dimensional smooth projective variety over a field k. Denote by $A^r(X)$ the free abelian group on irreducible closed codimension r subvarieties modulo rational equivalence; that is, we say $[W] \sim_{rat} 0$ if and only if there exist closed codimension $r-1$ subvarieties $V_1, \ldots, V_N$ of X and elements $f_i \in K(V_i)$ such that $[W] = \sum_i (f_i)$. The *Chow ring* of X is the group $A(X) = \bigoplus_{d=0}^n A^d(X)$. We will denote by $\mathrm{CH}(X)$ the ring $\mathbb{Q} \otimes A(X)$.

The Chow ring is a graded ring, where multiplication is given by the intersection product.

Given a proper morphism $f : X \to Y$, we have a well-defined ring morphism $f_* : A(X) \to A(Y)$ given as follows:

$$[V] \mapsto \begin{cases} [K(V) : K(f(V))][f(V)] & \dim V = \dim f(V); \\ 0 & \text{otherwise.} \end{cases}$$

Given a flat morphism $f : X \to Y$, we have a well-defined ring morphism $f^* : A(Y) \to A(X)$ given by $[V] \mapsto [f^{-1}(V)]$. The degree of f^* is the relative dimension of f.

Given a vector bundle $\mathcal{E}$ of rank r on X, the pullback $\pi^*\mathcal{E}$ of $\mathcal{E}$ under $\pi : \mathbb{P}(\mathcal{E}) \to X$ satisfies a nice property: it has a filtration with subquotients isomorphic to line bundles. Moreover, $\pi^* : A(X) \to A(\mathbb{P}(\mathcal{E}))$ is an injection, and this turns $A(\mathbb{P}(\mathcal{E}))$ into a free rank r $A(X)$-module, spanned by $\{1, \xi, \ldots, \xi^{r-1}\}$, where $\xi := \mathcal{O}_{\mathbb{P}(\mathbb{E})}(1)$. Thus, we can write

$$\xi^r - \pi^*(a_1)\xi^{r-1} + \ldots + (-1)^r \pi^*(a_r) = 0,$$

and we call $a_i \in A(X)$ the i^{th} *Chern class* of $\mathcal{E}$, which we denote by $c_i(\mathcal{E})$.
The *Chern polynomial* of $\mathcal{E}$ is defined to be

$$c_t(\mathcal{E}) = 1 + c_1(\mathcal{E})t + c_2(\mathcal{E})t^2 + \ldots + c_r(\mathcal{E})t^r.$$

It turns out that c_t commutes with pullbacks, and moreover is multiplicative on short exact sequences. Applying these facts to the morphism $\pi : \mathbb{P}(\mathcal{E}) \to X$, we get

$$\pi^* c_t(\mathcal{E}) = c_t(\pi^*\mathcal{E}) = c_t(\mathcal{L}_1) \cdot \ldots \cdot c_t(\mathcal{L}_r) = \prod_{i=1}^r (1 + c_1(\mathcal{L}_i)t) = \prod_{i=1}^r (1 + \alpha_i t).$$

The $\alpha_i \in A(\mathbb{P}(\mathcal{E}))$ are called the *Chern roots* of $\mathcal{E}$.

Definition 1.7.1. The *Chern character* of $\mathcal{E}$ is defined to be

$$\mathrm{ch}(\mathcal{E}) = \sum_{i=1}^r \exp(\alpha_i),$$

where $\alpha_1, \ldots, \alpha_r$ are the Chern roots, and $\exp(\alpha_i) = 1 + \alpha_i + \frac{1}{2}\alpha_i^2 + \ldots \in \mathrm{CH}(X)$.

We have an equality of formal power series

$$\frac{x}{1 - \exp(-x)} = 1 + \frac{1}{2}x + \sum_{i=1}^\infty \frac{B_{2i}}{(2i)!} x^{2i},$$

where B_i is the i^{th} Bernoulli number.

Definition 1.7.2. The *Todd class* of a vector bundle $\mathcal{E}$ is defined to be

$$\operatorname{td}(\mathcal{E}) = \prod_{j=1}^{r} \left(1 + \frac{1}{2}\alpha_j + \sum_{i=1}^{\infty} \frac{B_{2i}}{(2i)!}\alpha_j^{2i}\right),$$

where $\alpha_1, \dots, \alpha_r$ are the Chern roots of $\mathcal{E}$. The *Todd class of* X is defined to be $\operatorname{td}(X) := \operatorname{td}(\mathcal{T}_{X/k})$. Given a map $f : X \to Y$, the *relative Todd class of* f is defined to be $\operatorname{td}(X)/f^* \operatorname{td}(Y)$.

Define the degree map $\deg\colon A(X) \to \mathbb{Z}$ to be the composition $A(X) \to A(\operatorname{Spec}(k)) \cong \mathbb{Z}$ induced by the pushforward under the structure morphism. We will also denote it by $\int$.

Theorem 1.7.3 (Riemann-Roch for vector bundles)**.** Let X be a smooth projective curve. For any vector bundle $\mathcal{E}$, we have that

$$\chi(X, \mathcal{E}) = \deg(\operatorname{ch}(\mathcal{E}) \operatorname{td}(X)).$$

Proof. We need the following ingredients:

- Classical Riemann-Roch (for line bundles);
- Both the Euler characteristic and c_1 are additive on short exact sequences;
- Each vector bundle $\mathcal{E}$ of rank $r \geq 1$ can be written as an extension $0 \to \mathcal{L} \to \mathcal{E} \to \mathcal{E}' \to 0$, where $\mathcal{L}$ is a line bundle and $\mathcal{E}'$ is a rank $r-1$ vector bundle.

The proof then follows by induction on r. To see this, note that on a curve, we have $\operatorname{ch}(\mathcal{E}) = \sum_{i=1}^{r} \exp(\alpha_i) = \sum_{i=1}^{r}(1+\alpha_i) = r + c_1(\mathcal{E})$, and $\operatorname{td}(X) = \operatorname{td}(\omega_X^\vee) = 1 - K/2$, giving

$$\deg(\operatorname{ch}(\mathcal{E}) \operatorname{td}(X)) = \deg((r + c_1(\mathcal{E}))(1 - \frac{1}{2}K) = \deg(c_1(\mathcal{E})) + r(1-g).$$

□

The statement holds in general:

Theorem 1.7.4 (Hirzebruch-Riemann-Roch)**.** Let X be a smooth n-dimensional projective variety and let $\mathcal{E}$ be a vector bundle on X. Then

$$\chi(X, \mathcal{E}) = \deg(\operatorname{ch}(\mathcal{E}) \operatorname{td}(X)).$$

This follows from the vast generalisation

Theorem 1.7.5 (Grothendieck-Hirzebruch-Riemann-Roch)**.** Let $f : X \to Y$ be a proper morphism of smooth quasi-projective varieties over a field k. Then the diagram

$$\begin{tikzcd}
K_0(X) \arrow[r, "\operatorname{ch} \cdot \operatorname{td}(X)"] \arrow[d, "f_!"'] & \operatorname{CH}(X) \arrow[d, "f_*"] \\
K_0(Y) \arrow[r, "\operatorname{ch} \cdot \operatorname{td}(Y)"] & \operatorname{CH}(Y)
\end{tikzcd}$$

commutes.

Recall that we associated to any line bundle $\mathcal{L}$ on X a morphism $\varphi_{\mathcal{L}}\colon X \to X^t$ such that $\varphi_{\mathcal{L}}(x) = t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$.

Theorem 1.7.6 (Riemann-Roch for abelian varieties)**.** Let $\mathcal{L}$ be a line bundle on the g-dimensional abelian variety X. Then $\chi(\mathcal{L})^2 = \deg \varphi_{\mathcal{L}}$, and

$$\chi(\mathcal{L}) = \frac{c_1(\mathcal{L})^g}{g!}.$$

Proof. The second formula follows from Hirzebruch-Riemann-Roch, since $\mathrm{td}(X) = 1$ by Proposition 1.1.8. For the first statement we have to work a bit more. We will divide the proof into steps.

Step 1: Let $\mathcal{P}$ be the Poincaré bundle on $X \times X^t$, and denote by p_2 the projection $X \times X^t \to X^t$. Then

$$R^n p_{2,*}\mathcal{P} = \begin{cases} k_0 & n = g; \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, the sheaf cohomology of the Poincaré bundle is given by

$$H^n(X \times X^t, \mathcal{P}) = \begin{cases} k & n = g; \\ 0 & \text{otherwise.} \end{cases}$$

This can be proven using Grothendieck duality; here we take it for granted. A reference is [EvdGM, Thm. 9.1].

Step 2.1: Suppose $\mathcal{L}$ is non-degenerate, i.e. $\varphi_{\mathcal{L}}$ is an isogeny. We compute $\chi(\Lambda(\mathcal{L})) = (-1)^g \deg(\varphi_L)$ by applying flat base change and the Leray spectral sequence to exploit the cohomology result from Step 1. Indeed, $\Lambda(\mathcal{L}) = (\mathrm{id}_X \times \varphi_{\mathcal{L}})^*\mathcal{P}$. Flat base change says that if $f\colon X \to Y$ is qcqs and $g\colon Y' \to Y$ is flat, then

$$f^* R^i g_* \mathcal{F} \xrightarrow{\sim} R^i g'_*(f')^*\mathcal{F}.$$

In our case, the relevant pullback square is

$$\begin{tikzcd}
X \times X \arrow[r, "\mathrm{id} \times \varphi_{\mathcal{L}}"] \arrow[d, "p_2"'] & X \times X^t \arrow[d, "p_2"] \\
X \arrow[r, "\varphi_{\mathcal{L}}"] & X^t
\end{tikzcd}$$

and flat base change becomes

$$\varphi_{\mathcal{L}}^* R^i p_{2,*}\mathcal{P} \xrightarrow{\sim} R^i p_{2,*}\Lambda(\mathcal{L}).$$

Now the pre-image of zero under $\varphi_{\mathcal{L}}$ is precisely $K(\mathcal{L})$, so we obtain

$$R^n p_{2,*}\Lambda(\mathcal{L}) = \begin{cases} i_*\mathcal{O}_{K(\mathcal{L})} & n = g; \\ 0 & \text{otherwise.} \end{cases}$$

Now we can use the Leray spectral sequence for the morphism $p_2 : X \times X \to X$ and the line bundle $\Lambda(\mathcal{L})$. We obtain that $H^{p+q}(X \times X, \Lambda(\mathcal{L}))$ has a filtration with subquotients isomorphic to $E_\infty^{p+q-i,i} \cong H^{p+q-i}(X, R^i p_{2,*}\Lambda(\mathcal{L}))$ which we just saw is non-zero only for $i=0$ and $p+q=g$. Since moreover $\dim_k H^0(X, i_*\mathcal{O}_{K(\mathcal{L})}) = \deg \varphi_{\mathcal{L}}$, we obtain

$$\chi(\Lambda(\mathcal{L})) = (-1)^g \deg \varphi_{\mathcal{L}}.$$

Step 2.2: We calculate $\chi(\Lambda(\mathcal{L}))$ in another way, using the definition $\Lambda(\mathcal{L}) = m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1}$. Recall the projection formula: for $f : X \to Y$ a map of ringed spaces and $\mathcal{E}$ a locally free $\mathcal{O}_Y$-module of finite rank, we have

$$R^i f_*\mathcal{F} \otimes \mathcal{E} \xrightarrow{\sim} R^i f_*(\mathcal{F} \otimes f^*\mathcal{E}).$$

In our situation, we apply it with $f = p_2$ to obtain

$$R^i p_{2,*}(\Lambda(\mathcal{L})) = R^i p_{2,*}(m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1}) \otimes \mathcal{L}^{-1} = R^i p_{2,*}(m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1}),$$

because $R^i p_{2,*}(\Lambda(\mathcal{L}))$ is supported on $K(\mathcal{L})$ and $\mathcal{L}$ is trivial over $K(\mathcal{L})$. Hence the spectral sequence $E_2^{p,q} = H^p(X, R^q p_{2,*}\Lambda(\mathcal{L}))$ converges to both $H^{p+q}(X \times X, \Lambda(\mathcal{L}))$ and $H^{p+q}(X \times X, m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1})$. Thus these cohomology groups are the same.

Next, notice that $m \times p_1 : X \times X \xrightarrow{\sim} X \times X$ satisfies $(m \times p_1)^*(p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1}) = m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1}$. The cohomology of the former can be computed with the Künneth formula, which says that for $\mathcal{F}$ on X and $\mathcal{G}$ on Y quasi-coherent sheaves on separated k-schemes, we have

$$H^n(X \times Y, \mathcal{F} \boxtimes \mathcal{G}) = \bigoplus_{p+q=n} H^p(X, \mathcal{F}) \otimes H^q(Y, \mathcal{G}),$$

where $\mathcal{F} \boxtimes \mathcal{G} := p_1^*\mathcal{F} \otimes p_2^*\mathcal{G}$.
Applying this to our situation, we obtained $H^n(X \times X, \Lambda(\mathcal{L})) \cong H^n(X \times X, \mathcal{L} \boxtimes \mathcal{L}^{-1})$, so

$$\chi(\Lambda(\mathcal{L})) = \sum_n (-1)^n h^n(X \times X, \mathcal{L} \boxtimes \mathcal{L}^{-1}) = \sum_{p,q} (-1)^{p+q} h^p(X, \mathcal{L}) h^q(X, \mathcal{L}^{-1}) = \chi(\mathcal{L})\chi(\mathcal{L}^{-1}).$$

Finally, by the Riemann-Roch formula we know $\chi(\mathcal{L}^{-1}) = (-1)^g \chi(\mathcal{L})$, so we get

$$\chi(\Lambda(\mathcal{L})) = (-1)^g \chi(\mathcal{L})^2.$$

We already knew from Step 2.1 that $\chi(\Lambda(\mathcal{L})) = (-1)^g \deg(\varphi_{\mathcal{L}})$, so in fact $\deg(\varphi_{\mathcal{L}}) = \chi(\mathcal{L})^2$.

Step 3: Now suppose $\mathcal{L}$ is degenerate, i.e. $\varphi_{\mathcal{L}}$ is not an isogeny, i.e. $K(\mathcal{L})$ is infinite. Then by convention $\deg(\varphi_{\mathcal{L}}) = 0$, so we need to show $\chi(\mathcal{L}) = 0$. Similar to Step 2.2, we can show that

$$\chi(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1}) = (-1)^g \chi(\mathcal{L})^2,$$

and note that $m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1} = (\mathrm{id} \times \varphi_{\mathcal{L}})^*(\mathcal{P} \otimes p_1^*\mathcal{L})$. Now note that for any subscheme $G \subset K(\mathcal{L})$ of order r, we have a factorisation

$$\begin{tikzcd}
X \times X \arrow[rr, "\mathrm{id} \times \varphi_{\mathcal{L}}"] \arrow[dr] & & X \times X^t \\
& X \times X/G \arrow[ur, dotted] &
\end{tikzcd}$$

and the projection map is an isogeny. By the next corollary, we get that $\chi(m^*\mathcal{L} \otimes p_2^*\mathcal{L}^{-1})$ is divisible by $\operatorname{rk} G$. But $\operatorname{rk} G$ can be arbitrarily large, so $\chi(\mathcal{L}) = 0$. □

Corollary 1.7.7. Let $f : X \to Y$ be an isogeny and $\mathcal{L}$ a line bundle on Y. Then

$$\chi(X, f^*\mathcal{L}) = \deg(f)\chi(Y, \mathcal{L}).$$

Proof. Suppose f is an isogeny. Then

$$\chi(f^*\mathcal{L}) = \frac{c_1(f^*\mathcal{L})^g}{g!} = \frac{f^*(c_1(\mathcal{L})^g)}{g!}$$

so it suffices to show that $\int_X f^*[P] = \deg(f)$ for every closed point $P \in Y$. If f is separable, $f^{-1}(P)$ consists of $\deg(f)$ points with multiplicity one, so this case works. If f is purely inseparable, $f^{-1}(P)$ consists of a single point with multiplicity $\deg(f)$, so this case also works. Decomposing f into its separable and purely inseparable part (Proposition 1.3.14) and using that the degree is multiplicative gives the general case. □

This gives a new way to obtain a standard result about the cohomology of abelian varieties (which of course we can also deduce from Corollary 1.6.13):

Corollary 1.7.8. Let X be an abelian variety of positive dimension. Then $\chi(X, \mathcal{O}_X) = 0$.

Proof. The map $[n]_X$ has degree $n^{2g} > 1$ for $n > 1$. Applying Corollary 1.7.7, we obtain

$$\chi(X, \mathcal{O}_X) = n^{2g}\chi(X, \mathcal{O}_X),$$

so $\chi(X, \mathcal{O}_X) = 0$. □

Moreover, the proof of Theorem 1.7.6 lets us deduce an interesting statement about the cohomology of line bundles:

Corollary 1.7.9. Let $\mathcal{L}$ be a non-degenerate line bundle. Then there is a unique $0 \leq i \leq g$, called the *index* of $\mathcal{L}$, such that $H^i(X, \mathcal{L}) \neq 0$.

Proof. Arguing as in the above proof, we find that for $\mathcal{L}$ non-degenerate,

$$h^n(X \times X, \Lambda(\mathcal{L})) = \sum_{p+q=n} h^p(X, \mathcal{L})h^q(X, \mathcal{L}^{-1}) = \begin{cases} \deg(\varphi_{\mathcal{L}}) & n = g; \\ 0 & \text{otherwise.} \end{cases}$$

Thus h^p and h^q are non-zero for some $p + q = n$. If there existed $p' \neq p$ such that $h^{p'}(X, \mathcal{L}) \neq 0$, $h^{p'+q}(X \times X, \Lambda(\mathcal{L}))$ would be non-zero, which contradicts the formula. □

1.8 Characteristic polynomials

It might come as a surprise that one can define the notion of a characteristic polynomial for endomorphisms of abelian varieties, but one can, and it will have all the properties one expects of it. Before we get to it, let's recall what it means for a set-function between algebras to be polynomial.

Definition 1.8.1. Let K be a field, and let V be a free K-module (not necessarily of finite rank). A set-function $f \colon V \to K$ is said to be a *polynomial function* if for every $n > 0$ and any K-linearly independent set $\{v_1, \ldots, v_m\} \subset V$, there exists a polynomial $P \in K[X_1, \ldots, X_m]$ such that for any $\lambda_1, \ldots, \lambda_m \in K$,

$$f\left(\sum_{i=1}^{m} \lambda_i v_i\right) = P(\lambda_1, \ldots, \lambda_m).$$

Similarly, a function $V \to K^n$ is called polynomial if its n components are.
We say a polynomial function is *homogeneous of degree* r if for all $\lambda \in K$, we have $f(\lambda x) = \lambda^r f(x)$.

Remark 1.8.2. The reason for this slightly cumbersome definition is that we can not yet prove that endomorphism algebras of abelian varieties are finitely generated. We will see this in Corollary 2.1.3, but this result relies on the theory developed in this section, especially Theorem 1.8.4.

Note that if V is finite-dimensional with basis $\{e_1, \dots, e_n\}$, $f\colon V \to K$ is polynomial if and only if there is a polynomial P such that for any $v \in V$,

$$f(v) = f\left(\sum \lambda_i e_i\right) = P(\lambda_1, \dots, \lambda_n).$$

The precise polynomial P depends on the choice of basis, but the property of being (homogeneous) polynomial does not. One proof of this is that compositions of polynomial functions are polynomial, and one can check that the identity map $V \to V$ is a homogeneous degree 1 polynomial no matter which bases are chosen on the left and on the right.

Examples 1.8.3.
1. Any linear map is a homogeneous polynomial function of degree 1, as can be seen by choosing a matrix representing it.
2. Let L/k be a degree n field extension. Then the norm $\mathrm{Nm}_{L/k}$ and trace $\mathrm{Tr}_{L/k}$ are polynomial functions $L \to k$. Indeed, after choosing a k-basis for L, they are the compositions of the linear map $L \to M_{n\times n}(k)$ sending $\alpha \mapsto \cdot\alpha$, with the determinant, resp. trace function $M_{n\times n}(k) \to k$, both of which are clearly polynomial.
3. Given a bilinear map $B : S \times S \to T$, the composition $S \xrightarrow{\Delta} S \times S \xrightarrow{B} T$ is homogeneous of degree 2, as is easily verified by a calculation with an explicit basis.

Theorem 1.8.4. Let A be an abelian variety. Then there exists a homogeneous polynomial function of degree $2g$ on the endomorphism ring $\mathrm{End}^0(A)$ which sends $1 \otimes f \mapsto \deg f$.

Proof. Since A is projective, there exists an ample line bundle $\mathcal{L}$ on A. We may assume without loss of generality that it is symmetric; if not, replace it with $\mathcal{L} \otimes (-1)^*\mathcal{L}$. By Riemann-Roch and Corollary 1.7.7, we have

$$\chi(A, \mathcal{L}) = \frac{c_1(\mathcal{L})^g}{g!} \qquad \text{and} \quad \chi(A, f^*\mathcal{L}) = \deg(f)\chi(A, \mathcal{L}),$$

and hence

$$\deg(f) = \frac{c_1(f^*\mathcal{L})^g}{c_1(\mathcal{L})^g}.$$

Consider the map $\gamma : \mathrm{End}_k(A) \to \mathrm{CH}^1(A)$, $f \mapsto c_1(f^*\mathcal{L})$. We can write this as $\gamma = B_{\mathcal{L}}(f, f)/2$, where $B_{\mathcal{L}}\colon\ \mathrm{End}_k(A) \times \mathrm{End}_k(A) \to \mathrm{CH}^1(A)$ is given by

$$B_{\mathcal{L}}(f, h) = c_1((f + h)^*\mathcal{L} \otimes f^*\mathcal{L}^{-1} \otimes h^*\mathcal{L}^{-1});$$

here we use that $2^*\mathcal{L} \cong \mathcal{L}^4$ (Corollary 1.5.4).

It follows from the Theorem of the Cube (1.1.10) that $B_{\mathcal{L}}$ is bilinear: calculating $B_{\mathcal{L}}(f + f', h)$ and expanding $(f + f' + h)^*\mathcal{L}$ gives $B_{\mathcal{L}}(f, h) + B_{\mathcal{L}}(f', h)$. This says that in some sense, γ is a homogeneous degree 2 polynomial function. More explicitly, we verify that

$$f \longmapsto \deg f = \frac{\gamma(f)^g}{c_1(\mathcal{L})^g}$$

is homogeneous of degree $2g$. Let $f_1, \ldots, f_n$ be $\mathbb{Z}$-linearly independent endomorphisms and $a_1, \ldots, a_n \in \mathbb{Z}$. Then

$$\frac{\gamma(\sum a_i f_i)^g}{c_1(\mathcal{L})^g} = \frac{1}{2c_1(\mathcal{L})^g}\left(\sum_{i,j} a_i a_j B_{\mathcal{L}}(f_i, f_j)\right)^g = P(a_1, \ldots, a_n),$$

where $P \in \mathbb{Q}[X_1, \ldots, X_n]$ is the polynomial given by

$$\frac{1}{2c_1(\mathcal{L})^g}\sum_{k_{1,1}+\ldots+k_{n,n}=g}\binom{g}{k_{1,1}, \ldots, k_{n,n}}\prod_{i,j}(B_{\mathcal{L}}(f_i, f_j)X_iX_j)^{k_{i,j}},$$

by the multinomial theorem. Throughout this calculation, we've neglected to write the degree map $\mathrm{CH}^g(A) \to \mathbb{Z}$, but doing so makes clear that the polynomial has $\mathbb{Q}$-coefficients. It is also seen to be homogeneous of degree $2g$. Thus, the extension of $\deg\colon \mathrm{End}_k(A) \to \mathbb{N}$ to $\mathrm{End}^0(A)$ by declaring

$$q \otimes f \mapsto q^{2g} \deg f$$

gives a homogeneous degree $2g$ polynomial function on the endomorphism algebra. □

Definition 1.8.5. Let $f \in \mathrm{End}^0(A)$. The *characteristic polynomial* of f is defined to be

$$P_f(t) = \deg(t - f) \in \mathbb{Q}[t].$$

That is, $P_f(t)$ is the unique polynomial which interpolates the points $(n, \deg([n]_A - f)), n \in \mathbb{Z}$.

The minimal polynomial is monic and has degree $2g$ by Theorem 1.8.4. Indeed, since n and f both lie in the $\mathbb{Q}$-span of $\{\mathrm{id}_A, f\}$, we see that P can be represented by a two-variable polynomial $P(X, Y)$ (the case where id_A and f are linearly dependent is left as an exercise). Then $P(n, -1)$ is monic of degree $2g$ because the X^{2g}-coefficient of P is $\deg(\mathrm{id}_A) = 1$. We will also see that for $f \in \mathrm{End}_k(A)$, we have $P_f(t) \in \mathbb{Z}[t]$.

1.9 Weil pairings

The dual abelian variety bears a relationship to the theory of Cartier duals for finite group schemes. We saw that finite group schemes naturally occur as kernels of isogenies between abelian varieties, and in this setting the two dualities interact as well as possible [EvdGM, Thm. 7.5]:

Theorem 1.9.1. Let $f\colon X \to Y$ be an isogeny. Then $f^t\colon Y^t \to X^t$ is an isogeny as well, and

$$\ker f^t \cong (\ker f)^D.$$

We use this theorem to construct for each isogeny f a perfect pairing

$$e_f : \ker f \times \ker f^t \longrightarrow \mathbb{G}_m.$$

To do this, recall that the Cartier dual G^D represents the functor $\mathcal{H}om(G, \mathbb{G}_m)$, so that we can define the pairing on T-points via

$$e_f(x, y) = \alpha(y)(x),$$

where $\alpha : \ker f^t \xrightarrow{\sim} (\ker f)^D$. In particular, taking $f = [n]_X$ we get the *Weil pairings*

$$e_n : X[n] \times X^t[n] \longrightarrow \mu_n \subset \mathbb{G}_{m,k}.$$

To relate the Weil pairings for varying n, we need the following statement [EvdGM, Prop. 11.21(ii)]:

Proposition 1.9.2. Let $f : X \to Y$ and $g : Y \to Z$ be isogenies, and denote $h = g \circ f$. Then for all $x \in (\ker f)(T)$ and $y \in (\ker h^t)(T)$, we have

$$e_f(x, g^t(y)) = e_h(x, y).$$

We apply this to the case where $X = Y = Z$ and $f = [n]_X$, $g = [m]_X$. Then we obtain, for $x \in X[n](k_s)$ and $y \in X^t[nm](k_s)$,

$$e_{nm}(x, y) = e_n(x, my) = e_n(x, y)^m.$$

From this we can deduce that the Weil pairings e_{l^n} for varying n are compatible up to a twist (the so-called *Tate twist*), which we now explain. Consider the Tate modules $T_l(X) = \varprojlim X[l^n](k_s)$ and $T_l(X^t)$. Let $x = (0, x_1, x_2, \ldots) \in T_l(X)$ and $y = (0, y_1, y_2, \ldots) \in T_l(X^t)$ be elements, so $lx_{i+1} = x_i$ for all i. Then the above says that

$$e_{l^n}(x_n, y_n) = e_{l^{n+1}}(lx_{n+1}, y_{n+1}) = e_{l^{n+1}}(x_{n+1}, y_{n+1})^l.$$

This means that we can extend the Weil pairing to the Tate modules, and tensoring with $\mathbb{Q}$ gives

$$\langle -, - \rangle \colon V_l(X) \times V_l(X^t) \longrightarrow V_l(\mathbb{G}_m) =: \mathbb{Q}_l(1).$$

To finalise the construction, we can replace the duals by homomorphisms:

Definition 1.9.3. Let $f : X \to X^t$ be a homomorphism. Denote by e_n^f the pairing $X[n] \times X[n] \to \mu_n$ given by

$$e_n^f(x, y) = e_n(x, f(y)).$$

This extends to a pairing $H_f(x, y) := \langle x, f(y) \rangle \colon V_l(X) \times V_l(X) \to \mathbb{Q}_l(1)$.

We summarise the most important properties of this pairing in the following theorem:

Theorem 1.9.4. Let $f : X \to X^t$ be a homomorphism. Then the pairing H_f is bilinear, alternating, and $\mathrm{Gal}(k_s/k)$-equivariant. If f is an isogeny, it is non-degenerate.

As we will see, Weil pairings will play a crucial role in the proof of Tate's theorem. They will also appear again in Part II. It is sometimes useful to consider Weil pairings from the following point of view: one can associate to any ample divisor D the polarisation $f := \varphi_{\mathcal{O}(D)}$, which gives rise to the non-degenerate alternating pairing $H_f \in \mathrm{Hom}(\bigwedge^2 V_l(X), \mathbb{Q}_l(1))$. On the other hand, we have a chain of isomorphisms

$$H^2(X, \mathbb{Q}_l(1)) \xrightarrow{\sim} (\textstyle\bigwedge^2 H^1(X, \mathbb{Q}_l))(1) \xrightarrow{\sim} \mathrm{Hom}(\textstyle\bigwedge^2 H^1(X, \mathbb{Q}_l)^\vee, \mathbb{Q}_l(1)),$$

and since $H^1(X, \mathbb{Q}_l)^\vee \cong V_l(X)$, we again get a non-degenerate alternating pairing e^D associated to the element $\mathrm{cl}(D) \in H^2(X, \mathbb{Q}_l(1))$. This e^D is precisely the pairing H_f.

1.10 Polarisations

The last notion we need for Tate's theorem is that of a polarisation. Recall that we defined for any line bundle $\mathcal{L}$ a homomorphism $\varphi_{\mathcal{L}} \colon X \to X^t$ sending $x \mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$.

Definition 1.10.1. A homomorphism $f \colon X \to X^t$ is *symmetric* if $f = f^t$ under the canonical isomorphism $\kappa_X \colon (X^t)^t \cong X$ from Theorem 1.6.16.
A homomorphism $\vartheta \colon X \to X^t$ is called a *polarisation* if it is symmetric and there exists a field extension K/k such that ϑ_K is of the form $\varphi_{\mathcal{L}} \colon X_K \to X_K^t$ for an ample line bundle $\mathcal{L}$ on X_K. A polarisation is called *principal* if it is an isomorphism. In this case we say A is *principally polarised.*

Remark 1.10.2.
1. The line bundle $\mathcal{L}$ may not be defined over k, but if ϑ is a polarization, then there exists already a finite separable field extension K/k such that $\mathcal{L}$ is defined over K [EvdGM, Prop. 11.2].
2. Not every abelian variety is principally polarised, but elliptic curves always are (by the Abel-Jacobi theorem). However, any abelian variety over an algebraically closed field is isogenous to a principally polarised abelian variety [EvdGM, Cor. 11.26].
3. By Riemann-Roch (Theorem 1.7.6), the degree of an isogeny is always a square. Indeed, since the rank of a group scheme is invariant under base change, we have $\deg \vartheta = \deg \vartheta_K = \deg \varphi_{\mathcal{L}} = \chi(\mathcal{L})^2$. Moreover, we see that $\deg \vartheta = 1$ if and only if ϑ is principal.

To a polarisation $\vartheta : X \to X^t$ we can always associate an ample line bundle $\mathcal{M}$ on X, even if ϑ is not of the form $\varphi_{\mathcal{L}}$:

Proposition 1.10.3. Let $\vartheta : X \to X^t$ be a polarisation. Then the line bundle $\mathcal{M} := (\mathrm{id}, \vartheta)^* \mathcal{P}_X$ is ample on X.

Proof. Suppose K/k is an extension such that $\vartheta_K = \varphi_{\mathcal{L}}$. We have $\varphi_{\mathcal{M}} = \vartheta + \vartheta^t = 2\vartheta$, so $\varphi_{M_K} = 2\varphi_{\mathcal{L}} = \varphi_{\mathcal{L}^{\otimes 2}}$. Thus $\mathcal{M}$ is non-degenerate if and only if $\mathcal{L}$ is. Moreover, by the theory of indices of line bundles, one can show that $\mathcal{M}$ is effective if and only if $\mathcal{L}$ is effective if and only if $\mathcal{L}^{\otimes 2}$ is effective [EvdGM, Prop. 9.18(ii), Cor. 9.23]. Since being ample is equivalent to being effective and non-degenerate, the result follows. □

Proposition 1.10.4. Suppose $f : X \to Y$ is an isogeny and $\vartheta : Y \to Y^t$ is a polarisation. Then $f^*\vartheta := f^t \vartheta f$ is a polarisation of degree $\deg(f)^2 \deg(\vartheta)$.

Proof. By Theorem 1.9.1, $f^*\vartheta$ is a symmetric isogeny of degree $\deg(f)^2 \deg(\vartheta)$. To see that it is a polarisation, let K/k be such that $\vartheta_K = \varphi_{\mathcal{L}}$. Note that $f^t \varphi_{\mathcal{M}} f = \varphi_{f^*\mathcal{M}}$, since $t_x^* f^* \mathcal{M} = f^* t_{f(x)}^* \mathcal{M}$. Hence

$$(f^t \vartheta f)_K = f_K^t \varphi_{\mathcal{L}} f_K = \varphi_{f_K^* \mathcal{L}},$$

and $f_K^* \mathcal{L}$ is ample since f is finite. □

As a final application, we will define the Rosati involution on the endomorphism algebra of an abelian variety, which will play a role in Part II.

Definition 1.10.5. Let $\vartheta : X \to X^t$ be a polarisation. Since ϑ becomes invertible in $\mathrm{End}^0(X)$, we have a ring endomorphism of $\mathrm{End}^0(X)$ given by

$$f \longmapsto f^\dagger := \vartheta^{-1} f^t \vartheta,$$

called the *Rosati involution* associated to ϑ.

It is clear from the definition that the Rosati involution depends on the choice of ϑ only up to a conjugation. In particular, the restriction of $(-)^\dagger$ to the centre of the endomorphism algebra is well-defined.

An important fact about the Rosati involution is that it is positive [EvdGM, Thm. 12.26]. Thus, endomorphism algebras of abelian varieties are semisimple $\mathbb{Q}$-algebras equipped with a positive involution, which leads to a classification of abelian varieties into four types called the *Albert classification.* Unfortunately we will not go into this in more detail. However, we do have the tools at hand to prove another important application of the positivity of the Rosati involution, namely the Riemann hypothesis for abelian varieties over finite fields.

Suppose $k = \mathbb{F}_q$, and let X/k be an abelian variety. Then X has a Frobenius endomorphism π_X, which is topologically the identity and on sections sends $s \mapsto s^q$.

Theorem 1.10.6 (Riemann hypothesis for abelian varieties)**.** Let $X/\mathbb{F}_q$ be an abelian variety, and let f_X denote the characteristic polynomial of π_X. Then f_X has Weil q-numbers as roots.

Proof. Fix a polarisation $\vartheta : X \to X^t$. It is clear that π_X lies in the centre of $\operatorname{End}^0(X)$, so $\pi_X^\dagger$ does not depend on the choice of polarisation. We first show that $\pi_X^\dagger \pi_X = q$.
By definition,

$$\pi_X^\dagger \pi_X = \vartheta^{-1} \pi_X^t \vartheta \pi_X.$$

By Proposition 1.10.3, the bundle $\mathcal{L} := (\mathrm{id}, \vartheta)^* \mathcal{P}_X$ is ample on X, and we have $\varphi_{\mathcal{L}} = 2\vartheta$. Hence also

$$\pi_X^\dagger \pi_X = \varphi_{\mathcal{L}} \pi_X^t \varphi_{\mathcal{L}} \pi_X.$$

Thus, it suffices to show that $\pi_X^t \varphi_{\mathcal{L}} \pi_X = \varphi_{\mathcal{L}} [q]_X$. We check this on points. For $x \in X(T)$, we have

$$(\pi_X^t \varphi_{\mathcal{L}} \pi_X)(x) = \pi_X^* (t_{\pi_X(x)}^* \mathcal{L} \otimes \mathcal{L}^{-1}) = t_x^* \pi_X^* \mathcal{L}^{-1} \otimes \pi_X^* \mathcal{L}^{-1}.$$

Now since $\pi_X^* \mathcal{L} = \mathcal{L}^{\otimes q}$, this equals $\varphi_{\mathcal{L}^{\otimes q}}(x) = q \varphi_{\mathcal{L}}(x)$, as required.

Next, we use the positivity of the Rosati involution. We may assume that X is simple, in which case $\mathbb{Q}[\pi_X] \subset \operatorname{End}^0(X)$ is a number field preserved by the positive involution $(-)^\dagger$, since we just showed that $\pi_X^\dagger = q/\pi_X$. Hence $\mathbb{Q}[\pi_X]$ is either totally real and $(-)^\dagger = \mathrm{id}$, or $\mathbb{Q}[\pi_X]$ is an imaginary quadratic extension of a totally real field and $(-)^\dagger$ is complex conjugation. Since the roots of f_X are precisely the complex numbers occurring as $\iota(\pi_X)$ for some $\iota : \mathbb{Q}[\pi_X] \hookrightarrow \overline{\mathbb{Q}}$ (we will prove this in Proposition 2.4.4.1), the fact that $\pi_X^\dagger \pi_X = q$ means that $||\iota(\pi_X)||^2 = q$ for any ι. Moreover, f_X is monic with integer coefficients, so the roots of f_X are indeed Weil q-numbers. □

The above theorem deserves the name Riemann hypothesis (in the sense of the Weil conjectures) because as we will see, the roots of f_X are precisely the eigenvalues of Frobenius acting on the Tate module. Moreover, for abelian varieties, $H^1(X, \mathbb{Q}_l) \cong V_l(X)^\vee$, and $H^\bullet(X, \mathbb{Q}_l) \cong \bigwedge^\bullet H^1(X, \mathbb{Q}_l)$, so this determines the eigenvalues of Frobenius on the whole cohomology.

We now have the prerequisites needed to understand Tate's theorem.

2. Tate's theorem

In 1966, Tate published the beautiful paper "Endomorphisms of Abelian Varieties over Finite Fields" [Tat66], in which he proved the simplest case of the Tate conjecture. In this chapter, we will study the proof in detail.

2.1 Statement of the theorem

Setting: A is an abelian variety of dimension g over a finite field k of characteristic $p > 0$, and $G = \mathrm{Gal}(k) \cong \widehat{\mathbb{Z}}$, topologically generated by the Frobenius π. The theorem we want to prove is the following.

Theorem 2.1.1. Suppose k is a finite field of characteristic p, and let A', A'' be two abelian varieties defined over k. For any prime $l \neq p$, the map

$$\mathbb{Z}_l \otimes \mathrm{Hom}_k(A', A'') \longrightarrow \mathrm{Hom}_G(T_l(A'), T_l(A'')) \tag{2.1}$$

is an isomorphism.

The content of this statement is that the Tate module retains so much information about an abelian variety that G-equivariant morphisms between them always come from morphisms between the abelian varieties themselves. In particular, as we will see in Corollary 2.4.1, two abelian varieties are k-isogenous if and only if their Tate modules are G-isomorphic.

Half of the theorem is in fact doable without too much machinery:

Proposition 2.1.2. The map (2.1) is injective.

Proof. First note that $H := \mathrm{Hom}_k(A', A'')$ is torsion-free. We have remarked this before, but here is another argument: For $n > 0$, we have $nf = f \circ [n]_{A'}$ and $[n]_{A'}$ is surjective. So $nf = 0 \implies f = 0$.

To prove the proposition, we factor the map through the l-adic completion of $\mathrm{Hom}_k(A', A'')$:

$$\mathbb{Z}_l \otimes \mathrm{Hom}_k(A', A'') \xrightarrow{(1)} \widehat{\mathrm{Hom}_k(A', A'')} \xrightarrow{(2)} \mathrm{Hom}_G(T_l(A'), T_l(A''))$$

We will show injectivity of both maps.

(2): Since injections commute with inverse limits and since the right-hand side of (2) is its own l-adic completion, it suffices to show that

$$\mathrm{Hom}_k(A', A'')/(l^n) \longrightarrow \mathrm{Hom}_G(T_l(A'), T_l(A''))/(l^n)$$

is injective for all n. Suppose $\varphi \in \mathrm{Hom}_k(A', A'')$ such that $T_l(\varphi) = l^n f \in \mathrm{Hom}_G(T_l(A'), T_l(A''))$. Then $T_l(\varphi)$ vanishes on $A[l^n](k^s)$, i.e. $\varphi|_{A[l^n]} = 0$. Thus we get a factorisation

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d] & A \\
A/A[l^n] \arrow[r, "\sim"] \arrow[ur, dotted] & A \arrow[u, dotted, "g"']
\end{tikzcd}$$

Here the composition $A \to A/A[l^n] \xrightarrow{\sim} A$ is $[l^n]_A$. Hence $\varphi = l^n g$, i.e. $\varphi \equiv 0 \mod l^n$.

(1): Suppose we have an element $x = \sum x_i \otimes f_i$ in the kernel of (1). Let $M = \langle f_i \rangle_{\mathbb{Z}}$ be the free $\mathbb{Z}$-module generated by the f_i. Suppose for a moment that

$$M^{\text{sat}} := \{f \in \operatorname{Hom}_k(A', A'') \mid nf \in M \text{ for some } n \geq 1\}$$

is also finitely generated. Then $\mathbb{Z}_l \otimes M^{\text{sat}} \xrightarrow{\sim} \widehat{M^{\text{sat}}}$, since both sides can be identified with $\mathbb{Z}_l^n$ for some $n = \operatorname{rk}(M^{\text{sat}})$. Moreover, the map $\widehat{M^{\text{sat}}} \to \widehat{\operatorname{Hom}_k(A', A'')}$ is injective. To see this, we consider again the maps

$$M^{\text{sat}}/(l^n) \longrightarrow \operatorname{Hom}_k(A', A'')/(l^n).$$

Suppose $m \in M^{\text{sat}}$ satisfies the equation $m = l^n \varphi$ in $\operatorname{Hom}_k(A', A'')$. Then by definition of M^{sat}, we have $\varphi \in M^{\text{sat}}$, so already $m \equiv 0 \mod l^n$.

Now x already lies in $\mathbb{Z}_l \otimes M^{\text{sat}}$, and maps to zero in $\widehat{\operatorname{Hom}_k(A', A'')}$; hence $x = 0$ and (1) is injective.

It remains to show that if M is finitely generated, then so is M^{sat}.

By the Poincaré splitting theorem (1.4.2), we have an injection $\operatorname{Hom}_k(A', A'') \hookrightarrow \prod \operatorname{Hom}_k(A'_i, A''_j)$ for some simple abelian varieties A'_i, A''_j. If the saturation of M inside this product is finitely generated, we are done (since subgroups of finitely generated abelian groups are finitely generated); equivalently the saturation of the image of M in each factor of the product is finitely generated. So we may reduce to the case where A' and A'' are simple. But then $\operatorname{Hom}_k(A', A'') = 0$ unless A' and A'' are isogenous, in which case we get an injection $\operatorname{Hom}_k(A', A'') \hookrightarrow \operatorname{End}_k(A')$. This reduces us to the case where M is a finitely generated subgroup of $\operatorname{End}_k(A')$.

Now consider the finite-dimensional $\mathbb{Q}$-vector space $\mathbb{Q} \otimes M$. We can see M^{sat} as a sublattice: if $nf = g \in M$, then $f = \frac{1}{n} \otimes g \in \mathbb{Q} \otimes M$.

By Theorem 1.8.4, there exists a polynomial P which represents $f \mapsto \deg f$ after choosing a generating set for M. Then $U = \{|P(a \otimes f)| < 1\} \subset \mathbb{Q} \otimes M$ is an open neighbourhood of 0 such that $M^{\text{sat}} \cap U = 0$, since the degree of a non-zero endomorphism of a simple abelian variety is a non-zero integer. Thus M^{sat} is discrete in $\mathbb{Q} \otimes M$ and hence finitely generated. □

Since the right-hand side of (2.1) is finite-dimensional over $\mathbb{Z}_l$, we obtain the following remarkable fact:

Corollary 2.1.3. Let A and B be abelian varieties over a field k of positive characteristic. Then $\operatorname{Hom}_k(A, B)$ is a finitely generated abelian group.

Before we go on with the proof of Tate's theorem, it is natural to wonder how it relates to the Tate conjecture as described in the introduction. The connection is as follows:

Proposition 2.1.4. Tate's theorem is equivalent to the Tate conjecture (0.0.1) for abelian varieties over finite fields for $r = 1$.

Proof. We sketch a proof which relies on a number of identifications in étale cohomology. Firstly, there is a natural identification $H^1(A, \mathbb{Q}_l) \cong V_l(A)^\vee$. The Weil pairing

$$H^1(A, \mathbb{Q}_l) \times H^1(A^t, \mathbb{Q}_l) \longrightarrow \mathbb{Q}_l(-1)$$

then gives the identification $H^1(A^t, \mathbb{Q}_l) \cong V_l(A)$.
Using this, we have the following commutative diagram with G-equivariant maps:

$$\begin{tikzcd}
 & \mathbb{Q}_l \otimes \operatorname{End}_k(A) \arrow[rr] \arrow[dl, "(1)"'] & & \operatorname{End}_{\mathbb{Q}_l}(V_l(A)) & \\
\mathbb{Q}_l \otimes \operatorname{Pic}^0(A \times A^t) \arrow[dr, "(2)"'] & & & & (V_l(A))^\vee \otimes V_l(A) \arrow[ul, "\sim"'] \\
 & H^2(A \times A^t, \mathbb{Q}_l(1)) \arrow[rr, "(3)"] & & H^1(A, \mathbb{Q}_l) \otimes H^1(A^t, \mathbb{Q}_l(1)) \arrow[ur, "\sim"] &
\end{tikzcd}$$

Here the maps are as follows:

- (1): Induced by $\operatorname{End}_k(A) \ni f \longmapsto (f \times \mathrm{id})^* \mathcal{P}_A$;
- (2): Induced by the cycle class map on $\operatorname{Pic}^0(A \times A^t) \subset \operatorname{CH}^1(A \times A^t)$;
- (3): Induced by the Künneth isomorphism.

In Lemma 2.2.2, we will see that Tate's theorem is equivalent to the upper horizontal map being an isomorphism after taking G-equivariant endomorphisms on the target, which holds if and only if $(3) \circ (2) \circ (1)$ is an isomorphism after taking G-invariants on the target, which is equivalent to the Tate conjecture for $A \times A^t$ and $r = 1$. □

2.2 Reduction steps

It remains to show surjectivity of (2.1). In order to prove this, we start with some preliminary reduction steps.

Lemma 2.2.1. Consider the map

$$\mathbb{Q}_l \otimes_{\mathbb{Z}_l} \operatorname{Hom}_k(A', A'') \longrightarrow \operatorname{Hom}_G(V_l(A'), V_l(A'')). \tag{2.2}$$

Then (2.2) is injective, and bijective if and only if (2.1) is.

Proof. The map (2.2) is obtained by tensoring (2.1) with $\mathbb{Q}_l$ and then composing with the natural map

$$\mathbb{Q}_l \otimes_{\mathbb{Z}_l} \operatorname{Hom}_G(T_l(A'), T_l(A'')) \longrightarrow \operatorname{Hom}_G(V_l(A'), V_l(A'')).$$

This is an isomorphism because $T_l(A')$ is a free $\mathbb{Z}_l$-module of rank $2g$, so both sides can be identified with the G-invariant elements of $V_l(A'')^{2g}$. A map of this form is in general an isomorphism if whatever is in place of $T_l(A')$ is finitely presented.

Now injectivity of (2.2) is just flatness of $\mathbb{Q}_l$ over $\mathbb{Z}_l$. For the converse, denote by C the cokernel of the map (2.1); then we want to show that $\mathbb{Q}_l \otimes C = 0 \iff C = 0$. For this it suffices that C is torsion-free (as in any case it is finitely generated over a PID). Elements of C can only be annihilated by elements of the form l^n, so we will check that there is no l-torsion.

Suppose $\varphi : T_l(A') \to T_l(A'')$ is such that $l\varphi = \sum a_i \otimes T_l(f_i)$. Then $l\varphi$ is a limit of elements in $\operatorname{Hom}_G(T_l(A'), T_l(A''))$ of the form $T_l(f^{(n)})$ for $f^{(n)} = \sum a_{i,n} f_i$, where $a_{i,n} = a_i \pmod{l^n}$. Hence

$T_l(f^{(n)}) \in l\,\mathrm{Hom}_G(T_l(A'), T_l(A''))$ for large enough n. Thus $A[l] \subset \ker f^{(n)}$ for large n, meaning $f^{(n)}$ factors through l, i.e. we can write $f^{(n)} = lg^{(n)}$ for some $g^{(n)}$. If we denote by f the limit of the $f^{(n)}$ in $\mathbb{Z}_l \otimes \mathrm{Hom}_k(A', A'')$, then also f is a multiple of l, say $f = lg$. But by construction $T_l(f) = l\varphi$, so $T_l(g) = \varphi$, i.e. $\varphi = 0 \in C$. □

Next, we will see that we can restrict to endomorphism rings and a single prime l.

Lemma 2.2.2. To prove bijectivity of (2.2) for any pair of abelian varieties and any prime $l \neq p$, it suffices to show that there exists one l such that for any abelian variety A, the map

$$\mathbb{Q}_l \otimes \mathrm{End}_k(A) \hookrightarrow \mathrm{End}_G(V_l(A)) \tag{2.3}$$

is surjective, and that the dimension of the right-hand side does not depend on l.

Proof. To compare the statement with endomorphism rings to the statement with Hom-spaces, consider the product variety $A' \times A''$. This is a biproduct, so

$$\mathrm{End}_k(A' \times A'') \cong \mathrm{End}_k(A') \times \mathrm{Hom}_k(A', A'') \times \mathrm{Hom}_k(A'', A') \times \mathrm{End}_k(A'').$$

Similarly, $V_l(A' \times A'') \cong V_l(A') \times V_l(A'')$, and this is a biproduct too (in the category of G-modules). By naturality, we get a commutative square

$$\begin{tikzcd}
\mathbb{Q}_l \otimes \mathrm{End}_k(A' \times A'') \arrow[r, "\sim"] \arrow[d] & \mathbb{Q}_l \otimes \begin{pmatrix} \mathrm{End}_k(A') & \mathrm{Hom}_k(A', A'') \\ \mathrm{Hom}_k(A'', A') & \mathrm{End}_k(A'') \end{pmatrix} \arrow[d] \\
\mathrm{End}_G(V_l(A \times A'')) \arrow[r, "\sim"] & \begin{pmatrix} \mathrm{End}_G(V_l(A')) & \mathrm{Hom}_G(V_l(A'), V_l(A'')) \\ \mathrm{Hom}_G(V_l(A''), V_l(A')) & \mathrm{End}_G(V_l(A'')) \end{pmatrix}
\end{tikzcd}$$

If either of the vertical maps is an iso, so is the other one. The right vertical map is a product of maps of the form (2.1), and is an isomorphism if and only if all its components are.

For the l-independence, note that the dimension of the left-hand side of (2.3) does not depend on l. If the right-hand side also has l-independent dimension, we see that the map is an isomorphism for all $l \neq p$ as soon as it is for one, because it is always injective by Proposition 2.1.2. □

As a final reduction step, we consider two subalgebras of $\mathrm{End}(V_l(A))$ ($\mathbb{Q}_l$-linear endomorphisms):

- $E_l :=$ the image of the injection (2.3);
- $F_l :=$ the subalgebra generated by G.

The following classical theorem is our main ingredient:

Theorem 2.2.3 (Double Centraliser Theorem)**.** Let R be a semisimple algebra over a field k, and let V be a faithful R-module which is finite-dimensional over k. Then

$$C_{\mathrm{End}_k(V)}(C_{\mathrm{End}_k(V)}(R)) = R,$$

where $C_{\mathrm{End}_k(V)}(R')$ denotes the centraliser of R' in $\mathrm{End}_k(V)$.

The last reduction step is as follows:

Lemma 2.2.4. If F_l is semisimple (as an algebra), the bijectivity of (2.3) is equivalent to F_l being the centraliser of E_l in $\operatorname{End}(V_l(A))$.

Proof. By general theory, semisimplicity is preserved under tensoring with characteristic 0 field extensions. Thus by Proposition 1.4.4, $E_l \cong \mathbb{Q}_l \otimes \operatorname{End}_k(A)$ is semisimple. Then we can apply the double centraliser theorem in the case $k = \mathbb{Q}_l$, $V = V_l(A)$, and $R = F_l$, resp. E_l to obtain

$$C_{\operatorname{End}(V_l(A))}(C_{\operatorname{End}(V_l(A))}(F_l)) = F_l, \tag{2.4}$$

$$C_{\operatorname{End}(V_l(A))}(C_{\operatorname{End}(V_l(A))}(E_l)) = E_l. \tag{2.5}$$

The key observation is that by definition,

$$C_{\operatorname{End}(V_l(A))}(F_l) = \{f \in \operatorname{End}(V_l(A)) \mid f \circ \varphi = \varphi \circ f \ \forall \varphi \in F_l\} = \operatorname{End}_G(V_l(A)),$$

as F_l is generated by G.

Now suppose (2.3) is bijective. Then $E_l = C_{\operatorname{End}(V_l(A))}(F_l)$, so equation (2.4) gives that F_l is the centraliser of E_l, as required.

Conversely, suppose that F_l is the centraliser of E_l. Then equation (2.5) says that E_l is the centraliser of F_l, i.e. $E_l = \operatorname{End}_G(V_l(A))$, i.e. (2.3) is surjective. □

2.3 The proof

After the reduction steps, it suffices to show that the dimension of $\operatorname{End}_G(V_l(A))$ does not depend on the prime l, and that there exists an l such that F_l is semisimple and equals the centraliser of E_l in $\operatorname{End}_{\mathbb{Q}_l}(V_l(A))$.

One of the main actors in the proof will be the Frobenius endomorphism of an abelian variety. If $k = \mathbb{F}_q$, this is simply the endomorphism π_A of A sending $x \mapsto x^q$ on sections. It is a homomorphism, so it acts on the Tate module. Denoting by $\mathbb{F}$ an algebraic closure of k, we have for all n a commutative diagram

$$\begin{tikzcd}
\operatorname{Spec}(\mathbb{F}) \arrow[r] \arrow[d, "\pi"'] & A[l^n] \arrow[d, "\pi_A"] \\
\operatorname{Spec}(\mathbb{F}) \arrow[r] & A[l^n]
\end{tikzcd}$$

and hence the action of π_A is the same as the action of $\pi^{-1} \in \operatorname{Gal}(\mathbb{F}_q)$.

Lemma 2.3.1. Let A be an abelian variety over a finite field. Then $\mathbb{Q}[\pi_A] \subseteq \operatorname{End}^0(A)$ is a semisimple algebra. In particular, if π_A acts on a K-algebra with K a field of characteristic zero, then it acts semisimply.

Proof. From the definition of the Frobenius endomorphism, we see that it lies in the centre of the endomorphism algebra. Now a commutative $\mathbb{Q}$-algebra is semisimple if and only if it is reduced. In our case, $\operatorname{End}^0(A)$ is a product of matrix rings over division algebras, so the centre is a product of fields, hence reduced. For the last statement, note that semisimplicity is preserved under tensoring with characteristic zero field extensions, and a K-algebra is semisimple if and only if it acts semisimply on any representation. □

After Tate's theorem, we will be able to prove that in fact $\mathbb{Q}[\pi_A] = Z(\mathrm{End}^0(A))$.

The next observation is a finiteness statement. In our case, we obtain it because we work over a finite field, but a variant of this finiteness hypothesis is also what makes Faltings' proof of the analogue of Tate's theorem over number fields work. We briefly recall the definition of Hilbert polynomials:

Let $\mathcal{L}$ be an ample line bundle on a projective scheme X. Then for any coherent $\mathcal{O}_X$-module $\mathcal{F}$, the Euler characteristic of $\mathcal{F} \otimes \mathcal{L}^{\otimes n}$ is polynomial in n. More precisely, we have

$$\Phi_{\mathcal{F},\mathcal{L}}(n) = \chi(\mathcal{F} \otimes \mathcal{L}^{\otimes n}) \in \mathbb{Q}[n].$$

This is called the *Hilbert polynomial* of $\mathcal{F}$ with respect to $\mathcal{L}$. Given an embedding $i : X \hookrightarrow \mathbb{P}_k^N$, the Hilbert polynomial of X is defined as $\Phi_X := \Phi_{\mathcal{O}_X, i^*\mathcal{O}(1)}$.

Lemma 2.3.2. Let A be an abelian variety over a finite field k, and let $d \geq 1$ be an integer. Then there are only finitely many isomorphism classes of abelian varieties B which carry a degree d^2 polarisation over k and are isogenous to A.

Proof. This follows from the theorem of Grothendieck that the Hilbert scheme of subschemes of $\mathbb{P}_k^N$ with given Hilbert polynomial is of finite type over k and thus has finitely many k-points [FGI+00, Chapter 5], Chapter 5. Assuming this, let λ be a degree d^2 polarisation on B, and let $\mathcal{L}$ be the corresponding ample line bundle. As mentioned in Remark 1.2.7, $\mathcal{L}^{\otimes 3}$ is very ample, and by Riemann-Roch and Corollary 1.7.9,

$$h^0(\mathcal{L}^{\otimes 3}) = \chi(\mathcal{L}^{\otimes 3}) = \frac{c_1(\mathcal{L}^{\otimes 3})^g}{g!} = \frac{3^g c_1(\mathcal{L})^g}{g!} = 3^g d,$$

so we obtain an embedding of B into $\mathbb{P}_k^N$, where $N = 3^g d - 1$. Moreover, the Hilbert polynomial of this embedding is given by

$$\Phi_B(n) = \chi(\mathcal{L}^{\otimes 3n}) = \frac{c_1(\mathcal{L}^{\otimes 3n})^g}{g!} = (3n)^g d.$$

Thus, both N and Φ_B depend only on g and d. This proves the lemma. □

Since we are studying centralisers, the following lemma will be useful.

Lemma 2.3.3. Let K be a field of characteristic zero, and let V and W be a finite-dimensional K-vector spaces. Suppose $\varphi_V \in \mathrm{End}_K(V)$, $\varphi_W \in \mathrm{End}_K(W)$ act semisimply. Then

$$\dim\{f \in \mathrm{End}_K(V) \mid \varphi_W \circ f = f \circ \varphi_V\} = r(\varphi_V, \varphi_W),$$

where

$$r(\varphi_V, \varphi_W) := \sum_P a(P) b(P) \deg(P)$$

and $f_V = \prod_P P^{a(P)}$, $f_W = \prod_P P^{b(P)}$ are the decomposition of the characteristic polynomials of φ_V and φ_W into irreducible factors.

Proof. The situation clears up when we regard V and W as $K[X]$ modules, with X acting through φ_V, resp. φ_W. Then the semisimplicity assumption implies that V and W decompose according to the characteristic polynomials. More precisely, we write $M_P := K[X]/(P(X))$ for the simple $K[X]$-module corresponding to the irreducible polynomial P. Then we have

$$V \cong \bigoplus_P M_P^{a(P)}, \qquad W \cong \bigoplus_P M_P^{b(P)}.$$

Now $\dim_K \operatorname{Hom}_{K[X]}(M_P, M_Q)$ is zero unless $P = Q$, in which case it is $\deg(P)$ (consider the image of $1 \in M_P$). Thus indeed $\operatorname{Hom}_{K[X]}(V, W) = r(\varphi_V, \varphi_W)$. □

Note that the value $r(f, g)$ does not depend on the field over which f and g are factorised, because irreducible polynomials have no repeated factors in characteristic zero.

Proposition 2.3.4. The dimension of $\operatorname{End}_G(V_l(A))$ is independent of the prime l.

Proof. The Frobenius π_A acts on $V_l(A)$ via a matrix. Let f_A be its characteristic polynomial. Then f_A has $\mathbb{Q}$-coefficients which do not depend on l (see Theorem 2.3.5 for a proof), and we can factorise it over any extension K of $\mathbb{Q}$ as

$$f_A = \prod_P P^{a(P)}$$

where the product is over all irreducible polynomials in $K[X]$.

We want to determine $r := \dim \operatorname{End}_G(V_l(A))$. Since G is topologically generated by the Frobenius element, which acts on $V_l(A)$ as the inverse to π_A, we obtain

$$r = \dim\{f \in \operatorname{End}_{\mathbb{Q}_l}(V_l(A)) \mid \pi_A \circ f = f \circ \pi_A\}.$$

By Lemma 2.3.1, the Frobenius morphism acts semisimply, so by Lemma 2.3.3, $r = r(f_A, f_A)$. This is independent of l, as required. □

It remains to show that there exists some l for which $\mathbb{Q}_l \otimes \operatorname{End}_k(A) \xrightarrow{\sim} \operatorname{End}_G(V_l(A))$, or equivalently, for which F_l is semisimple and equals the centraliser of E_l in $\operatorname{End}_k(V_l(A))$.

Let $\vartheta : A \to A^t$ be a polarisation of A defined over k, and denote $\deg \vartheta = d^2$. Then the function

$$H_\vartheta : V_l(A) \times V_l(A) \longrightarrow \mathbb{Q}_l(1), \qquad (x, y) \longmapsto \langle x, \vartheta(y) \rangle$$

where $\langle -, - \rangle$ denotes the Weil pairing, defines a non-degenerate alternating bilinear form (cf. Theorem 1.9.4). Recall that a subspace $W \subset V$ is called *isotropic* with respect to a form if $\langle W, W \rangle = 0$.

The rest of the proof now goes as follows:

1. There exists an l for which F_l is isomorphic to a direct sum of copies of $\mathbb{Q}_l$.
2. For any such l, let D denote the centraliser of E_l. Let W be an isotropic subspace of $V_l(A)$ which is stable under G. By descending induction on $\dim W$, show that W is stable under D.
3. Applying this result with $\dim W = 1$, we see that every eigenvector of F_l in $V_l(A)$ is an eigenvector of D: indeed, if $F_l v \subseteq \langle v \rangle$, then $\langle v \rangle$ is stable under G and so also $Dv \subseteq \langle v \rangle$. Now $F_l \cong \bigoplus \mathbb{Q}_l$ decomposes $V_l(A) \cong \bigoplus V_i$ as an F_l-algebra, on each of whose summands F_l acts by a scalar. So D acts on every summand by a scalar too.

4. An endomorphism d acting on each non-zero element of a vector space V_i by a scalar must be a scalar. Indeed, for any v, w non-zero, $d(v+w) = \lambda(v+w) = \mu_1 v + \mu_2 w$, so $\mu_1 = \mu_2$. So $D \subseteq F_l$ which implies $D = F_l$, so we are done.

Proof of 1. Consider again $\mathbb{Q}[\pi_A] \subseteq \operatorname{End}^0(A)$. We saw that this is a semisimple subalgebra contained in the centre, hence is a product of fields, say $\prod K_i$. We also know $F_l = \mathbb{Q}_l \otimes \mathbb{Q}[\pi_A]$, so we can write

$$F_l = \prod_{v \mid l} (K_i)_v,$$

so it is a product of l-adic fields. We now want to show that there exists a prime l such that $(K_i)_v \cong \mathbb{Q}_l$ for all i and all $v \mid l$. For this, we need l to split completely in all the K_i, i.e. (l) needs to be a product of distinct prime ideals in $\mathcal{O}_{K_i}$. This is the case for infinitely many primes l: by Chebotarev, the primes that split completely in a finite Galois extension $K/\mathbb{Q}$ have positive density, and any such prime must be split in any subextension; so take for K the Galois closure of the compositum of the K_i. □

Proof of 2: Base case. Suppose W is a G-stable subspace which is maximal isotropic for H_ϑ (this exists because F_l acts by diagonal matrices, hence we can pick a basis of G-stable elements). Consider for $n \geq 0$

$$X_n := (T_l(A) \cap W) + l^n T_l(A)$$

which is an index l^{ng} $\mathbb{Z}_l$-submodule of $T_l(A)$.

Let X_n' be the image of X_n in $T_l(A)/l^n T_l(A) \cong A[l^n](k_s)$. Since X_n' is a G-stable subset, it in fact defines a finite subgroup scheme of order l^{ng}, so we can take the quotient $B(n) := A/X_n'$ and get a separable isogeny $A \to B(n)$. Since $l^n T_l(A) \subset X_n$, the map $l^n : A \to A$ factors through a map $f_n : B(n) \to A$. Its kernel is X_n', so $\deg f_n = l^{ng}$.

We now want to show that $\operatorname{im} T_l(f_n) = X_n$. The factorisation

$$T_l(A) \to T_l(B(n)) \xrightarrow{T_l(f_n)} T_l(A)$$

is multiplication by l^n. This implies that $\operatorname{im} T_l(f_n)$ contains $l^n T_l(A)$, and we have

$$\frac{\operatorname{im} T_l(f)}{l^n T_l(A)} \cong \operatorname{im}(f : B(n)[l^n](k_s) \to A[l^n](k_s)). \tag{2.6}$$

Since $B(n) = A/X_n'$, we have $B(n)[l^n](k_s) = [l^n]_A^{-1}(X_n')/X_n'$, and under this identification, f simply sends $a + X_n' \mapsto l^n a + X_n'$. In other words, the image from (2.6) is precisely X_n', so the image of $T_l(f)$ is precisely X_n.

Now $B(n)$ has a degree d^2 polarisation $l^{-n} f_n^* \vartheta$ defined over k. To see this, note that $f_n^* \vartheta = f_n^t \vartheta f_n$ is a polarisation of degree $(\deg f_n)^2 \deg \vartheta = l^{2gn} d^2$ (cf. Proposition 1.10.4). Considering now the alternating bilinear form $H_{f_n^* \vartheta} : T_l(B(n)) \times T_l(B(n)) \to \mathbb{Z}_l(1)$, we have

$$H_{f_n^* \vartheta}(x, y) = \langle x, f_n^t \vartheta f_n y \rangle = \langle f_n x, \vartheta f_n y \rangle = H_\vartheta(f_n x, f_n y).$$

Now $f_n x, f_n y$ lie in X_n and W is isotropic for H_ϑ, so $H_\vartheta(X_n, X_n) = H_\vartheta(l^n T_l(A), X_n) \subset l^n \mathbb{Z}_l(1)$. This implies that the polarisation $f_n^* \vartheta$ can be written as $\psi_n \circ l^n$, where ψ_n is a polarisation of degree d^2. This shows that $B(n)$ has the claimed polarisation.

Since each $B(n)$ is isogenous to A, Lemma 2.3.2 implies that infinitely many of the $B(n)$ are isomorphic. Say $I \subset \mathbb{N}$ is an infinite index set such that $B(i) \cong B(j)$ for all $i, j \in I$. Let n be the minimal element in I and let $v_i : B(n) \to B(i)$ be an isomorphism. Let $u_i := f_i v_i f_n^{-1} \in \operatorname{End}^0(A)$. Then $V_l(u_i)(X_n) = X_i \subset X_n$. By compactness of $\operatorname{End}_{\mathbb{Z}_l}(X_n)$ there is a convergent subsequence $(V_l(u_j))_{j\in J}$ of $(V_l(u_i))$, say with limit $u : X_n \to X_n$. Since the $V_l(u_i)$ live in E_l, which is closed, also $u \in E_l$.

Putting everything together, $u(X_n) = \bigcap_{j\in J} X_j = T_l(A) \cap W$, so $u(V_l(A)) = W$. So if D is the centraliser of E_l, we have $DW = Du(V_l(A)) = u(DV_l(A)) \subseteq u(V_l(A)) = W$, which is what we wanted. □

Proof of 2: Inductive step. Suppose W is a G-stable isotropic subspace with $\dim W < g$. The orthogonal complement $W^\perp$ is G-stable too, because ϑ and the Weil pairing are both G-equivariant. Hence both W and $W^\perp$ are stable under F_l, which we assumed to be a product of copies of $\mathbb{Q}_l$. Therefore

$$W^\perp = W \oplus \sum_{i=1}^{m} L_i,$$

where each L_i is a one-dimensional F_l-stable $\mathbb{Q}_l$-vector space. Since the bilinear form is non-degenerate, $W \oplus W^\perp \cong V_l(A)$, so $m = 2(g - \dim W) \geq 2$, so we can write $W = (W \oplus L_1) \cap (W \oplus L_2)$. Each of the $W \oplus L_i$ is isotropic since W and the L_i are isotropic subspaces with $L_i \subset W^\perp$. They are also G-stable, so by induction D preserves $W \oplus L_1$ and $W \oplus L_2$, hence W. □

We have one fact left to prove, which we used in Proposition 2.3.4:

Theorem 2.3.5. The characteristic polynomial of the Frobenius action on $V_l(A)$ is independent of $l \neq p$.

Proof. More generally, we will show that if $f : A \to A$ is any endomorphism, then

$$\deg f = \det V_l(f).$$

From this we can deduce that the characteristic polynomial $P(t)$ of $V_l(f)$ coincides with the characteristic polynomial of f. Indeed, for any $n \in \mathbb{Z}$, we have

$$\begin{aligned} P(n) &= \det(n \cdot \mathbb{1} - V_l(f)) \\ &= \det(V_l([n]_A - f)) \\ &= \deg([n]_A - f). \end{aligned}$$

It follows moreover that $P(t)$ has $\mathbb{Z}$-coefficients. Indeed, its coefficients lie in $\mathbb{Q}$ because this is true for the characteristic polynomial of f. Moreover, $\operatorname{End}_k(A)$ is free of finite rank over $\mathbb{Z}$, so any endomorphism f satisfies a monic polynomial $Q \in \mathbb{Z}[t]$; hence so does $V_l(f)$. Since the minimal polynomial of $V_l(f)$ divides Q, its roots are algebraic integers, and therefore so are its coefficients. So these coefficients are rational algebraic integers, so rational integers. Incidentally, this shows that the characteristic polynomial of any endomorphism lies in $\mathbb{Z}[t]$.

So let's show that $\deg f = \det V_l(f)$. By a *norm form* on a K-algebra R we mean a non-zero polynomial function $N \colon R \to K$ such that $N(ab) = N(a)N(b)$. The functions $f \mapsto \deg f$ and $f \mapsto \det V_l(f)$ are multiplicative and polynomial, so both extend uniquely to norm forms of degree $2g$ on $\mathbb{Q}_l \otimes \operatorname{End}_k(A)$. We denote them by N_1 and N_2, respectively.

We first show that $|\deg f|_l = |\det V_l(f)|_l$. To determine $|\deg f|_l$, we have to know what power of l divides f, and we see that this power of l is the $(2g)^{-1}$-power of the order of the cokernel of $f : A[l^n](k_s) \to A[l^n](k_s)$ for $n \gg 0$. Passing to the limit, this is the same as the order of the cokernel of $V_l(f)$, but at the same time this measures how many times l divides $V_l(f)$. Finally,

$$\deg(l^n f) = l^{2gn} \deg(f), \qquad \det(l^n V_l(f)) = l^{2gn} \det(V_l(f)),$$

so the l-adic orders are equal.

Since polynomials and the l-adic norm are continuous and $\mathbb{Z}$ is dense in $\mathbb{Z}_l$, we also have $|N_1(\alpha)|_l = |N_2(\alpha)|_l$ for all $\alpha \in \mathbb{Z}_l \otimes \mathrm{End}_k(A)$, and finally since $N(l^{-n}\alpha) = N(l)^{-n}N(\alpha)$ we have $|N_1(\alpha)|_l = |N_2(\alpha)|_l$ for all $\alpha \in \mathbb{Q}_l \otimes \mathrm{End}_k(A)$.

An important fact about norm forms is that for a *simple* finite-dimensional K-algebra A, there exists a canonical norm form N on A such that any other norm form on A is a power of N [Mum74, §19]. Thus, taking $\mathbb{Q}_l \otimes \mathrm{End}_k(A) \cong \prod_{i=1}^r A_i$ as a product of simple algebras, we can write N_1 and N_2 as a product of norm forms on the individual factors, so that

$$N_1(\alpha_1, \ldots, \alpha_r) = \prod_{i=1}^r N_i(\alpha_i)^{n_{1,i}},$$

where each of the norms N_i is the canonical norm form on A_i. Similarly we can decompose N_2.

Now let $1 \le j \le r$. Setting $\alpha_i = 1$ for all $i \ne j$, we see that

$$|N_j(\alpha_j)^{n_{1,j} - n_{2,j}}|_l = 1$$

for all $\alpha_j \in A_j$. Since N_j is homogeneous of positive degree, this means $n_{1,j} = n_{2,j}$, and since j was arbitrary, we obtain $N_1 = N_2$. □

This finishes the proof of Tate's theorem.

2.4 Consequences

Tate's theorem has some interesting corollaries. In a vague sense, we now know that any Tate l-module contains lots of information about the abelian variety. Let's make this more precise.

Corollary 2.4.1. Let A and B be abelian varieties over a finite field, and denote by f_A and f_B the characteristic polynomials of their Frobenius endomorphisms. Then the following statements are equivalent:

1) A and B are isogenous;

2) $V_l(A)$ and $V_l(B)$ are G-isomorphic;

3) $f_A = f_B$;

4) A and B have the same zeta functions.

Proof. 1) $\implies$ 2): An isogeny $\varphi\colon A \to B$ has finite kernel, and $\dim\ker V_l(\varphi) = 2\dim\ker(\varphi)$ (use Poincaré splitting). Hence $V_l(\varphi)$ is a G-equivariant isomorphism $V_l(A) \xrightarrow{\sim} V_l(B)$.
2) $\implies$ 1): Given a G-equivariant isomorphism $\psi : V_l(A) \to V_l(B)$, we can find by Theorem

2.1.1 a sequence $(\varphi_i)_{i\in\mathbb{N}}$ of morphisms $A \to B$ such that $(V_l(\varphi_i))$ approximates ψ. Since ψ is injective, $\dim\ker(\varphi_i) = 0$ for large enough i, and such φ_i will be an isogeny.
2) $\implies$ 3): This holds because f_A and f_B are determined by the action of the Frobenius element in G on $V_l(A) \cong V_l(B)$.
3) $\implies$ 2): We saw in the proof of the theorem that the Frobenius element acts semisimply on the Tate module, and hence the isomorphism class of a representation is determined by its characteristic polynomial.
3) $\iff$ 4): By the Weil conjectures, the zeta function is determined by the eigenvalues of Frobenius acting on the étale cohomology, which are determined by the eigenvalues of the Frobenius acting on the Tate modules (remember $V_l(A) \cong H^1(A, \mathbb{Q}_l)^\vee$), which are determined by the characteristic polynomials f_A, resp. f_B. □

One can also say more about endomorphism algebras. For instance:

Corollary 2.4.2. Suppose A is a g-dimensional abelian variety over a finite field. Then we have $2g \leq \dim \mathrm{End}^0(A) \leq 4g^2$.

Proof. Let f_A be the characteristic polynomial of the Frobenius of A, and suppose it factors into irreducibles as $\prod_P P^{a(P)}$. Then we have seen that

$$\dim \mathrm{End}^0(A) = \dim \mathrm{End}_G(V_l(A)) = \sum_P a(P)^2 \deg(P).$$

Since the degree of f_A is $2g$, we have $\dim \mathrm{End}^0(A) \geq 2g$ with equality if and only if P has all distinct roots, and $\dim \mathrm{End}^0(A) \leq 4g^2$ with equality if and only if f_A is a power of a linear polynomial. In the latter case, the centre of the endomorphism algebra is trivial and A is isogenous to the g^{th} power of a supersingular elliptic curve. □

Corollary 2.4.3. Let A be an abelian variety over a finite field. Then $Z(\mathrm{End}^0(A)) = \mathbb{Q}[\pi_A]$.

Proof. We already saw $\mathbb{Q}[\pi_A] \hookrightarrow Z(\mathrm{End}^0(A))$. By Lemma 2.2.4 and Tate's theorem,

$$\mathbb{Q}_l \otimes \mathbb{Q}[\pi_A] = F_l = C_{\mathrm{End}(V_l(A))}(E_l) = \mathbb{Q}_l \otimes Z(\mathrm{End}^0(A)),$$

so $\mathbb{Q}[\pi_A] = Z(\mathrm{End}^0(A))$. □

Classification of isogeny classes over $\mathbb{F}_q$

If A is simple (or a power of a simple), $\mathrm{End}^0(A)$ is a division algebra, so $\mathbb{Q}[\pi_A]$ is a field which we can study abstractly.

Proposition 2.4.4. Let A be a g-dimensional simple abelian variety over a finite field, and let f be the characteristic polynomial of its Frobenius endomorphism. Let $\mathbb{Q}[\pi_A]$ be the centre of $\mathrm{End}^0(A)$, and let h be the minimal polynomial of π_A over $\mathbb{Q}$.

1) f is a power of the minimal polynomial h.

2) The reduced degree $[\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} = [\mathrm{End}^0(A) : \mathbb{Q}[\pi_A]]^{1/2}[\mathbb{Q}[\pi_A] : \mathbb{Q}]$ equals $2g$.

Proof. 1) By Theorem 2.3.5, we know that f equals the characteristic polynomial of $V_l(\pi_A)$ acting on the Tate module, which has $\mathbb{Q}$-coefficients. Thus, $f(\alpha) = 0$ if and only if α is an eigenvalue of $V_l(\pi_A)$, in which case $h(\alpha)$ is an eigenvalue of $h(V_l(\pi_A)) = V_l(h(\pi_A)) = 0$, i.e. $h(\alpha) = 0$. Thus, all roots of f are roots of h, and since h is irreducible, $f = h^n$ for some n.

2) Tate's proof showed that we can calculate the dimension of the endomorphism algebra as

$$[\mathrm{End}^0(A):\mathbb{Q}] = r(f,f) = n^2\deg(h).$$

On the other hand, $\deg(h) = [\mathbb{Q}[\pi_A]:\mathbb{Q}]$, and hence $n = [\mathrm{End}^0(A):\mathbb{Q}[\pi_A]]^{1/2}$. Now comparing degrees in the equation $f = h^n$ gives $2g = [\mathrm{End}^0(A):\mathbb{Q}]_{\mathrm{red}}$. □

By the Weil conjectures, the roots of the characteristic polynomial of the Frobenius endomorphism are the eigenvalues of the q-Frobenius acting on the Tate module, which are Weil numbers. We recall the definition.

Definition 2.4.5. An algebraic number α is a *Weil p^n-number of weight m* if the following two properties hold:

- For all conjugates α' of α, we have $||\alpha'||^2 = p^{nm}$;
- There exists $N \in \mathbb{N}$ such that $p^N\alpha$ is an algebraic integer.

Denote the group of Weil p^n-numbers by $W(p^n)$, and the subset of weight 1 Weil numbers which are algebraic integers by $W_{1,+}(p^n)$.

It follows immediately from the definition and the product formula for norms that for a Weil number π, the only prime $l \neq \infty$ satisfying $||\pi||_l \neq 1$ is $l = p$. Moreover, any Weil number of weight zero is a root of unity.

By Corollary 2.4.1, the isogeny class of an abelian variety over $\mathbb{F}_q$ is determined by the characteristic polynomial of its Frobenius endomorphism, and by Proposition 2.4.4.1, its roots are precisely the roots of the minimal polynomial of π_A. Thus, the Weil numbers associated to an isogeny class of abelian varieties occur as the images of π_A under embeddings $\mathbb{Q}[\pi_A] \hookrightarrow \overline{\mathbb{Q}}$. This leads to a beautiful classification theorem:

Theorem 2.4.6 (Honda-Tate)**.** There is a bijection

$$\left\{\begin{matrix}\text{Isogeny classes of simple}\\ \text{abelian varieties over } \mathbb{F}_{p^n}\end{matrix}\right\} \xleftrightarrow{1:1} \left\{\begin{matrix}\mathrm{Gal}(\mathbb{Q})\text{-orbits in}\\ W_{1,+}(p^n)\end{matrix}\right\}$$

Proof. The map is defined by sending $A \mapsto \{\tau(\pi_A) \mid \tau\colon Z(\mathrm{End}^0(A)) \hookrightarrow \overline{\mathbb{Q}}\}$. Each $\tau(\pi_A)$ is a weight 1 Weil p^n-number by the Weil conjectures, and an algebraic integer because $\mathrm{End}(A) \ni \pi_A$ is a finite $\mathbb{Z}$-algebra. As explained above, the map is injective by Corollary 2.4.1.
It remains to show surjectivity. For this, one needs to construct an abelian variety for any given Weil number in $W_{1,+}(p^n)$. This was proven by Honda in [Hon68] and is beyond the scope of this thesis; a reference is [Oor]. □

We can get a similar classification for abelian varieties over $\overline{\mathbb{F}}_p$. For any such abelian variety, there exists some $q = p^n$ such that A and all its endomorphisms are defined over $\mathbb{F}_q$. We call such $A_0/\mathbb{F}_q$ a *model* for A. However, the eigenvalues of the Frobenius of A_0 depend on the choice of model: for instance, the complex norm of π_{A_0} will be $\sqrt{q}$, so certainly depends on q.

To get rid of this dependency, we construct a modified group of Weil numbers as follows.

Definition 2.4.7. For a prime number p, define $W(p^\infty) := \varinjlim W(p^n)$, where the limit is over the maps $\pi \mapsto \pi^k : W(p^n) \to W(p^{nk})$ for all $n, k \geq 1$.

Thus, an element of $W(p^\infty)$ is given by a class $[(\pi, n)]$ such that $\pi \in W(p^n)$. Note that it no longer makes sense to talk about, say, $p \in W(p^\infty)$, because p can be considered as a Weil p-number of weight 2, but also as a Weil p^2-number of weight 1. However, the elements $[(p, 1)]$ and $[(p, 2)]$ do make sense, and are distinct in $W(p^\infty)$. In fact, one easily checks that $[(\pi_1, n_1)] = [(\pi_2, n_2)]$ if and only if $\pi_1^{n_2}$ and $\pi_2^{n_2}$ differ by a root of unity.

Note that taking the image in $W(p^\infty)$ of a Weil number coming from an abelian variety removes the dependency on the choice of model. Denoting $W_{1,+}(p^\infty) := \varinjlim W_{1,+}(p^n)$, we obtain the following classification theorem:

Theorem 2.4.8. There is a bijection

$$\left\{\begin{matrix}\text{Isogeny classes of simple} \\ \text{abelian varieties over } \overline{\mathbb{F}}_p\end{matrix}\right\} \xleftrightarrow{1:1} \left\{\begin{matrix}\text{Gal}(\mathbb{Q})\text{-orbits in} \\ W_{1,+}(p^\infty)\end{matrix}\right\}$$

Proof. Since the transition maps $W(p^n) \to W(p^{nk})$ are Gal($\mathbb{Q}$)-equivariant, the right-hand side makes sense. The map is given by sending A to the set $\{[\tau(\pi_{A_0}), n] \mid \tau : \mathbb{Q}[\pi_{A_0}] \hookrightarrow \overline{\mathbb{Q}}\}$, where $A_0/\mathbb{F}_{p^n}$ is a model for A. As explained in the preceding paragraph, this is well-defined, and a bijection by Honda-Tate. □

Remark 2.4.9. We even have that the Galois orbit corresponding to A is in bijection with $\text{Hom}(\mathbb{Q}[\pi_A], \overline{\mathbb{Q}})$, i.e. the map

$$\text{Hom}(\mathbb{Q}[\pi_{A_0}], \overline{\mathbb{Q}}) \longrightarrow \Theta, \tag{2.7}$$

where Θ is the Galois orbit of Frobenius eigenvalues of A_0 in $W_{1,+}(p^\infty)$, is bijective. This is obvious if we take the Galois orbit in $W_{1,+}(q)$ with $A_0/\mathbb{F}_q$, but since roots of unity are identified in the colimit, we need to be careful. Recall however that our definition of model requires that $\text{End}(A) \cong \text{End}(A_0)$, and in particular $Z(\text{End}(A)) \cong Z(\text{End}(A_0)) \cong \mathbb{Q}[\pi_{A_0}]$. If now π_{A_0} were conjugate to $\zeta_m \pi_{A_0}$ for some root of unity ζ_m, then $A' := A_0 \times_{\mathbb{F}_q} \text{Spec}(\mathbb{F}_{q^m})$ has Frobenius $\pi_{A'} = \pi_{A_0}^m$. But $\pi_{A'}$ has fewer conjugates than π_{A_0}, hence $\mathbb{Q}[\pi_{A'}] \subsetneq \mathbb{Q}[\pi_{A_0}]$, contradicting the fact that A_0 was a model of A. Hence (2.7) is indeed injective as well as surjective.

Examples 2.4.10.
1. By the theorem, there is a unique isogeny class of simple abelian varieties over $\overline{\mathbb{F}}_p$ whose endomorphism rings have trivial centre (corresponding to the Galois orbit of $[\sqrt{p}]$). One can show that this is the class of a supersingular elliptic curve, i.e. an elliptic curve whose p-adic Tate module is zero.
2. Honda-Tate over $\mathbb{F}_q$, $q = p^n$ tells us we have two cases:

- if n is even, there exist two non-isogenous simple abelian varieties whose Frobenius eigenvalues are $\sqrt{q}$, resp. $-\sqrt{q}$;
- if n is odd, there exists a simple abelian variety whose Frobenius eigenvalues are $\{\pm\sqrt{q}\}$.

In the first case, these are again supersingular elliptic curves which become isogenous after a degree two base extension. However, there will always be one supersingular elliptic curve over $\mathbb{F}_{q^2}$ which can't be defined over a smaller field (the one corresponding to $-q$).
In the second case, one can show that this must be a surface. Since $(\pm\sqrt{q})^2 = q$, a degree two base extension will split this surface into a product of elliptic curves (up to isogeny), both of which lie in the same isogeny class.

Part II

Motives and the Tate conjecture

3. Preliminaries

In this part of the thesis, we will study the series of papers [Mil94], [Mil99a] and [Mil99b]. The main result we will work towards is the following:

Theorem 3.0.1. The Hodge conjecture for CM abelian varieties over $\overline{\mathbb{Q}}$ implies the Tate conjecture for abelian varieties over finite fields.

The proof relies heavily on the machinery of motives, Tannakian categories, and affine group schemes. In this preliminary chapter, we will revise the parts of the theory we need in order to understand the proof.

3.1 Affine groups

By an *affine group*, we will mean an affine k-group scheme G for some field k. Its global sections $\mathcal{O}_G(G)$ form a commutative Hopf algebra, and if it is finitely generated as a k-algebra, we call G an affine algebraic group. Any affine group is the limit of its algebraic quotients, which allows one to reduce to affine algebraic groups in many situations.

3.1.1 Representations

One example of an affine algebraic group is $\mathrm{GL}(V)$ for some n-dimensional k-vector space V. By definition, $\mathrm{GL}(V)$ is the group functor on k-algebras sending

$$R \longmapsto \mathrm{GL}(V \otimes_k R) = \mathrm{Aut}_R(V \otimes_k R),$$

and is represented by the Hopf algebra $k[X_{1,1}, X_{1,2}, \dots, X_{n,n}, T]/(T \cdot \det = 1)$.

A *representation* of G on a vector space V is a natural transformation $G \to \mathrm{GL}(V)$. To give a representation of G on V is the same as to give a co-action of $\mathcal{O}_G(G)$ on V. The category of finite-dimensional representations of G is denoted $\mathsf{Rep}_k(G)$.

Example 3.1.1. A one-dimensional representation is the same as a morphism $G \to \mathbb{G}_m$, i.e. a character of G. Indeed, $\mathbb{G}_m(R) = R^\times \cong \mathrm{GL}(k \otimes_k R)$.

Groups of multiplicative type

Let A be an abelian group (not necessarily finitely generated). One can associate to it a group scheme $D(A)$ via the rule

$$D(A)(R) = \mathrm{Hom}(A, R^\times).$$

The groups above are called *diagonalisable.* The name is justified by the following proposition [Mil15a, Thm. 14.12]:

Proposition 3.1.2. An affine group G is diagonalisable if and only if all its representations are diagonalisable, i.e. all its representations decompose as a direct sum of eigenspaces, where G acts through a character on each eigenspace.

Next, we show that the functor D is fully faithful:

Proposition 3.1.3. The functor $D : \mathsf{Ab} \to \mathsf{AffGrp}_k^{\mathrm{diag}}$ is an equivalence of categories.

Proof. Note that $D(A)$ is represented by the group algebra $k[A]$. Hence, we can reconstruct A from $D(A)$ by taking characters:

$$X(D(A)) = \mathrm{Hom}_k(D(A), \mathbb{G}_m) \cong \mathrm{Hom}_{\mathsf{Hopf}_k}(k[T^{\pm 1}], k[A]) \cong A,$$

where the last isomorphism follows because the image of T must be a group-like element of $k[A]$. One can check that taking characters gives a quasi-inverse to D. □

We will now extend this equivalence by considering abelian groups as $\mathrm{Gal}(k)$-modules with trivial action.

Definition 3.1.4. For any affine group G, we define its *geometric characters* to be $X^*(G) := \mathrm{Hom}(G_{k^{\mathrm{sep}}}, \mathbb{G}_{m,k^{\mathrm{sep}}})$. It is a $\mathrm{Gal}(k)$-module with action $\sigma \cdot f = \sigma f \sigma^{-1}$.
An affine group G is *of multiplicative type* if $G_{k^{\mathrm{sep}}}$ is diagonalisable.

Proposition 3.1.3 in combination with Galois descent gives us:

Proposition 3.1.5. There is an equivalence of categories

$$X^* \colon \left\{ \begin{matrix} \text{Affine groups of} \\ \text{multiplicative type over } k \end{matrix} \right\} \xrightarrow{\sim} \left\{ \begin{matrix} \text{Abelian groups with} \\ \text{continuous } \mathrm{Gal}(k)\text{-action} \end{matrix} \right\}$$

given by sending a multiplicative type group to its geometric characters.

Explicitly, if G is a group of multiplicative type and if $K \subset k^{\mathrm{sep}}$, we have

$$G(K) = \mathrm{Hom}(X^*(G), k^{\mathrm{sep},\times})^{\mathrm{Gal}(K)}.$$

The above proposition is important because once we know we are working with multiplicative groups, we can reduce to working with their characters.

Examples 3.1.6.
1. The diagonalisable group associated to $\mathbb{Z}^n$ is $\mathbb{G}_m^n$, since $\mathbb{G}_m^n(R) = (R^\times)^n \cong \mathrm{Hom}(k[\mathbb{Z}^n], R^\times)$. In particular, the multiplicative group is a group of multiplicative type.
2. Let K/k be a finite separable extension, and consider $\mathbb{Z}^{\mathrm{Gal}(K/k)}$ with Galois action defined by permuting the factors. Then the corresponding multiplicative group is $(\mathbb{G}_m)_{K/k}$, the restriction of scalars of $\mathbb{G}_{m,K}$ to k. This is the group whose points are

$$(\mathbb{G}_m)_{K/k}(R) = \mathbb{G}_{m,K}(R \otimes_k K).$$

By Proposition 3.1.2, a group is of multiplicative type if and only if it is reductive (i.e. any representation is semisimple) and over an algebraic closure, every simple representation has rank one. If $\mathrm{char}(k) = 0$, equivalently G is commutative and reductive [Mil15a, Thm. 14.24, 17.17].

3.1.2 Tannakian categories

A Tannakian category is a category which is equivalent to the category of representations of some affine group scheme. It can be defined intrinsically as follows.

Definition 3.1.7. A k-linear rigid symmetric monoidal category $(\mathcal{T}, \otimes)$ with $\mathrm{End}(\mathbb{1}) = k$ is called *Tannakian* if it admits a fibre functor, i.e. an exact k-linear tensor functor $\omega \colon \mathcal{C} \to R\text{-}\mathsf{Mod}$ for some k-algebra $R \neq 0$. If we can take $R = k$, we say $\mathcal{C}$ is *neutral*.

The terminology means that $\mathcal{T}$ is:

- k-linear: abelian and $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ is a k-vector space for all X, Y;
- monoidal: there exists a k-bilinear tensor product $\otimes\colon \mathcal{C}\times\mathcal{C}\to\mathcal{C}$ with unit object $\mathbb{1}$, satisfying associativity and commutativity constraints;
- symmetric: the natural morphisms $c_{X,Y} : X\otimes Y \xrightarrow{\sim} Y\otimes X$ obey $c_{X,Y}^{-1} = c_{Y,X}$;
- rigid: any object X admits a dual $X^\vee = \underline{\mathrm{Hom}}(X,\mathbb{1})$, where $\underline{\mathrm{Hom}}(X,-)$ is the right adjoint to the functor $-\otimes X$.

For more details on the terminology, see [Del90, §2] or [DM18, §1].

When the base field has characteristic zero, one can obtain a fibre functor once one extends scalars to an algebraic closure [Del]:

Theorem 3.1.8 (Deligne)**.** Let $\mathcal{T}$ be a Tannakian category over an algebraically closed field. Then $\mathcal{T}$ is neutral.

The following theorem characterizes Tannakian categories.

Theorem 3.1.9. Let $\mathcal{T}$ be a neutral Tannakian category over k with fibre functor ω. Then $\mathcal{T}$ is equivalent to the category $\mathsf{Rep}_k(G)$, where $G =: \pi_1(\mathcal{T})$ is an affine group. In fact, we have an isomorphism $G \cong \underline{\mathrm{Aut}}^{\otimes}(\omega)$, where

$$\underline{\mathrm{Aut}}^{\otimes}(\omega) = \{\Phi\colon \omega \xrightarrow{\sim} \omega \mid \Phi_{V\otimes W} = \Phi_V \otimes \Phi_W \text{ and } \Phi_{\mathbb{1}} = \mathrm{id}_k\},$$

which we can consider as a functor $\mathsf{Alg}_k \to \mathsf{Grp}$ sending $R \mapsto \underline{\mathrm{Aut}}^{\otimes}(\omega_R)$, where

$$\omega_R : \mathcal{C} \xrightarrow{\omega} \mathsf{Vec}_k \xrightarrow{-\otimes R} \mathsf{Mod}_R.$$

Note that ω induces a monoidal functor $\mathcal{C} \to \mathrm{Rep}_k(\underline{\mathrm{Aut}}^{\otimes}(\omega))$; the theorem is proven by showing that this functor is an equivalence. This leads to duality statements between $\mathcal{T}$ and $\pi_1(\mathcal{T})$: for instance, if $\mathrm{char}(k) = 0$, $\mathcal{T}$ is semisimple if and only if $\pi_1(\mathcal{T})$ is reductive.

Taking the fundamental group of a Tannakian category is functorial in some sense. To make this precise, we define the category of Tannakian categories as follows.

Definition 3.1.10. Let k be a field. Denote by Tann_k the category whose objects are neutral Tannakian categories $(\mathcal{T},\omega)$ over k, and whose morphisms $(\mathcal{T},\omega) \to (\mathcal{T}',\omega')$ are those exact k-linear tensor functors $\mathcal{T}\to\mathcal{T}'$ for which the diagram

$$\begin{tikzcd}
\mathcal{T} \arrow[rr] \arrow[dr, "\omega"'] & & \mathcal{T}' \arrow[dl, "\omega'"] \\
& \mathsf{Vec}_k &
\end{tikzcd}$$

commutes.

Proposition 3.1.11. The fundamental group π_1 defines a contravariant functor $\mathsf{Tann}_k \to \mathsf{AffGrp}_k$. Moreover, given a morphism $F : (\mathcal{T},\omega) \to (\mathcal{T}',\omega')$, the induced map $\pi_1(\mathcal{T}') \to \pi_1(\mathcal{T})$ is injective if every object of $\mathcal{T}'$ appears as a subquotient of direct sums of tensor products of objects of the form $F(X)$ with $X \in \mathcal{T}$.

Proof. Let $F : \mathcal{T} \to \mathcal{T}'$ be an exact k-linear tensor functor commuting with the fibre functors. Then for any $\Phi \in \underline{\mathrm{Aut}}^{\otimes}(\omega')(R)$ and any $X \in \mathcal{T}$, define $\pi_1(F)(\Phi)_X := \Phi_{F(X)}$. This is an element of $\underline{\mathrm{Aut}}^{\otimes}(\omega)(R)$ by the conditions on F, and since $(\Phi \circ \Psi)_{F(X)} = \Phi_{F(X)} \circ \Psi_{F(X)}$, $\pi_1(F)$ is a group homomorphism. It is clear that $\pi_1(\mathrm{id}_{\mathcal{T}}) = \mathrm{id}_{\pi_1(\mathcal{T})}$ and that $\pi_1(F \circ G) = \pi_1(G) \circ \pi_1(F)$. Hence π_1 defines a functor.
Next, it is clear from the definition that any $\Phi \in \underline{\mathrm{Aut}}^{\otimes}(\omega)$ is determined by its action on a tensor generating family of $\mathcal{T}$, which is the condition spelled out in the statement of the proposition. So if the essential image of F contains a tensor generating family, $\pi_1(F)$ is injective. □

Theorem 7.1 of [Del90] provides a useful way to determine whether a tensor category over a field over characteristic zero admits a fibre functor. To state it, we need to generalise the notion of traces and exterior powers to Tannakian categories:

Definition 3.1.12. Let $c_{X,Y} : X \otimes Y \xrightarrow{\sim} Y \otimes X$ denote the commutativity constraint. For any morphism $f : X \to Y$, define

$$\delta(f) : \mathbb{1} \xrightarrow{\mathrm{coev}_X} X \otimes X^{\vee} \xrightarrow{c_{X,X^{\vee}}} X^{\vee} \otimes X \xrightarrow{\mathrm{id}_{X^{\vee}} \otimes f} X^{\vee} \otimes Y.$$

If $X = Y$, we define the *trace* of f to be $\mathrm{Tr}(f) = \mathrm{ev}_X \circ \delta(f) \in \mathrm{End}(\mathbb{1}) = k$.
Define the *rank* of X to be $\mathrm{rk}(X) = \mathrm{Tr}(\mathrm{id}_X)$.
The n^{th} *exterior power* of X, denoted $\bigwedge^n X$, is the image of the antisymmetrization map

$$a_n^X = \sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}(\sigma)} \sigma \colon X^{\otimes n} \longrightarrow X^{\otimes n}.$$

Note that if F is a k-linear tensor functor, we have $\mathrm{rk}(X) = \mathrm{rk}(F(X))$ and $F(\bigwedge^n X) = \bigwedge^n F(X)$.

Theorem 3.1.13 (Deligne)**.** Suppose $\mathrm{char}(k) = 0$. Let $(\mathcal{C}, \otimes)$ be a k-linear rigid symmetric monoidal category with $\mathrm{End}(\mathbb{1}) = k$. Then the following are equivalent:

1) $\mathcal{C}$ is Tannakian;

2) For any $X \in \mathcal{C}$, we have $\mathrm{rk}(X) \in \mathbb{N}_0$;

3) For any $X \in \mathcal{C}$, there exists some $n \geq 0$ such that $\bigwedge^n X = 0$.

Remark 3.1.14. Note that the rank one objects in any Tannakian category $\mathcal{T}$ form a group under the tensor product, isomorphic to $X(\pi_1(\mathcal{T}))$. Indeed, under the equivalence $\omega : \mathcal{T} \to \mathsf{Rep}_k(\pi_1(\mathcal{T}))$, the rank one objects correspond to the one-dimensional representations, which can be identified with the characters of $\pi_1(\mathcal{T})$ by Example 3.1.1.
This gives a categorical description of the characters of an affine group.

As a final application of the above definitions, we can generalise the notion of characteristic polynomial of an endomorphism to Tannakian categories.

Definition 3.1.15. Let $(\mathcal{T}, \otimes)$ be Tannakian with $\mathrm{End}(\mathbb{1}) = k$. Let $X \in \mathcal{C}$ and $\varphi \in \mathrm{End}(X)$ and suppose $\mathrm{rk}(X) = d \in \mathbb{N}$. The *characteristic polynomial* of φ is defined to be

$$f_{\varphi}(t) := \sum_{i=0}^{d} \mathrm{Tr}\left(\varphi^{d-i} \colon \bigwedge^{d-i} X \to \bigwedge^{d-i} X\right) t^i.$$

This is a monic polynomial of degree d with coefficients in k.

Remark 3.1.16. We can define the characteristic polynomial of an endomorphism in any Karoubian rigid symmetric monoidal category with $\mathrm{End}(\mathbb{1}) = k$ and $\mathrm{char}(k) = 0$. Indeed, we only need to have traces and exterior powers, and if $\mathrm{char}(k) = 0$, we have that the fractional multiple $a_n^X/n!$ of the antisymmetrization map is an idempotent. Thus if $\mathcal{T}$ is Karoubian, the image of this map is a well-defined object.

Note that for any k-linear tensor functor F, we have $f_\varphi(t) = f_{F(\varphi)}(t)$, by naturality of the constructions. Moreover, if $\mathcal{C}$ is the category of k-vector spaces, the above definition simplifies to the usual characteristic polynomial.

Remark 3.1.17. If $\mathcal{T}$ is a Tannakian category over k and R is a k-algebra, there is a natural way to obtain an R-linear category $\mathcal{T} \otimes R$ such that $\pi_1(\mathcal{T} \otimes R) \cong \pi_1(\mathcal{T}) \otimes R$. It comes with a k-linear functor $\mathcal{T} \to \mathcal{T} \otimes R$, and for all $X, Y \in \mathcal{T}$,

$$\mathrm{Hom}(X \otimes R, Y \otimes R) \cong R \otimes \mathrm{Hom}(X, Y).$$

For details on this construction, see [Sta08]. As an application, we see that the fundamental group of $\mathcal{T}$ is of multiplicative type if and only if $\pi_1(\mathcal{T} \otimes \overline{k})$ is diagonalisable, if and only if (by Proposition 3.1.2) $\mathcal{T} \otimes \overline{k}$ is a semisimple category all of whose simple objects are of rank 1, and if $\mathrm{char}(k) = 0$, if and only if $\mathcal{T}$ is semisimple and $\pi_1(\mathcal{T})$ is commutative.

3.2 CM abelian varieties

3.2.1 Complex multiplication

We have already seen that the structure of the endomorphism algebra of abelian varieties over finite fields is well understood. For abelian varieties over general fields, one thing we can do is bound the dimension. We start with some general facts on representations of semisimple (possibly non-commutative) algebras over a field K of characteristic 0, of which endomorphism algebras are examples. Recall that by Wedderburn's theorem, any such algebra is isomorphic to a product of matrix algebras over division K-algebras. For more background on the theory, see [GS06, Chapter 2].

Definition 3.2.1. Let E be a finite-dimensional semisimple K-algebra, and write $E \cong \prod_{i=1}^n E_i$ as a product of simples. The *reduced degree* of E is defined as

$$[E : K]_{\mathrm{red}} = \sum_{i=1}^{n} [E_i : Z(E_i)]^{\frac{1}{2}} [Z(E_i) : Z].$$

The definition makes sense because any central simple algebra $E_i/Z(E_i)$ has a splitting field $F/Z(E_i)$, so that $E_i \otimes_{Z(E_i)} F$ becomes a matrix algebra over F. In particular, the dimension of E_i over $Z(E_i)$ is a square.

Lemma 3.2.2. Let M be a faithful representation of a semisimple K-algebra E. Then

$$[E : K]_{\mathrm{red}} \leq \dim M,$$

and equality holds if and only if the simple factors of E are matrix algebras over fields (rather than general division algebras).

Proof. This follows from the classification of representations of simple K-algebras: if $E \cong M_{n\times n}(D)$ is simple, then any simple representation of E is isomorphic to D^n. Hence $M \cong (D^n)^{\oplus m}$, so

$$\dim_K M = mn[D : Z(D)][Z(D) : k] \geq n[D : Z(D)]^{\frac{1}{2}}[Z(D) : k] = [E : K]_{\mathrm{red}},$$

with equality if and only if $m = 1$ and $D = Z(D)$. If E is a product of simples, M is a faithful representation only if M contains at least one simple representation for each of its factors, and the result follows from a similar computation. □

Corollary 3.2.3. Let A be an abelian variety. Then the reduced degree satisfies

$$[\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} \leq 2g.$$

Proof. If $l \neq \mathrm{char}(k)$, l-adic étale cohomology is a Weil cohomology theory, and $H^1_l(A)$ has dimension $2g$ (which follows from Corollary 1.5.8, and in a different way from the motive of an abelian variety, cf. Theorem 3.3.9). This is a faithful representation of $\mathbb{Q}_l \otimes \mathrm{End}^0(A)$, so by Lemma 3.2.2,

$$[\mathbb{Q}_l \otimes \mathrm{End}^0(A) : \mathbb{Q}_l]_{\mathrm{red}} = [\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} \leq 2g.$$

□

CM abelian varieties are those abelian varieties for which equality holds.

Definition 3.2.4. A g-dimensional abelian variety A/k is *of CM type* or a *CM abelian variety* if $[\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} = 2g$.

Note that an abelian variety is CM if and only if each of its isogeny factors is CM. We have already seen examples of CM abelian varieties:

Proposition 3.2.5. Any abelian variety over a finite field is of CM type.

Proof. This is Proposition 2.4.4.2. □

Recall that a *CM field* is a field $K/\mathbb{Q}$ which is an imaginary quadratic extension of a totally real subfield.

Proposition 3.2.6. A simple abelian variety is of CM type if and only if there exists an embedding $K \hookrightarrow \mathrm{End}^0(A)$, where K is a degree $2g$ number field.

Proof. This follows from the following general fact on division algebras: if E is a division K-algebra with $[E : Z(E)] = d^2$, then any maximal subfield of E has degree d over $Z(E)$.
Hence, if A is CM, such a subfield has degree $2g$ over $\mathbb{Q}$. Conversely, if $\mathrm{End}^0(A)$ contains a degree $2g$ subfield L, we may assume without loss of generality that it contains the centre (if not, we take the compositum). Hence the above fact implies

$$\begin{aligned}[\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} &= [\mathrm{End}^0(A) : Z(\mathrm{End}^0(A))]^{1/2}[Z(\mathrm{End}^0(A)) : \mathbb{Q}] \\ &\geq [L : Z(\mathrm{End}^0(A))][Z(\mathrm{End}^0(A)) : \mathbb{Q}] = 2g.\end{aligned}$$

Since the reverse inequality holds in general, A is of CM type. □

We will be interested in CM abelian varieties defined over $\overline{\mathbb{Q}}$. When we base change to $\mathbb{C}$, we get access to many powerful tools: for example, $A_{\mathbb{C}}$ is a quotient of $\mathbb{C}^g$ by a lattice Λ, which can be intrinsically described as $\Lambda \cong H_1(A(\mathbb{C}), \mathbb{Z})$. The induced representation of $\mathrm{End}^0(A)$ on the $2g$-dimensional vector space $H_1(A(\mathbb{C}), \mathbb{Q})$ is faithful. It is also called the Hodge structure associated to A; we have

$$H_1(A(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{C} \cong T_0(A) \oplus \overline{T_0(A)}, \tag{3.1}$$

where in fact this is an isomorphism of *representations*, with $T_0(A) \cong \mathbb{C}^g$ being the tangent space at 0, so that $A \cong T_0(A)/\Lambda$ [SD74, Lem. 39].

Corollary 3.2.7. If $A/\overline{\mathbb{Q}}$ is a simple g-dimensional CM abelian variety, then $\mathrm{End}^0(A)$ is a CM field of degree $2g$.

Proof. We have a faithful representation of $\mathrm{End}^0(A)$ on $H_1(A(\mathbb{C}), \mathbb{Q})$, so by Lemma 3.2.2, $\mathrm{End}^0(A)$ is a matrix algebra over its centre. Since A is simple, $\mathrm{End}^0(A)$ is a division algebra, so $\mathrm{End}^0(A)$ is a field. By Proposition 3.2.6, it has degree $2g$. Moreover, the Rosati involution defines a positive involution on the field, so either it is a CM field or it is totally real. But the totally real case is impossible: one can show that if $L \subset \mathrm{End}^0(A)$ is a totally real subfield, then $[L : \mathbb{Q}] \leq \dim(A)$ [Mil20, Lem. 3.7]. □

Remark 3.2.8. There exist simple CM abelian varieties in positive characteristic whose endomorphism algebras are not fields. The argument above fails, because in characteristic p, we only have a $2g$-dimensional faithful representation of $\mathbb{Q}_l \otimes \mathrm{End}^0(A)$ for $l \neq \mathrm{char}(k)$. In fact, the existence of CM abelian varieties over k whose endomorphism algebra is not a field shows that there cannot exist a Weil cohomology theory with $\mathbb{Q}$-coefficients for varieties over k, since otherwise we could argue as in the above corollary.
However, the l-adic representation does give (by Lemma 3.2.2) that the endomorphism algebra is split over l for all $l \neq \mathrm{char}(k)$, so the possible endomorphism algebras are still quite restricted.

CM abelian varieties over $\overline{\mathbb{Q}}$ can be classified based on their CM-types. Let us define what we mean by this.

Definition 3.2.9. Let E be a CM field of degree $2g$. A *CM-type* on E is a function

$$\varphi\colon \mathrm{Hom}(E, \overline{\mathbb{Q}}) \longrightarrow \{0, 1\} \hookrightarrow \mathbb{Z}$$

such that for any $\tau : E \to \overline{\mathbb{Q}}$, we have $\varphi(\tau) + \varphi(\iota\tau) = 1$. A CM type is *primitive* if it is not of the form $\tau \mapsto \varphi_0(\tau|_{E_0})$ for some CM-type φ_0 on a CM subfield $E_0 \subsetneq E$.
We say two CM-types (E, φ) and (E', φ') are isomorphic if there exists an isomorphism of fields $\sigma : E \xrightarrow{\sim} E'$ such that $\varphi' = \sigma^*\varphi$.

Conceptually, one may think of a CM-type as a partition of the set of embeddings $E \hookrightarrow \overline{\mathbb{Q}}$: namely, if we let $\Phi = \{\tau\colon E \hookrightarrow \overline{\mathbb{Q}} \mid \varphi(\tau) = 1\}$, we have $\mathrm{Hom}(E, \overline{\mathbb{Q}}) = \Phi \sqcup \iota\Phi$. Note that $\mathrm{Gal}(\mathbb{Q})$ acts on the set of CM-types via $(\sigma\varphi)(\tau) = \varphi(\sigma^{-1}\tau)$.

We will now associate a CM-type to any simple abelian variety over $\overline{\mathbb{Q}}$.

If A is of CM type with endomorphism algebra E, the action of E on $T_0(A)$ decomposes $T_0(A)$ into a sum of 1-dimensional eigenspaces. Hence for some multiset Φ, we have

$$T_0(A) \cong \bigoplus_{\tau \in \Phi} \mathbb{C}_\tau,$$

where E acts on $\mathbb{C}_\tau$ via $\tau \in \mathrm{Hom}(E, \mathbb{C})$. Equation (3.1) now says that

$$T_0(A) \oplus \overline{T_0(A)} \cong H_1(A(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{C} \cong E \otimes \mathbb{C} \cong \bigoplus_{\tau : E \hookrightarrow \mathbb{C}} \mathbb{C}_\tau,$$

and hence Φ must contain g distinct elements and in fact be a primitive CM-type on E.

The following theorem states that this CM-type already classifies the abelian variety up to isogeny.

Theorem 3.2.10. Associating an abelian variety to its CM-type as above gives a bijection

$$\left\{\begin{matrix}\text{Isogeny classes of simple} \\ \text{CM abelian varieties over } \overline{\mathbb{Q}}\end{matrix}\right\} \xleftrightarrow{1:1} \left\{\begin{matrix}\text{Isomorphism classes of} \\ \text{primitive CM-types } (E, \varphi)\end{matrix}\right\}$$

Proof. We construct an inverse. Let (E, φ) be a primitive CM-type, and let

$$\Phi = \{\tau \in \mathrm{Hom}(E, \overline{\mathbb{Q}}) \mid \varphi(\tau) = 1\}.$$

There exists a complex abelian variety A_φ whose $\mathbb{C}$-points are $\mathbb{C}^\Phi / \mathcal{O}_E$, where $\mathcal{O}_E$ is embedded into $\mathbb{C}^g$ via $a \mapsto (\tau(a))_{\tau \in \Phi}$. By construction, its associated CM-type is φ, which will also be the case for any specialisation of A_φ to $\overline{\mathbb{Q}}$. This specialisation exists because up to isogeny, any CM abelian variety over a field of characteristic zero can be defined over a number field [ST61, Prop. 26, p. 109]. □

We will modify this theorem slightly to better suit our purposes. We first define the reflex field of a CM-type.

Definition 3.2.11. Let φ be a CM-type on E. Its *reflex field* K is the fixed field of the stabiliser of φ in $\mathrm{Gal}(\mathbb{Q})$ (so if E is Galois, we have $K \subseteq E$). The reflex field of a simple CM abelian variety over $\overline{\mathbb{Q}}$ is the reflex field of its associated CM-type.

Theorem 3.2.12. Let K be a Galois CM number field. There is a natural bijection

$$\left\{\begin{matrix}\text{Isogeny classes of CM abelian varieties over } \overline{\mathbb{Q}} \\ \text{with reflex field contained in } K\end{matrix}\right\} \xleftrightarrow{1:1} \left\{\begin{matrix}\mathrm{Gal}(\mathbb{Q})\text{-orbits} \\ \text{of CM-types on } K\end{matrix}\right\}$$

Proof. After Theorem 3.2.10, all we need to see is that the isomorphism classes of CM-types on K are in bijection with $\mathrm{Gal}(\mathbb{Q})$-orbits of CM-types on K. This is just a reformulation of what it means for CM-types to be isomorphic: if $\sigma : (K, \varphi) \xrightarrow{\sim} (K, \varphi')$, then $\varphi' = \tilde{\sigma}^{-1} \cdot \varphi$ for any $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{Q})$ lifting σ. Conversely, if $\varphi = \sigma \cdot \varphi'$, then $\sigma^{-1}|_K$ induces an isomorphism $(K, \varphi') \to (K, \varphi)$. □

3.2.2 Reduction of CM abelian varieties

Besides the classification of isogeny classes, abelian varieties have another excellent property: they have potential good reduction. This result is due to Serre and Tate [ST68]. We will not go into the proof, but we will at least explain what the statement means.

Let K be a field, and denote by v a discrete valuation on K. Denote its valuation ring by $\mathcal{O}_v$ and its residue field by k.

Definition 3.2.13. Let X be a proper smooth K-scheme. We say X *has good reduction at* v if there exists a proper smooth $\mathcal{O}_v$-scheme X' whose generic fibre $X' \times_{\mathcal{O}_v} \operatorname{Spec}(K)$ is isomorphic to X. We say X has *potential good reduction at* v if X_L has good reduction at all valuations dividing v for some finite extension L/K.
In both cases, the *reduction* of X at v is the special fibre $X_k := X' \times_{\mathcal{O}_v} \operatorname{Spec}(k)$ of X'.

It is not immediately obvious that the construction is functorial, i.e. that a K-morphism $X \to Y$ induces a k-morphism $X_k \to Y_k$. This is true, however; it follows from the Néron mapping property, and the fact that X' is indeed a Néron model of X, if it exists. In particular, using this, one can show that an abelian variety (X, m, i, e) over K gives rise to an abelian variety (X_k, m_k, i_k, e_k). The interested reader is referred to [BLR90, Chapter 1], where Néron models are defined and the above claims are proved.

We apply this to the case where X is an abelian variety, K is a number field, and v is the p-adic valuation for a prime number p.

Example 3.2.14. Let $E/\mathbb{Q}$ be an elliptic curve. Write down a Weierstrass equation for it, and consider its discriminant Δ. Then E has good reduction at a prime p if and only if $\Delta \not\equiv 0 \mod p$. Hence, E has good reduction at every prime over $\mathbb{Q}$ if and only if $\Delta = \pm 1$. But it turns out that this diophantine problem has no solutions over $\mathbb{Q}$, so there are no elliptic curves with good reduction everywhere.

In contrast to the above example, we have the following remarkable theorem:

Theorem 3.2.15 (Serre-Tate)**.** Let A be an abelian variety of CM type over a number field. Then A has potential good reduction everywhere.

3.3 Motives

3.3.1 Motivation

Around the 1960's, Grothendieck envisioned a theory of motives which would lead to a proof of the Weil conjectures. Philosophically, motives capture the cohomological essence of a projective variety. Let k be a base field. Denote by $\mathcal{V}_k$ the category of smooth projective k-varieties and by $\mathsf{Mot}(k)$ the (yet undefined) category of motives over k. The main property of the category of motives is that for every Weil cohomology theory $H^\bullet : \mathcal{V}_k \to \mathsf{Vec}_{\mathbb{K}}$, there should exist a diagram

$$\begin{tikzcd}
\mathcal{V}_k \arrow[rr, "H^\bullet"] \arrow[dr] & & \mathsf{Vec}_{\mathbb{K}} \\
& \mathsf{Mot}(k) \arrow[ur, dotted] &
\end{tikzcd}$$

Thus, motives are something in between varieties and vector spaces. This is in many ways true, as we will see: motives are defined as (twists of pieces of) varieties, but behave in many ways like vector spaces do.

The category of motives should explain some phenomena that arise in cohomology. For instance, there are several different notions of cohomology in algebraic geometry, say singular and de Rham cohomology in the complex setting. The fact that these cohomology theories agree on smooth projective varieties is explained by the fact that the cohomological structure is already determined on a motivic level.

Problematically, though, the category of motives is not known to exist in general. A satisfying candidate would satisfy several good properties: for instance, it should be a semisimple Tannakian category, and Weil cohomology theories should factor through it as above. So far, nobody has been able to construct such a category for general base fields. However, if the base field is finite and the motives come from abelian varieties, we can construct a category satisfying the requirements. In the next sections, we will construct this category and use it to study the Tate conjecture.

3.3.2 Construction of the category of motives

The main idea in the construction of the category of motives is to replace morphisms of varieties by algebraic cycles, which in this context are called correspondences.

Definition 3.3.1. Let X/k be a noetherian scheme whose irreducible components are projective varieties. Let $\mathscr{Z}^r(X)$ denote the free abelian group on codimension r closed integral subvarieties of X, and we write for any field $\mathbb{K}$ of characteristic zero,

$$\mathscr{Z}^r(X)_{\mathbb{K}} := \mathscr{Z}^r(X) \otimes_{\mathbb{Z}} \mathbb{K}, \qquad \mathscr{Z}^{\bullet}(X)_{\mathbb{K}} := \bigoplus_{r=0}^{\dim X} \mathscr{Z}^r(X)_{\mathbb{K}}.$$

If $\mathbb{K} = \mathbb{Q}$, we usually drop it from the notation.
An *adequate equivalence relation on cycles* is an equivalence relation $\sim$ on $\mathscr{Z}^{\bullet}(X)_{\mathbb{K}}$ for each X, satisfying the following properties:

1. $\sim$ is compatible with the $\mathbb{K}$-linear structure and respects the grading on $\mathscr{Z}^{\bullet}(X)_{\mathbb{K}}$;
2. For each $\alpha, \beta \in \mathscr{Z}^{\bullet}(X)_{\mathbb{K}}$, there exists $\beta' \sim \beta$ such that β' intersects α properly;
3. If $\alpha \sim 0$ in $\mathscr{Z}^{\bullet}(X)_{\mathbb{K}}$ and $\beta \in \mathscr{Z}^{\bullet}(X \times Y)_{\mathbb{K}}$ intersects $p_X^*\alpha$ properly, then $p_{Y,*}(p_X^*\alpha \cap \beta) \sim 0$ in $\mathscr{Z}^{\bullet}(Y)_{\mathbb{K}}$.

Given an adequate equivalence relation $\sim$, we denote by $\mathrm{CH}^{\bullet}_{\sim}(X)_{\mathbb{K}}$ the graded $\mathbb{K}$-vector space $\mathscr{Z}^{\bullet}_{\mathbb{K}}(X)/\sim$.

Note that condition 2 implies that the intersection product is well-defined on $\mathrm{CH}^{\bullet}_{\sim}(X)_{\mathbb{K}}$, turning it into a $\mathbb{K}$-algebra.

Examples 3.3.2.
1. Rational equivalence is an adequate equivalence relation on cycles, and in this case $\mathrm{CH}^{\bullet}_{\sim}(X)$ is the usual Chow ring. It is the finest possible adequate equivalence relation [And04, Lem. 3.2.2.1], so for any adequate equivalence relation $\sim$, the algebra $\mathrm{CH}^{\bullet}_{\sim}(X)$ is a quotient of the Chow ring.
2. Fix a Weil cohomology theory $H^{\bullet}$ with coefficient field $\mathbb{K}$. Then *homological equivalence* is the adequate equivalence relation $\sim_{\mathrm{hom}}$ defined by $\alpha \sim_{\mathrm{hom}} \beta \iff \mathrm{cl}(\alpha) = \mathrm{cl}(\beta)$, where $\mathrm{cl} : \mathscr{Z}^r(X)_{\mathbb{K}} \to H^{2r}(X)$ denotes the cycle class map.
3. Define *numerical equivalence*, denoted $\sim_{\mathrm{num}}$, as follows: for $\alpha, \beta \in \mathscr{Z}^r(X)_{\mathbb{K}}$, say $\alpha \sim_{\mathrm{num}} \beta$ if and only if for all $\gamma \in \mathscr{Z}^{\dim X - r}(X)_{\mathbb{K}}$, we have

$$\int \alpha \cap \gamma = \int \beta \cap \gamma.$$

Numerical equivalence is the coarsest possible adequate equivalence relation. To see this, let $\sim$ be any other one; then we want to show that if $\mathscr{Z}^r(X)_{\mathbb{K}} \ni \alpha \sim 0$ and $\beta \in \mathrm{CH}^{\dim X - r}_{\sim}(X)_{\mathbb{K}}$, we have $\int \alpha \cap \beta = 0$.
By property 2, we may assume β intersects α properly. Then applying property 3 with $Y = \mathrm{Spec}(k)$ gives the desired result.

The Theorem of the Base says that for a proper smooth variety X, the algebra $\mathrm{CH}^1_{\sim}(X)$ is finitely generated when $\sim$ is at least as coarse as algebraic equivalence. If $\sim$ is at least as coarse as homological equivalence, $\mathrm{CH}^{\bullet}_{\sim}(X)$ is finitely generated because its dimension is bounded by $H^{\bullet}(X)$. In general, no precise statement is known about when these groups are finitely generated. One cannot expect this to hold in general: for example, if $\sim$ is rational equivalence, consider the Chow group of an elliptic curve $E/\mathbb{C}$. Then $\mathrm{CH}^{\bullet}_{\sim}(E) \cong \mathbb{Q} \oplus \mathrm{Pic}(E)(\mathbb{C})$, which is not finitely generated as the uncountable group $E(\mathbb{C})$ injects into it via the Abel-Jacobi map.

Fix an adequate equivalence relation on cycles. Define a category $\mathcal{M}^0_{\sim}(k)$ whose objects are smooth projective k-varieties, and whose morphisms are given by

$$\mathrm{Hom}_{\mathcal{M}^0_{\sim}(k)}(X,Y) := \mathrm{Corr}^0_{\sim}(X,Y) := \mathrm{CH}^{\dim X}_{\sim}(X \times Y),$$

which we call *degree zero correspondences from X to Y*. The composition law is given as follows: for $\alpha\colon X \to Y$, $\beta\colon Y \to Z$, we have

$$\beta \circ \alpha := p_{XZ,*}(p^*_{XY}\alpha \cap p^*_{YZ}\beta) \in \mathrm{CH}^{\dim X}_{\sim}(X \times Z),$$

where the maps are all projections to the indicated two factors of $X \times Y \times Z$. For example, the identity morphism on X is the diagonal Δ_X. The category $\mathcal{M}^0_{\sim}(k)$ is also easily seen to admit biproducts, with $X \oplus Y \cong X \sqcup Y$. Note that $\mathcal{M}^0_{\sim}(k)$ is $\mathbb{Q}$-linear by definition, and tensoring the Hom-spaces by $\mathbb{K}$ gives a $\mathbb{K}$-linear category $\mathcal{M}^0_{\sim}(k) \otimes \mathbb{K}$ for any characteristic zero field $\mathbb{K}$.

Remark 3.3.3. This construction gives a *contravariant* functor $h\colon \mathcal{V}_k \to \mathcal{M}^0_{\sim}(k)$, sending a morphism $\varphi\colon X \to Y$ to the graph $\Gamma_\varphi \in \mathrm{CH}^{\dim Y}_{\sim}(Y \times X)$. This is a choice, and the reason for it is that one usually studies the category of motives (which we still haven't defined yet) through its realisation functors, such as the functors $\mathsf{Mot}_{\sim}(k) \to \mathsf{Vec}_{\mathbb{K}}$ coming from Weil cohomology theories. With the above convention, these functors will be covariant.

We will keep the notation $hX = h(X)$ for the motive coming from the variety $X \in \mathcal{V}_k$, regardless of what (intermediate) category of motives the target category is; it should in all situations be clear from the context.

We will perform a few more steps before arriving at the category of motives. The first is to take the Karoubi envelope of $\mathcal{M}^0_{\sim}(k)$.

Definition 3.3.4. Let $\mathcal{C}$ be a pre-additive category. The *Karoubi envelope* of $\mathcal{C}$ is the category $\mathrm{Kar}(\mathcal{C})$ whose objects are pairs (X,p) where $X \in \mathrm{Ob}(\mathcal{C})$ and $p \in \mathrm{End}_{\mathcal{C}}(X)$ is a projection, i.e. $p \circ p = p$. The morphisms are given by

$$\mathrm{Hom}_{\mathrm{Kar}(\mathcal{C})}((X,p),(Y,q)) = q \circ \mathrm{Hom}_{\mathcal{C}}(X,Y) \circ p.$$

Note that $\mathcal{C}$ embeds fully faithfully into $\mathrm{Kar}(\mathcal{C})$ by sending $X \mapsto (X, \mathrm{id}_X)$.

Taking the Karoubi envelope is a way of formally adding images and kernels of projections, and one should think of (X,p) as the image of p. The following lemma justifies this:

Lemma 3.3.5. Let $\mathcal{C}$ be a pre-additive category and $p : X \to X$ a projection. Then $X \cong (X,p) \oplus (X, 1-p)$ in $\mathrm{Kar}(\mathcal{C})$.

Proof. One readily checks that the maps

$$X \xrightarrow{(p,1-p)} (X,p) \oplus (X,1-p) \qquad\qquad (X,p) \oplus (X,1-p) \xrightarrow{(p,1-p)^T} X$$

are mutual inverses. □

Taking the Karoubi envelope thus gives us a category $\mathcal{M}_\sim(k) := \mathrm{Kar}(\mathcal{M}^0_\sim(k))$. Already at this stage, we see something interesting happen. Pick a point $x \in \mathbb{P}^1_k$, and consider the constant morphism $x : \mathbb{P}^1_k \to \mathbb{P}^1_k$. It is clearly a projection, and so its graph defines an endomorphism of $\mathbb{P}^1_k \in \mathcal{M}_\sim(k)$ which decomposes the object. Since the image of x is just a point, we get

$$\mathbb{P}^1_k \cong \mathrm{Spec}(k) \oplus \mathbb{L},$$

where $\mathbb{L}$ is the direct complement of x. As we will see later, this motivic decomposition reflects the fact that the cohomology of $\mathbb{P}^1_k$ is one-dimensional in degrees 0 (coming from $\mathrm{Spec}(k)$) and 2 (coming from $\mathbb{L}$), and zero otherwise.

We want our category of motives to be Tannakian. There is a monoidal structure on $\mathcal{M}_\sim(k)$ such that $hX \otimes hY = h(X \times Y)$, but it does not admit duals. For this reason, we have to admit "twists" of our objects, which alter the degrees of the correspondences. More precisely, we define

$$\mathrm{Corr}^n_\sim(X,Y) := \mathrm{CH}^{\dim X + n}_\sim(X \times Y).$$

Next we define the category $\mathsf{Mot}_\sim(k)$ to be the category with objects (X,p,m) where $(X,p) \in \mathcal{M}_\sim(k)$ and $m \in \mathbb{Z}$, and

$$\mathrm{Hom}((X,p,m),(Y,q,n)) = p \circ \mathrm{Corr}^{n-m}(X,Y) \circ q.$$

This is a monoidal category with duals, namely

$$(X,p,m) \otimes (Y,q,n) = (X \times Y, p \times q, m+n), \qquad (X,p,m)^\vee = (X,p,\dim X - m).$$

It is now a good exercise to check that $\mathbb{L} \cong (\mathrm{Spec}(k), \mathrm{id}, -1)$ and hence every object of $\mathsf{Mot}_\sim(k)$ can be written as $(X,p,0) \otimes \mathbb{L}^{\otimes n}$ for some $n \in \mathbb{Z}$. We will see later that this twist by $\mathbb{L}$ is closely related to Tate twists on l-adic cohomology. The definition of the dual should remind one of Poincaré duality.

In summary, we can construct, without any assumptions, an additive, Karoubian, rigid tensor category of "motives" over any field for a chosen adequate equivalence relation. To get a Tannakian category, however, we need to make further assumptions on the equivalence relation $\sim$. In fact, if $\sim$ is rational equivalence and $k \not\subseteq \overline{\mathbb{F}}_p$, the category $\mathsf{Mot}_\sim(k)$ is never abelian [Sch94, Cor. 3.5]. The right choice is numerical equivalence:

Theorem 3.3.6 (Jannsen, 1992)**.** Let k be any field, and let $\sim$ be an adequate equivalence relation on cycles. Then for any field F of characteristic zero, the F-linear category of motives $\mathsf{Mot}_\sim(k)$ is a semisimple abelian category if and only if $\sim$ is numerical equivalence.

Proof. First, suppose $\mathsf{Mot}_\sim(k)$ is semisimple and abelian. To show $\sim = \sim_{\mathrm{num}}$, it suffices to show that if $\gamma \not\sim 0$ then $\gamma \not\sim_{\mathrm{num}} 0$: this implies that $\sim$ is coarser than $\sim_{\mathrm{num}}$, but numerical equivalence

is the coarsest equivalence relation.
So suppose $\gamma \in \mathrm{CH}^r_\sim(X)$ is non-zero. Then γ defines a non-zero morphism $\mathbb{1} \to hX(r)$, which must be a monomorphism, because $\mathrm{Spec}(k)$ is simple (its endomorphisms form a field). By semi-simplicity, γ is split, so there exists $\delta \in \mathrm{CH}^{\dim(X)-r}(X)$ such that $\delta \circ \gamma = \mathrm{id}_{\mathrm{Spec}(k)}$. But $\delta \circ \gamma = \int \delta \cap \gamma \neq 0$, so $\gamma \not\sim_{\mathrm{num}} 0$.

Next, assume $\sim = \sim_{\mathrm{num}}$. We will show that the endomorphism ring of any motive is semisimple. Since the endomorphism rings for numerical equivalence are finite-dimensional F-vector spaces, they are Artinian as left modules over themselves, and hence semisimplicity is equivalent to having vanishing Jacobson radical. Now $\mathrm{CH}^\bullet_{\mathrm{num}}(X)_F \cong \mathrm{CH}^\bullet_{\mathrm{num}}(X) \otimes F$ because the intersection product is a perfect pairing on cycles modulo numerical equivalence; see also [And04, Prop 3.2.7.1], . Hence the Jacobson radical of $\mathrm{CH}^{\dim(X)}_{\mathrm{num}}(X \times X)_F$ is trivial if and only if it is trivial for some choice of characteristic zero field $\mathbb{K}$ replacing F.

Now fix a Weil cohomology theory $H^\bullet$ with coefficient field $\mathbb{K}$. Then we have a Lefschetz trace formula: for any $f, g \in \mathrm{CH}^{\dim(X)}_{\mathrm{hom}}(X \times X)_{\mathbb{K}}$, we have

$$\langle f \cdot g^t \rangle = \sum_{i=0}^{2\dim(X)} (-1)^i \operatorname{Tr}(f \circ g \mid H^i(X)).$$

Fix a variety X. Since $\sim_{\mathrm{num}}$ is coarser than $\sim_{\mathrm{hom}}$, we have a quotient map

$$B := \mathrm{CH}^{\dim(X)}_{\mathrm{hom}}(X \times X)_{\mathbb{K}} \twoheadrightarrow \mathrm{CH}^{\dim(X)}_{\mathrm{num}}(X \times X)_{\mathbb{K}} =: A. \tag{3.2}$$

Because the rings are Artinian, their Jacobson radicals are nilpotent, so equal the nilradical (the largest nilpotent two-sided ideal; all its elements are nilpotent). Moreover, an Artinian ring is semisimple if and only if its Jacobson radical is trivial. Let J_A, J_B denote the Jacobson radicals of A, B respectively. The map (3.2) induces a map $J_B \to J_A$ because the image $S(J_B)$ of J_B is a nilpotent two-sided ideal. On the other hand, $B/J_B \twoheadrightarrow A/S(J_B)$ shows that $A/S(J_B)$ is semisimple, so $S(J_B) \supset J_A$. Thus $J_B \twoheadrightarrow J_A$.

Now consider $f \in J_A$, and pull it back to $f' \in J_B$. Since J_B is an ideal consisting of nilpotent elements, $f' \circ g$ is nilpotent for any g, so by the trace formula, $\langle f' \cdot g^t \rangle = 0$. Hence $f' \sim_{\mathrm{num}} 0$ i.e. $f = 0$. So the Jacobson radical of A is trivial, as we wanted.

So we have shown that $\mathsf{Mot}_{\mathrm{num}}(k)$ is an F-linear pseudo-abelian category with semisimple endomorphism rings. But this is equivalent to the category being semisimple [Jan92, Lem 2]. □

3.3.3 Realisation functors

Consider now a Weil cohomology theory $H^\bullet \colon \mathcal{V}_k \to \mathsf{Vec}_{\mathbb{K}}$. What does it mean for it to factor through $\mathsf{Mot}_\sim(k)$?

Suppose we have a factorisation $H^\bullet = F \circ h$. Since $h\mathbb{P}^1_k = h\,\mathrm{Spec}(k) \oplus \mathbb{L}$, we see that $F(\mathbb{L}) = H^2(\mathbb{P}^1_k) =: \mathbb{K}(-1)$ (the cohomology of $\mathbb{P}^1_k$ is non-zero only in degrees 0 and 2 for any Weil cohomology theory). If we are to obtain a tensor functor, we then have to set

$$F(X, p, m) = F((X, p, 0) \otimes \mathbb{L}^{-m}) = \mathrm{im}(H^\bullet(p)) \otimes \mathbb{K}(m).$$

Defining F on morphisms comes down to defining natural maps

$$\mathrm{CH}^{\bullet}_{\sim}(X \times Y) \longrightarrow \mathrm{Hom}_{\mathbb{K}}(H^{\bullet}(X), H^{\bullet}(Y))$$

for all X and Y. If we let $X = \mathrm{Spec}(k)$, we see that we need to define a cycle class map on this quotient of the Chow group. Moreover, if we have such a cycle class map, we can use it to define

$$\begin{aligned}\mathrm{CH}^{i}_{\sim}(X \times Y) &\longrightarrow H^{2i}(X \times Y)\\ &\xrightarrow{\sim} \bigoplus_{j=0}^{2i} H^{j}(X) \otimes H^{2i-j}(Y)\\ &\xrightarrow{\sim} \bigoplus_{j=0}^{2i} \mathrm{Hom}_{\mathbb{K}}(H^{j}(X), H^{j}(Y)),\end{aligned}$$

so giving a factorisation F is really the same as giving such a cycle class map. Of course, $H^{\bullet}$ comes with a cycle class map on $\mathrm{CH}(X)$ for any X, but this factors through $\mathrm{CH}_{\sim}(X)$ only if $\sim$ is finer than homological equivalence.

This is where we see a discrepancy: the category of motives only satisfies the universal property we want it to have if we impose at most homological equivalence, but we only get a semisimple category of motives if $\sim$ is numerical equivalence. The hope is that $\sim_{\mathrm{hom}} = \sim_{\mathrm{num}}$ for any Weil cohomology theory; this is known as Standard Conjecture D.

In summary, if $\sim = \sim_{\mathrm{num}}$, the only question we need to answer to determine if $\mathsf{Mot}_{\sim}(k)$ is Tannakian is whether it admits a fibre functor. For this, recall Theorem 3.1.13, which says that a pre-Tannakian category admits a fibre functor if and only if the rank of every object is a natural number. However, if we look at the rank of a variety in $\mathsf{Mot}_{\sim}(k)$, we get

$$\mathrm{rk}(hX) = \langle \Delta_X \cdot \Delta_X \rangle = \chi(X) = \sum_{i=0}^{\dim(X)} (-1)^i \dim_k H^i(X, \mathcal{O}_X),$$

which may be negative. However, this would be fixed if the sum on the right was not alternating. To make this happen, we need the Künneth components of the diagonal to be algebraic; that is, for every X, we want the morphisms $H^{\bullet}(X) \to H^i(X) \hookrightarrow H^{\bullet}(X)$ to be induced by algebraic cycles $p_i \in \mathrm{CH}_{\sim}(X \times X)$. It follows that we obtain decompositions

$$hX = \bigoplus_{i=0}^{2\dim X} h^i(X) := \bigoplus_{i=0}^{2\dim X} (X, p_i, 0).$$

If we have this, we can modify the commutativity constraint on the category of motives: where before we had $c_{X,Y} : X \otimes Y \xrightarrow{\sim} Y \otimes X$, we can now define

$$\tilde{c}_{X,Y} := X \otimes Y = \bigoplus_{n,m} h^n X \otimes h^m Y \xrightarrow{\bigoplus (-1)^{nm} c_{n,m}} \bigoplus_{n,m} h^m Y \otimes h^n X = Y \otimes X,$$

where we denote the restriction of $c_{X,Y}$ to $h^n X \otimes h^m Y$ by $c_{n,m}$. Calculating $\mathrm{rk}(hX)$ now gives $\sum \dim_k H^i(X, \mathcal{O}_X) \in \mathbb{N}$. This proves:

Corollary 3.3.7. Suppose that for every X, the Künneth components of the diagonal are algebraic. Then $\mathsf{Mot}_{\mathrm{num}}(k)$ is a semisimple Tannakian category.

We will still denote the category of motives with its modified commutativity constraint by $\mathsf{Mot}_\sim(k)$. We stress again that this is not known to be possible in general: the Künneth components of the diagonal being algebraic is Standard Conjecture C. It is known for abelian varieties [Kü93] and when k is a finite field:

Theorem 3.3.8. *Suppose $k = \mathbb{F}_q$. Then the Künneth components of the diagonal are algebraic, and hence $\mathsf{Mot}_{\text{num}}(k)$ is Tannakian.*

Proof. This follows from Deligne's proof of the Weil conjectures; see [KM74, Thm. 2] or [Mil94, §1]. □

3.3.4 Motives of abelian varieties

We will now focus on motives of abelian varieties over finite fields and their algebraic closures. **When writing $\mathsf{Mot}_\sim(k)$, we from now on mean the Tannakian subcategory of motives generated by abelian varieties.** In particular, $\mathbb{L} \in \mathsf{Mot}_\sim(k)$. An important fact about motives of abelian varieties is Künnemann's theorem [Kü93]:

Theorem 3.3.9. *Let A be an abelian variety. Then there is an isomorphism $h^r(A) \cong \bigwedge^r h^1(A)$ in the category of motives.*

Thus, for any Weil cohomology theory, the Betti numbers of an abelian variety are the same as those of a complex torus. Moreover, $h^1(A)$ generates the same Tannakian category as hA. As a corollary we obtain the following:

Proposition 3.3.10. *Let A be an abelian variety over a finite field. Then its Frobenius π_A acts semisimply on the l-adic étale cohomology.*

Proof. Since l-adic cohomology is a Weil cohomology theory, we have $H^r(A, \mathbb{Q}_l) = \bigwedge^r H^1(A, \mathbb{Q}_l)$. Since $H^1(A, \mathbb{Q}_l)$ is the dual of the Tate module, and we proved that π_A acts semisimply on the Tate module (Tate's theorem), π_A acts semisimply on the whole cohomology. □

3.3.5 Lefschetz motives

The category of Lefschetz motives is a slightly modified version of the motives defined above, for which we can actually prove the standard conjectures. More precisely, following [Mil99a], we will construct a category of Lefschetz motives, which will be semisimple, Tannakian, and for which $\sim_{\text{hom}} = \sim_{\text{num}}$.

Definition 3.3.11. Let k be a field, and let $\sim$ be an adequate equivalence relation on cycles. For a smooth projective variety X/k, denote by $D_\sim(X)$ the subalgebra of $\mathrm{CH}^\bullet_\sim(X)$ generated by divisors: that is, $D_\sim(X) := \mathbb{Q}[\mathrm{CH}^1_\sim(X)]$.
Define the *degree 0 Lefschetz correspondences* from X to Y as $\mathrm{LCorr}^0_\sim(X, Y) := D_\sim(X \times Y)$. Denote by $\mathsf{LMot}(k)$ the category of Lefschetz motives for numerical equivalence, constructed in the usual way, and with objects generated only by the motives of abelian varieties.

For this definition to make sense, we actually need to know some facts about Lefschetz classes, for instance:

- Pullbacks of Lefschetz classes are Lefschetz;
- Pushforwards of Lefschetz classes are Lefschetz;
- Graphs of regular maps are Lefschetz.

The first of these is obvious, as the pullback of a divisor is a divisor and φ^* is a ring homomorphism, but neither of the other two are immediate. In fact, suppose $Z \subset X$ is a closed subvariety which is not a Lefschetz class. Then $i_*[1] = [Z]$ is not Lefschetz. However, if A and B are abelian varieties and $\varphi : A \to B$ is a morphism, then φ_* sends Lefschetz classes to Lefschetz classes. The above properties are shown to hold in [Mil99a, §5]. In particular, if $k = \mathbb{F}_q$, the graph of the Frobenius endomorphism on any k-variety is Lefschetz.

Note that Janssen's proof goes through and we obtain that $\mathsf{LMot}(k)$ is semisimple abelian. Moreover, if k is the algebraic closure $\mathbb{F}$ of a finite field, we write $\mathsf{LMot}(k)$ for the semisimple Tannakian category obtained by modifying the commutativity constraint.

Theorem 3.3.12. For Lefschetz motives, numerical equivalence equals homological equivalence.

Proof. We will see in Theorem 3.3.20 that the Lefschetz group $L(A)$ of an abelian variety is reductive, so its finite-dimensional representations are semisimple. Examples of such representations are the l-adic cohomology groups of A. Hence, the non-degenerate pairing inducing Poincaré duality

$$H^{2r}(\bar{A}, \mathbb{Q}_l(r)) \otimes H^{2g-2r}(\bar{A}, \mathbb{Q}_l(g-r)) \longrightarrow H^{2g}(\bar{A}, \mathbb{Q}_l(g)) \xrightarrow{\sim} k$$

induces a non-degenerate pairing

$$H^{2r}(\bar{A}, \mathbb{Q}_l(r))^{L(A)} \otimes H^{2g-2r}(\bar{A}, \mathbb{Q}_l(g-r))^{L(A)} \longrightarrow k.$$

In the course of the proof of Theorem 3.3.20, we will see that the cohomology classes fixed by $L(A)$ are precisely those generated by the image of the cycle class map applied to the Lefschetz classes of A. What this says is that if α is a Lefschetz class and $\alpha \not\sim_{\text{hom}} 0$, there exists a Lefschetz class β on A such that $\alpha \cdot \beta \neq 0$. This is what we wanted to show. □

Corollary 3.3.13. Let $\mathbb{F} = \overline{\mathbb{F}}_p$. Then for any $l \neq p$, we have a fibre functor $\omega_l : \mathsf{LMot}(\mathbb{F}) \to \mathsf{Vec}_{\mathbb{Q}_l}$ induced by l-adic cohomology.

Proof. This follows from the section on realisation functors and Theorem 3.3.12. □

3.3.6 The Frobenius endomorphism of a motive

Fix a prime number p. We write $q = p^n$ for some n, and $\mathbb{F} := \overline{\mathbb{F}}_p$.

Suppose X is a smooth projective variety over $\mathbb{F}_q$. Then the q-Frobenius (or absolute Frobenius) is an endomorphism of X, which we denote by π_X. We can extend this to motives as follows. If hX is a pure motive, the Frobenius is simply the graph of π_X, which we also denote by π_X. We define the Frobenius of $(X, p, 0)$ as $p \circ \pi_X \circ p$ (composition as correspondences). To extend the definition of Frobenius to all motives, we impose the condition that $\pi_{X \otimes Y} = \pi_X \otimes \pi_Y$. Then since $(X, p, m) = (X, p, 0) \otimes \mathbb{L}^{-m}$, we only need to define it on $\mathbb{L}$. Now we know that $h\mathbb{P}^1 \cong h\mathbb{1} \oplus \mathbb{L}$, and Frobenius acts through multiplication by q on the Chow group, whereas the Frobenius of a point is trivial. So we define $\pi_{\mathbb{L}} := q$.

We can now generalise Proposition 3.3.10 as follows:

Proposition 3.3.14. Let X be a motive generated by abelian varieties, and let $\omega : \mathsf{Mot}_{\sim}(\mathbb{F}_q) \to \mathsf{Vec}_{\mathbb{K}}$ be an exact $\mathbb{Q}$-linear tensor functor. Then π_X acts semisimply on $\omega(X)$.

Proof. Write $X = (A, p, m)$ for some abelian variety A. Then $hA(m) \cong X \oplus X'$, where $X' = (A, 1-p, m)$. Now π_A acts semisimply on $\omega(hA)$ by Lemma 2.3.1, so the scalar multiple $\pi_{A(m)}$ acts semisimply on $\omega(hA(m))$. This vector space decomposes as $\omega(X) \oplus \omega(X')$ under the action of $\pi_{A(m)}$, so $\pi_{A(m)}$ acts semisimply on both factors. But the action on the first summand is the action of π_X, by definition of the Frobenius endomorphism. □

The following surprisingly non-trivial lemma shows that the Frobenius endomorphisms are central elements [Sou84, Prop. 2.ii]:

Proposition 3.3.15. Let $f \in \mathrm{Corr}^{\bullet}_{\sim}(X, Y)$. Then $f \circ \pi_X = \pi_Y \circ f$. That is, Frobenius commutes with algebraic cycles.

Now that we have defined the Frobenius endomorphism for any motive over $\mathbb{F}_q$, we can consider its characteristic polynomial (as we can do in any rigid monoidal k-linear category). This polynomial is preserved under exact k-linear tensor functors, so using the diagram

$$\begin{tikzcd}
\mathsf{LMot}(\mathbb{F}_q) \arrow[r] \arrow[d] & \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q) \\
\mathsf{Rep}_{\mathbb{Q}_l}(\mathrm{Gal}(\mathbb{F}_q)) \arrow[r] & \mathsf{Vec}_{\mathbb{Q}_l}
\end{tikzcd}$$

where the downward arrow is the l-adic realisation functor, we get the following result:

Proposition 3.3.16. The characteristic polynomial of the Frobenius endomorphism of a motive $(X, p, m) \in \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q)$ has Weil q-numbers as eigenvalues.

Proof. Since the Frobenius endomorphism is the graph of a regular map, it is Lefschetz. Hence the characteristic polynomial of $\pi_X \in \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q)$ can be calculated in $\mathsf{LMot}(\mathbb{F}_q)$, and via the realisation functor, it can be calculated in $\mathsf{Vec}_{\mathbb{Q}_l}$, where the abstract definition coincides with the usual characteristic polynomial.

If hX is a pure motive, the image of $\pi_X \in \mathrm{LCorr}^0(hX, hX)$ in $\mathrm{End}_{\mathbb{Q}_l}(H_l^{\bullet}(X))$ equals the image of $\pi_X \in \mathrm{End}_k(X, X)$ in $\mathrm{End}_{\mathbb{Q}_l}(H_l^{\bullet}(X))$. By the Weil conjectures, the eigenvalues of Frobenius acting on $H_l^{\bullet}(X)$ are Weil numbers. Hence the statement holds for pure motives.

Since $(X, p, 0) \oplus (X, 1-p, 0) \cong hX$, the characteristic polynomial of $(X, p, 0)$ is a factor of the one for hX. Hence its roots are Weil numbers too. Finally, $(X, p, m) \cong (X, p, 0) \otimes \mathbb{L}^{-m}$, so the eigenvalues of (X, p, m) are those of $(X, p, 0)$ multiplied by q^{-m}, and hence still Weil numbers. □

3.3.7 Some fundamental groups

Recall from Definition 2.4.5 that the Weil q-numbers form a Gal($\mathbb{Q}$)-module $W(q)$, and that $W_{1,+}(p^{\infty})$ is in bijection with isogeny classes of abelian varieties over $\mathbb{F}$. We know that we can construct affine groups corresponding to Galois modules: these are the groups of multiplicative type. We define $P(q)$, resp. P to be the multiplicative groups with characters $W(q)$, resp. $W(p^{\infty})$.

We can describe the Tannakian category $\mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P(q))$ explicitly as follows: its objects are pairs (V, Φ) where $V \in \mathsf{Vec}_{\overline{\mathbb{Q}}_l}$ and Φ is a semisimple automorphism of V whose eigenvalues lie in $W(q)$. Indeed, $P(q)$ is of multiplicative type, hence diagonalisable over $\overline{\mathbb{Q}}_l$, and the action on each eigenspace is through a character.

From this description, Proposition 3.3.16 allows us to define a functor

$$\mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q) \otimes \overline{\mathbb{Q}}_l \longrightarrow \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P(q)).$$

Indeed, $\mathsf{Mot}_{\mathrm{num}}(\mathbb{F})$ admits an abstract fibre functor ω over $\overline{\mathbb{Q}}_l$ by Theorem 3.1.8. Hence we can define the functor by sending a motive X to the pair $(\omega(X), \omega(\pi_X))$. Restricting it to Lefschetz motives gives a commutative diagram

$$\begin{tikzcd}
\mathsf{LMot}(\mathbb{F}_q) \otimes \overline{\mathbb{Q}}_l \arrow[r] \arrow[dr] & \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q) \otimes \overline{\mathbb{Q}}_l \arrow[d] \\
 & \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P(q))
\end{tikzcd}$$

The composition of the downward functors with the functor $\mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P(q)) \to \mathsf{Vec}_{\overline{\mathbb{Q}}_l}$ gives the fibre functor ω, which is exact and faithful; therefore the downward functors are exact and faithful. Thus we can apply Proposition 3.1.11 to the above diagram to get a commutative diagram of fundamental groups:

$$\begin{tikzcd}
L(q) & M(q) \arrow[l] \\
P(q) \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Let us see what happens when we replace $\mathbb{F}_q$ by $\mathbb{F}$. For any $m \geq 1$, we have functors

$$\mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q) \longrightarrow \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_{q^m})$$

induced by base change. Moving to the algebraic closure, we have $\mathsf{Mot}_{\mathrm{num}}(\mathbb{F}) = \varinjlim \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q)$ as the 2-colimit over these functors. The reason is that for any two abelian varieties A and A' over $\mathbb{F}$, there is a finite subfield over which both of them have models and such that $\mathrm{Hom}_{\mathbb{F}_q}(A_0, A_0') \cong \mathrm{Hom}_{\mathbb{F}}(A, A')$. To see this, note that homomorphism groups are finitely generated, so there is a finite field over which all finitely many generators are defined.

The base change functor does not commute with fibre functors, since it raises the eigenvalues of Frobenius to the m^{th} power, but it respects the classes of the eigenvalues in $W(p^\infty)$. The same arguments apply as in the classification of isogeny classes of abelian varieties over $\mathbb{F}$, but in this setting we can rephrase them as follows: we have commutative diagrams (for all $q = p^n$ and $m \geq 1$)

$$\begin{tikzcd}
\mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q) \arrow[r] \arrow[d] & \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_{q^m}) \arrow[d] \\
\mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P(q)) \arrow[r] & \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P(q^m))
\end{tikzcd}$$

where the bottom morphism sends a representation (V, Φ) to (V, Φ^m).

Phrased yet another way, we can take the limit over the maps $P(q) \to M(q)$ to get an induced map $P \to M$, where we defined P through $X^*(P) := W(p^\infty)$. We can apply the same arguments to the groups $L(q)$.

Proposition 3.3.17. We have a commutative diagram with injective maps:

$$\begin{tikzcd} L & & M \arrow[ll, hook'] \\ & P \arrow[lu, hook] \arrow[ru, hook'] & \end{tikzcd}$$

Proof. The construction of the diagram was discussed above. To show that the maps are injective, we need to show that every object in $\mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P)$ is a subquotient of an object coming from $\mathsf{Mot}_{\text{num}}(\mathbb{F})$. But this is Honda's theorem: for every Weil number in $W(p^\infty)$, there exists an abelian variety over $\mathbb{F}$ whose Frobenius acting on the Tate module has those eigenvalues (cf. Theorem 2.4.8). We obtain the Weil numbers which are not of weight 1 because the l-adic realisation functor ω_l on $\mathsf{LMot}(\mathbb{F})$ sends a variety to its entire l-adic cohomology, not just its Tate module, and the twists by $\mathbb{L}$ allow for non-algebraic integers to occur.

The map $M \to L$ is induced by the natural inclusion functor $\mathsf{LMot}(\mathbb{F}) \to \mathsf{Mot}_{\text{num}}(\mathbb{F})$ which is faithful (but in general not full), $\mathbb{Q}$-linear and exact. It is injective because the image of the functor generates all abelian motives. □

From now on, we identify P with a subgroup of M via the inclusion $P \hookrightarrow M$ we constructed above.

3.3.8 The Lefschetz group

Definition 3.3.18. Let A be an abelian variety over k. Denote by $\langle A \rangle^{\otimes}$ the smallest subcategory of $\mathsf{LMot}(k)$ containing $\mathbb{L}$ and A, and which is closed under subquotients, direct sums, tensor products, and duals. Note that it is again a Tannakian category.
The *Lefschetz group* of A, denoted $L(A)$, is defined to be the fundamental group of $\langle A \rangle^{\otimes}$.

Fix a Weil cohomology theory $H^\bullet$ with coefficient field $\mathbb{K}$. For an abelian variety A, denote by $H_1(A)$ the dual of $H^1(A)$. Define $C(A)$ to be the centraliser of $\operatorname{End}^0(A)$ in $\operatorname{End}_{\mathbb{K}}(H_1(A))$.

Lemma 3.3.19. *Let A be a CM abelian variety. Then $C(A) \cong Z(\operatorname{End}^0(A)) \otimes \mathbb{K}$. In particular, $C(A)$ is commutative.*

Proof. If A is of CM type, we have $[\operatorname{End}^0(A) \otimes \mathbb{K} : \mathbb{K}]_{\text{red}} = [\operatorname{End}^0(A) : \mathbb{Q}]_{\text{red}} = 2g$. Because $H^1(A)$ is a $2g$-dimensional faithful representation of $\operatorname{End}^0(A) \otimes \mathbb{K}$, Lemma 3.2.2 tells us that $\operatorname{End}^0(A) \otimes \mathbb{K}$ is a product of matrix algebras over fields L_i, and $H^1(A)$ is isomorphic to a direct sum $\bigoplus L_i^{n_i}$. Hence the centraliser of $\operatorname{End}^0(A)$ in $\operatorname{End}_{\mathbb{K}}(H^1(A)) \cong \operatorname{End}^0(A) \otimes \mathbb{K}$ is just the centre $Z(\operatorname{End}^0(A) \otimes \mathbb{K}) \cong Z(\operatorname{End}^0(A)) \otimes \mathbb{K}$. □

$C(A)$ has a well-defined Rosati involution $(-)^\dagger$. We recall the construction. Let D be any ample divisor on A. Then we have

$$\operatorname{cl}(D) \in H^2(A)(1) \cong (\textstyle\bigwedge^2 H^1(A))(1) \cong \operatorname{Hom}(\textstyle\bigwedge^2 H_1(A), \mathbb{K}(1)), \tag{3.3}$$

so we can associate a skew-symmetric bilinear form e^D to D. Because D is ample, e^D is nondegenerate. Hence there exists an involution $(-)^\dagger$ such that for all $a, b \in H_1(A)$ and for any $f \in \operatorname{End}_{\mathbb{K}}(H_1(A))$, we have

$$e^D(f(a), b) = e^D(a, f^\dagger(b)).$$

The restriction of $(-)^\dagger$ to $C(A)$ is the Rosati involution defined by D, and depends on the choice of D only up to a conjugation.

Theorem 3.3.20. Let A be an abelian variety. Then for any $\mathbb{K}$-algebra R,

$$L(A)(R) \cong \{\gamma \in C(A) \otimes R \mid \gamma^\dagger \gamma \in R^\times\}.$$

Proof. Let $\omega : \mathsf{LMot}(k) \to \mathsf{Vec}_{\mathbb{K}}$ denote the fibre functor induced by the Weil cohomology theory $H^\bullet$. By definition,

$$L(A) = \underline{\mathrm{Aut}}^{\otimes}(\omega|_{\langle A\rangle^{\otimes}}).$$

Thus, $L(A)(\mathbb{K})$ consists of those automorphisms Φ such that for any $f : B \to C$ in $\langle A\rangle^{\otimes}$,

$$\begin{tikzcd}
\omega(B) \arrow[r, "\Phi_B"] \arrow[d, "\omega(f)"'] & \omega(B) \arrow[d, "\omega(f)"] \\
\omega(C) \arrow[r, "\Phi_C"] & \omega(C)
\end{tikzcd}$$

commutes (and such that $\Phi_{X\otimes Y} = \Phi_X \otimes \Phi_Y$, $\Phi_{\mathbb{1}} = \mathrm{id}_{\mathbb{K}}$).

We have an embedding $L(A) \hookrightarrow \mathrm{GL}(\omega(h^1(A))) \times \mathbb{G}_m$ by sending $\Phi \mapsto \Phi_{h^1(A)} \times \Phi_{\mathbb{L}}$, and its image consists of the automorphisms with the above property. But the square above commutes if and only if for any $\alpha \in \mathrm{LCorr}^\bullet_\sim(X \times Y)$, the class $\mathrm{cl}(\alpha)$ is fixed by $\Phi_{X\otimes Y}$. Indeed, the action of correspondences on cohomology is given via the cycle class map composed with the isomorphism

$$H^{2i}(X \times Y) \longrightarrow \bigoplus_{j=0}^{2i} \mathrm{Hom}_{\mathbb{K}}(H^j(X), H^j(Y)),$$

which commutes with the action of algebraic cycles. Thus, $\mathrm{cl}(\alpha)$ is fixed by $\Phi_{X\otimes Y}$ if and only if $\Phi_X(\mathrm{cl}(\alpha)\Phi_Y^{-1}) = \mathrm{cl}(\alpha)$.

This realizes $L(A)$ as the biggest algebraic subgroup of $\mathrm{GL}(H_1(A)) \times \mathbb{G}_m$ fixing all Lefschetz classes. Denote by $L'(A)$ the affine algebraic group from the statement, i.e.

$$L'(A)(R) = \{\gamma \in C(A) \otimes R \mid \gamma^\dagger \gamma \in R^\times\}.$$

Define a map $L'(A) \to \mathrm{GL}(H_1(A)) \times \mathbb{G}_m$ on points by sending $\gamma \mapsto (\gamma, \gamma^\dagger\gamma)$. This is clearly injective; we want to show that its image is $L(A)$. Since both groups are of multiplicative type, it suffices to show that they fix the same vectors in any representation, i.e. we want that $\mathrm{Hom}_{L'(A)}(\mathbb{1}, V) = \mathrm{Hom}_{L(A)}(\mathbb{1}, V)$ for any representation V of $\mathrm{GL}(H_1(A)) \times \mathbb{G}_m$.

Since $L(A)$ by definition fixes the Lefschetz classes, it suffices to show that for every embedding $f : \mathbb{1} \hookrightarrow T^{m,n} := (h^1(A))^{\otimes m}(n)$, the group $L'(A)$ is the maximal subgroup fixing the image of $\omega(f)$. Here we use that any finite-dimensional representation of $L(A)$ is contained in a direct sum of those of the form $T^{m,n}$ (see [DM82, Prop. 3.1(a)], for the more general statement, and note that in this case, $h^1(A)^\vee \cong h^{2g-1}(A)(g)$).
In our case, $\mathrm{Hom}(\mathbb{1}, T^{m,n}) = \mathrm{LCorr}^n_\sim(\mathrm{Spec}(k) \times h^1(A^m))$, so the image of $\omega(f)$ consists of the divisor classes in $H^{2n}(A^r)(n)$. Milne showed that the Serre group of A, given by

$$S(A)(R) = \{\gamma \in C(A) \otimes R \mid \gamma^\dagger\gamma = 1\} \subset L'(A),$$

fixes precisely the divisor classes in $H^\bullet(A^r)$ for all r, disregarding Tate twists [Mil99a, Thm. 3.2]. On the other hand, the second entry of $L'(A)$ ensures that a fixed divisor class in $H^{2n}(A^m)(n')$ is non-zero only if $n = n'$. Indeed, let $\gamma \in L'(A)(R)$. Then for any $a, b \in H_1(A)$,

$$e^D(\gamma a, \gamma b) = e^D(a, \gamma^\dagger \gamma b) = \gamma^\dagger \gamma e^D(a, b),$$

and hence $(\gamma, \gamma^\dagger\gamma) \in (\mathrm{GL}(H_1(A)) \times \mathbb{G}_m)(R)$ fixes $\mathrm{cl}(D) \in H^2(A)(1)$, as one can see by tracing the isomorphism (3.3). This is enough to deduce that γ fixes all divisor classes on A^r for all r. Thus $L'(A) = L(A)$, as required. □

Theorem 3.3.21. An isogeny $A \to \prod A_i^{n_i}$ of A onto its simple isogeny factors realizes $L(A)$ as a subgroup of $\prod L(A_i)$.

Proof. We first prove the statement with L replaced by C. Recall that we defined

$$C(A) = \{M \in \mathrm{End}_{\mathbb{K}}(H_1(A)) \mid M \circ H_1(f) = H_1(f) \circ M \ \forall f \in \mathrm{End}^0(A)\}.$$

Then for any $n \in \mathbb{N}$, since $\mathrm{End}^0(A^n) \cong M_{n\times n}(\mathrm{End}^0_k(A))$ and $H_1(A^n) = H_1(A)^{\oplus n}$, we see that $C(A) \cong C(A^n)$ via the diagonal embedding.

In a similar way, we see that if $A \cong \prod A_i$, then $C(A) \subseteq \prod C(A_i)$ by projecting an endomorphism M onto its factors; this is injective because the projections occur as $H_1(\pi_i)$ and elements in $C(A)$ commute with these. If $\mathrm{Hom}(A_i, A_j) = 0$ for $i \neq j$, this is an isomorphism, because then any endomorphism M of $H_1(A)$ is determined by its projections, which have to lie in $C(A_i)$ if M is to be in $C(A)$. Thus, if $A \to \prod A_i^{n_i}$ is an isogeny, we get an isomorphism

$$C(A) \cong C(A_1) \times \ldots \times C(A_n).$$

Moreover, the involutions agree: if D_i is the divisor on A_i defining the involution on $C(A_i)$, then $\prod_i (D_i \times \prod_{j\neq i} A_j)$ defines the same involution on $C(A)$.

By Theorem 3.3.20, this implies that for any R, we have

$$L(A)(R) \cong \{(\gamma_i) \in \prod L(A_i)(R) \mid \gamma_i^\dagger \gamma_i = \gamma_j^\dagger \gamma_j \in R^\times \ \forall i, j\}$$

and hence $L(A) \subset \prod L(A_i)$. □

Corollary 3.3.22. Write L for the fundamental group of $\mathsf{LMot}(k)$. Then

$$L \hookrightarrow \prod_A L(A),$$

where A ranges over the isogeny classes of abelian varieties over k. In particular, if k is a finite field or an algebraic closure of a finite field, L is commutative.

Proof. Combine Theorem 3.3.21 with the fact that $\mathsf{LMot}(k) = \varinjlim_A \langle A \rangle^\otimes$ as a 2-colimit over the abelian varieties A/k. The commutativity statement follows from Lemma 3.3.19 and the fact that any abelian variety over a finite field is of CM type. □

The corollary shows that we can very explicitly describe the fundamental group of Lefschetz motives if we have a classification of the isogeny classes. We have seen such classifications for CM abelian varieties and abelian varieties over $\overline{\mathbb{F}}_p$, and we will apply the corollary in those situations.

Remark 3.3.23. In this section, we argued in a circular way: we defined the Lefschetz group as the fundamental group of $\langle A\rangle^{\otimes}$, but we needed properties of the Lefschetz group to deduce that this category was Tannakian in the first place. The correct way to argue is to first define the Lefschetz group abstractly; then show that its fixed vectors are the Lefschetz classes, and use this to define a Tannakian category of Lefschetz motives; and finally show that this Lefschetz group coincides with the fundamental group of $\langle A\rangle^{\otimes}$. This was done properly in [Mil99a] and [Mil99b], whereas our aim was to introduce the reader to these concepts with as few requirements as possible.

4. Hodge implies Tate

4.1 Overview

We denote by p a prime number, and by $\mathbb{F}$ the algebraic closure of $\mathbb{F}_p$. The main theorem we want to prove is the following [Mil99b, Thm. 7.1]:

Theorem 4.1.1. Suppose the Hodge conjecture holds for all CM abelian varieties over $\overline{\mathbb{Q}}$. Then the Tate conjecture holds for all abelian varieties over $\mathbb{F}$.

The Tate conjecture is a statement about finitely generated fields, so "the Tate conjecture over the algebraic closure of a finite field" does not really make sense. What we really mean is the following:

Conjecture 4.1.2 (Tate conjecture over $\mathbb{F}$)**.** Let $X/\mathbb{F}$ be a smooth projective variety. Then for each $0 \leq r \leq \dim(X)$, the kernel of the cycle class map

$$\mathrm{cl}^r : \mathcal{Z}^r(X) \longrightarrow H^{2r}(X, \mathbb{Q}_l(r))$$

consists of the cycles numerically equivalent to zero, and induces an isomorphism

$$\mathrm{CH}^r_{\mathrm{num}}(X) \otimes \mathbb{Q}_l \xrightarrow{\sim} \bigcup_{X_q/\mathbb{F}_q} H^{2r}(X, \mathbb{Q}_l(r))^{\mathrm{Gal}(\mathbb{F}_q)},$$

where the union is over all models of X over a finite field, i.e. those X_q such that $X_q \times_{\mathbb{F}_q} \mathbb{F} \cong X$.

Since X and its cycles are all defined over some finite subextension of $\mathbb{F}$, we see that the Tate conjecture over $\mathbb{F}$ is equivalent to the Tate conjecture over any $\mathbb{F}_{p^n}$.

Assuming the Hodge conjecture, we will construct a commutative square of exact $\mathbb{Q}$-linear tensor functors between Tannakian categories, which induces a commutative square of fundamental groups:

$$\begin{tikzcd}
\mathsf{LCM}(\overline{\mathbb{Q}}) \arrow[r] \arrow[d] & \mathsf{CM}(\overline{\mathbb{Q}}) \arrow[d] \\
\mathsf{LMot}(\mathbb{F}) \arrow[r] & \mathsf{Mot}_{\mathrm{num}}(\mathbb{F})
\end{tikzcd}
\qquad
\begin{tikzcd}
T & S \arrow[l] \\
L \arrow[u] & M \arrow[l] \arrow[u]
\end{tikzcd}$$

The dependency on the Hodge conjecture comes from the existence of the functor $\mathsf{CM}(\overline{\mathbb{Q}}) \to \mathsf{Mot}_{\mathrm{num}}(\mathbb{F})$: to construct it, we need to assume that all absolute Hodge cycles are algebraic.

As it turns out, all the groups appearing in the diagram on the right are of multiplicative type (i.e. determined by their geometric characters as Galois modules), and we can compute all of them, except possibly M (without assuming the Tate conjecture). We have, however, constructed an injection $P \hookrightarrow M$ of the Weil-number pro-torus into M (Proposition 3.3.17), and we understand the characters of P very well. When we precompose with this inclusion, we will be able to prove:

Theorem 4.1.3. There is a commutative square of affine groups

$$\begin{tikzcd}
T & S \arrow[l] \\
L \arrow[u] & P \arrow[l] \arrow[u]
\end{tikzcd}$$

such that all maps are injective, and which realizes $P = S \cap L$ inside T.

Since the above affine groups are of multiplicative type, we can study this square through the induced commutative square of character groups:

$$\begin{tikzcd}
X^*(T) \arrow[r] \arrow[d] & X^*(S) \arrow[d] \\
X^*(L) \arrow[r] & W(p^\infty)
\end{tikzcd}$$

The Tate conjecture implies that $P = M$. Conversely, Theorem 4.1.3 implies the Tate conjecture for abelian varieties over $\mathbb{F}$, which will prove the main theorem.

We will start by defining the categories and functors that make up the square, and explicitly describe their action on character groups. Once this is done, we will proceed to prove Theorem 4.1.3.

4.2 Construction of the commutative square

4.2.1 The categories

In what follows, all our categories will in the end be defined over $\overline{\mathbb{Q}}_l$ for some $l \neq p$, even though we do not include this in the notation and even define and compute with them over smaller base fields, where possible. Then in the end, we may simply extend scalars to $\overline{\mathbb{Q}}_l$. This choice of base field ensures that all our categories have fibre functors: Theorem 3.1.8 implies that $\mathsf{Mot}_{\mathrm{num}}(\mathbb{F})$ has a fibre functor over $\overline{\mathbb{Q}}_l$, and we have a functor $\mathsf{LMot}(\mathbb{F}) \to \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P)$ induced by the l-adic realisation functor. Finally, extending scalars does not change the characters of the groups of multiplicative type which occur as the fundamental groups of the categories.

Define $\mathsf{LCM}(\overline{\mathbb{Q}})$ to be the Tannakian subcategory of $\mathsf{LMot}(\overline{\mathbb{Q}})$ whose objects are generated by abelian varieties of CM type over $\overline{\mathbb{Q}}$. We denote the fundamental group of $\mathsf{LCM}(\overline{\mathbb{Q}})$ by T. Because we only use CM abelian varieties, Lemma 3.3.19 and Corollary 3.3.22 imply that T is commutative, and since its category of representations is semisimple by Jannsen's theorem, it is a group of multiplicative type over $\mathbb{Q}$, taking singular cohomology as our Weil cohomology theory.

The category $\mathsf{LMot}(\mathbb{F})$ is the Tannakian category of Lefschetz motives of abelian varieties over $\mathbb{F}$. We denote its fundamental group by L. It is of multiplicative type, again by Jannsen and Corollary 3.3.22, and defined over $\mathbb{Q}_l$, l-adic cohomology as Weil cohomology theory. Because it is of multiplicative type, L is also defined over $\mathbb{Q}$, although we won't need this.

For the last category, $\mathsf{CM}(\overline{\mathbb{Q}})$, we need the notion of absolute Hodge cycles. These are defined as follows: if $X/\overline{\mathbb{Q}}$ is an abelian variety, one can consider its algebraic deRham cohomology $H^\bullet_{\mathrm{dR}}(X)$ and its étale cohomology $H^\bullet_{\text{ét}}(X) := \left(\varprojlim H^\bullet(X_{\text{ét}}, \mathbb{Z}/n\mathbb{Z})\right) \otimes \mathbb{Q}$. An embedding $\sigma \colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ determines a canonical morphism

$$H^\bullet_{\mathbb{A}}(X) := H^\bullet_{\mathrm{dR}}(X) \times H^\bullet_{\text{ét}}(X) \longrightarrow H^\bullet_{\mathbb{A}}(X_{\sigma,\mathbb{C}}).$$

A cohomology class in $H^{2r}_{\mathbb{A}}(X)(r)$ is called *Hodge relative to σ* if its image under the above map lies in the subspace $\underline{H^{2r}_{\mathbb{A}}(X_{\sigma,\mathbb{C}},\mathbb{Q})(r)}$ and is of type (0,0). It is called *absolutely Hodge* if it is Hodge relative to every embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Like Lefschetz classes, absolute Hodge cycles have good properties: for instance, they are preserved under pushforwards and pullbacks by regular maps; they contain the algebraic classes; and the Künneth components of the diagonal are absolute Hodge cycles. Moreover, for abelian varieties it is known that a cycle is absolutely Hodge as soon as it is Hodge relative to a single embedding. All these statements can be found in [DM82]. For our purposes, it is enough to know that absolute Hodge cycles have good enough properties to act as correspondences in a category of motives.

More precisely, define $\mathsf{CM}(\overline{\mathbb{Q}})$ to be the category whose objects are motives of CM abelian varieties over $\overline{\mathbb{Q}}$, and whose correspondences are absolute Hodge cycles. It is constructed completely analogously to how we constructed the categories $\mathsf{Mot}_{\sim}(k)$, and we can modify the commutativity constraint because the Künneth components of the diagonal are absolutely Hodge. Twists are given by tensoring with $h^2(\mathbb{P}^1)^\vee$. Moreover, it is a semisimple category because the endomorphism rings are semisimple [DM18, Prop. 6.3]. We denote its fundamental group by S, and we call this the Serre group.

Remark 4.2.1. In [Mil99a], Milne defines the Serre group $S(A)$ of an abelian variety in a similar way as we defined the Lefschetz group. It is a reductive group over the coefficient field $\mathbb{K}$ of a Weil cohomology theory. Its points are given by

$$S(A)(R) = \{\gamma \in C(A) \otimes R^\times \mid \gamma^\dagger \gamma = 1\},$$

where $C(A)$ is the centraliser of $\mathrm{End}^0(A)$ in $\mathrm{End}_{\mathbb{K}}(H_1(A))$. Thus $L(A)$ is an extension of $\mathbb{G}_m$ by $S(A)$, and $S(A)$ is isomorphic to the product of $S(A_i)$ for each simple isogeny factor A_i of A (even better than Theorem 3.3.21). Milne proves that the Serre group of an abelian variety fixes precisely the divisor classes on $H^{2r}(A)$ (ibid. Theorem 3.2), but $S(A)$ crucially does not see the Tate twists, unlike the Lefschetz group.

We stress that the Serre group $S(A)$ is *not* in general to S what the Lefschetz group $L(A)$ is to L. Indeed, $S(A)$ fixes the divisor classes (on the subcategory $\langle A\rangle^{\otimes} \hookrightarrow \mathsf{CM}(\overline{\mathbb{Q}})$), whereas S fixes the Hodge classes in the cohomology of A. This does give a relationship between S and $S(A)$, namely: the Serre group $S(A)$ of A fixes precisely the Hodge classes of A if and only if no power of A supports an exotic Hodge class (cf. ibid. Proposition 4.8). When we talk about the Serre group in this chapter, we will always mean S or its variant S^K defined below, and not $S(A)$.

4.2.2 The functors

Viewing algebraic cycles as absolute Hodge cycles gives a faithful functor $\mathsf{LCM}(\overline{\mathbb{Q}}) \to \mathsf{CM}(\overline{\mathbb{Q}})$.

The functor $\mathsf{LMot}(\mathbb{F}) \to \mathsf{Mot}_{\mathrm{num}}(\mathbb{F})$ is the identity on objects. On morphisms, it is induced by the inclusions $\langle \mathrm{CH}^1_{\mathrm{num}}(X)\rangle \hookrightarrow \mathrm{CH}^\bullet_{\mathrm{num}}(X)$.

It remains to define reduction functors. We have already seen that we can reduce CM abelian varieties over $\overline{\mathbb{Q}}$. This extends to motives:

Proposition 4.2.2. There exists an exact $\mathbb{Q}$-linear tensor functor $\mathsf{LCM}(\overline{\mathbb{Q}}) \to \mathsf{LMot}(\mathbb{F})$ which sends hA to $hA_{\mathbb{F}}$.

Proof. First of all, we fix an embedding $i : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.
We first define the functor (call it R) on motives hA where A is a CM abelian variety over $\overline{\mathbb{Q}}$. Let A_0 be a model of A over a number field K, and L be a finite extension of K over which A_0 has good reduction at p, which exists by Theorem 3.2.15. Then an embedding $L \hookrightarrow \overline{\mathbb{Q}}$ determines a valuation v_L of L lying over p, given by the composition

$$v_L : L \longhookrightarrow \overline{\mathbb{Q}} \xrightarrow{i} \overline{\mathbb{Q}}_p \xrightarrow{v_p} \mathbb{Q} \cup \{\infty\}.$$

Since v_p takes the same values on Galois conjugates, this valuation does not depend on the choice of embedding. Now $A_0 \times_K \mathrm{Spec}(L)$ has good reduction at v_L. Its reduction A_k is an abelian variety over $k = \mathbb{F}_q$ for some $q = p^n$. Finally, define $R(hA) = hA_{\mathbb{F}} := h(A_k \times_{\mathbb{F}_q} \mathbb{F})$.

To describe the functor on morphisms, we use the morphisms

$$\mathrm{CH}^r(A) \xleftarrow{\sim} \mathrm{CH}^r(A') \longrightarrow \mathrm{CH}^r(A_k),$$

given by intersection with the generic, resp. the special fibre. Clearly, this procedure sends divisors to divisors and respects intersection products, so Lefschetz classes in $\mathrm{CH}^\bullet(A)$ get sent to Lefschetz classes in $\mathrm{CH}^\bullet(A_k)$.

This shows that if $M = (A, p, m)$ is a general motive, the assignment $R(M) = (A_{\mathbb{F}}, p_{\mathbb{F}}, m)$ is well-defined. From this description it follows easily that R defines a $\mathbb{Q}$-linear tensor functor; it is exact because it is additive. □

In a similar way, we obtain:

Proposition 4.2.3. Suppose the Hodge conjecture holds for CM abelian varieties over $\mathbb{C}$. Then there exists a $\mathbb{Q}$-linear exact tensor functor $\mathsf{CM}(\overline{\mathbb{Q}}) \to \mathsf{Mot}_{\mathrm{num}}(\mathbb{F})$ which sends hA to $hA_{\mathbb{F}}$.

Proof. On objects, we can argue as in the previous proposition. To define the functor on morphisms, we need that every absolute Hodge cycle is algebraic. By [DM82, Prop. 2.9], absolute Hodge classes on $A/\overline{\mathbb{Q}}$ are in bijection with absolute Hodge classes on $A_{\mathbb{C}}$, and algebraic cycles on A are in bijection with algebraic cycles on $A_{\mathbb{C}}$. Hence, the Hodge conjecture for abelian varieties of CM type over $\mathbb{C}$ implies that there are morphisms

$$\mathrm{CH}^\bullet_{AH}(X \times Y) \longrightarrow \mathrm{CH}^\bullet_{\mathrm{num}}(X_{\mathbb{F}} \times Y_{\mathbb{F}}),$$

and for the rest we can argue as in the previous proposition. □

4.2.3 A filtration by CM fields

We want to construct a filtration on our categories which will allow us to work with simpler groups. We do this as follows. Fix a Galois CM field K of finite degree over $\mathbb{Q}$. Denote by $\mathsf{LCM}^K(\overline{\mathbb{Q}})$ the Tannakian subcategory of motives generated by abelian varieties whose reflex field is contained in K. Similary define $\mathsf{CM}^K(\overline{\mathbb{Q}})$, and denote their fundamental groups by T^K, resp. S^K. Then $T = \varprojlim T^K$ and $S = \varprojlim S^K$. To get a similar description of the other fundamental groups, we need to say something about the essential image of the above categories under the reduction functors.

$\mathsf{LMot}^K(\mathbb{F})$ and $W^K(p^\infty)$

Fix a CM field $K \subset \overline{\mathbb{Q}}$ which is Galois over $\mathbb{Q}$. We want $\mathsf{LMot}^K(\mathbb{F})$ to be the essential image of $\mathsf{LCM}^K(\overline{\mathbb{Q}})$. What we need to understand for this is which eigenvalues of Frobenius can occur for the reduction of a CM abelian variety over $\overline{\mathbb{Q}}$ with reflex field contained in K. This is explained by the theorem of Shimura and Taniyama. We can state it as follows [Mil20, Thm 8.1, Cor. 8.3, Rem. 8.6]:

Theorem 4.2.4. Let A be a CM abelian variety over $\overline{\mathbb{Q}}$ with good reduction at p and with reflex field contained in a Galois CM field K. Then there exists an endomorphism $\pi \in \mathrm{End}(A)$ whose reduction is the Frobenius of $A_{\mathbb{F}}$. Moreover, if φ is a CM-type corresponding to A under Theorem 3.2.12 and if $A_0/\mathbb{F}_q$ is a model for $A_{\mathbb{F}}$, then for any prime $w \mid p$ of K, we have

$$f_{\pi_{A_0}}(w) := \frac{\mathrm{ord}_w(\pi_{A_0})}{\mathrm{ord}_w(q)}[K_w : \mathbb{Q}_p] = \sum_{\tau^{-1}(w_K)=w} \varphi(\tau),$$

where w_K is the prime of K over p used to define the reduction functor, and the sum on the right ranges over the embeddings $\tau : K \hookrightarrow \overline{\mathbb{Q}}$ such that $\tau^{-1}(w_K) = w$.

The important thing to take away from this theorem is that there exists an explicit relationship between the CM-type of a CM abelian variety over $\overline{\mathbb{Q}}$ and the Frobenius of its reduction. Since we already know this Frobenius is a Weil q-number, it can be determined by its v-adic orders for any $v \mid p$, and the theorem gives us the information to calculate these.

We see that for abelian varieties over $\mathbb{F}$ coming from $\mathsf{LCM}^K(\overline{\mathbb{Q}})$, we will always have $f_\pi(v) \in \mathbb{Z}$ for any $v \mid p$ of K. Motivated by this, we define

$$W^K(p^n) := \{\pi \in K \cap W(p^n) \mid f_\pi(v) \in \mathbb{Z} \text{ for all } v \mid p\},$$

and $W^K(p^\infty) := \varinjlim W^K(p^n)$. This is a $\mathrm{Gal}(\mathbb{Q})$-submodule of $W(p^\infty)$, and we denote the multiplicative group with characters $W^K(p^\infty)$ by P^K. Then since $X^*(P) = W(p^\infty)$, we have $P = \varprojlim P^K$.

We define $\mathsf{LMot}^K(\mathbb{F})$ to be the Tannakian subcategory generated my motives of abelian varieties whose Frobenius lies in $W^K(p^\infty)$. Denote its fundamental group by L^K. Then $L = \varprojlim L^K$. Hence we have constructed for any K satisfying our criteria a commutative diagram

$$\begin{tikzcd}
\mathsf{LCM}^K(\overline{\mathbb{Q}}) \arrow[r] \arrow[d] & \mathsf{CM}^K(\overline{\mathbb{Q}}) \arrow[d] \\
\mathsf{LMot}^K(\mathbb{F}) \arrow[r] & \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P^K)
\end{tikzcd}$$

and if we let K grow, we get back our original diagram.

4.3 Calculation of the character groups

The next step is to calculate the character groups corresponding to the fundamental groups in the above diagram. We already know the characters of P^K: by definition, they are given by

$W^K(p^\infty)$. It remains to calculate the other three. There are two ways one could go about this: one is by working with the categories directly, and identifying the group of rank 1 objects under $\otimes$. The other is by working with the fundamental groups. We will follow Milne and take the second approach: we have good descriptions of the fundamental groups involved, whereas determining the group of rank 1 motives seems tricky: proving that a motive is of rank 1 comes down to constructing algebraic cycles which cut out this motive, but constructing algebraic cycles is a notoriously difficult problem.

4.3.1 $X^*(T^K)$

For a Galois CM field $K/\mathbb{Q}$ of degree $2g$, denote by $\mathsf{LCM}^K(\overline{\mathbb{Q}})$ the Tannakian subcategory of motives generated by CM abelian varieties over $\overline{\mathbb{Q}}$ whose reflex field is contained in K. Denote its fundamental group by T^K. By the classification theorem 3.2.12, the isogeny classes of abelian varieties whose motives generate this category are indexed by Galois orbits of CM-types on K. Let Φ be such a CM-type. Since the Lefschetz group of an abelian variety is determined by its isogeny class, we can define $T^\Phi := L(A_\Phi)$, where A_Φ is any abelian variety whose associated CM-type corresponds to Φ.

Proposition 4.3.1. Let Φ be as above. Then

$$X^*(T^\Phi) = \frac{\{f\colon \Phi \to \mathbb{Z}\}}{\{f \mid f = f\iota \text{ and } \sum_{\varphi\in\Phi} f(\varphi) = 0\}}.$$

Proof. By Lemma 3.3.19 and Theorem 3.3.20, the geometric points of the Lefschetz group of $A = A_\Phi$ are given by

$$L(A)(\overline{\mathbb{Q}}) = \{\gamma \in Z(\mathrm{End}^0(A)) \otimes \overline{\mathbb{Q}} \mid \gamma^\dagger\gamma \in \overline{\mathbb{Q}}^\times\}.$$

Since A is a simple CM abelian variety over $\overline{\mathbb{Q}}$, its endomorphism algebra is a field of degree $2g$, which we denote E_Φ. Thus we realise $L(A) \subset (\mathbb{G}_m)_{E_\Phi/\mathbb{Q}}$. This inclusion induces a surjection of character groups

$$X^*((\mathbb{G}_m)_{E_\Phi/\mathbb{Q}}) \cong \mathbb{Z}^{\mathrm{Hom}(E_\Phi,\overline{\mathbb{Q}})} \longrightarrow X^*(L(A)). \tag{4.1}$$

We can identify $\mathrm{Hom}(E_\Phi, \overline{\mathbb{Q}})$ with Φ: the left-hand side is $\mathrm{Gal}(\mathbb{Q})$ modulo the stabiliser of some chosen $\varphi \in \Phi$, which is isomorphic to Φ as $\mathrm{Gal}(\mathbb{Q})$-sets via $\sigma \mapsto \sigma\varphi$. With this notation, we want to show that the kernel of (4.1) equals $\{f\colon \Phi \to \mathbb{Z} \mid f = f\iota \text{ and } \sum_{\varphi\in\Phi} f(\varphi) = 0\}$. Write $\Phi = \{\varphi_0, \dots, \varphi_{g-1}, \iota\varphi_0, \dots, \iota\varphi_{g-1}\}$.

The kernel of (4.1) consists of those characters χ such that for all $a \in L(A)(\overline{\mathbb{Q}})$, we have $\chi(a) = 1$. Now because the Rosati involution restricts to complex conjugation on $C(A)$, we see that $\gamma^\dagger\gamma \in \overline{\mathbb{Q}}^\times \subset (\overline{\mathbb{Q}}^\times)^\Phi$ if and only if $\gamma_i\iota\gamma_i$ is independent of i, where $\gamma_i = \varphi_i^*(\gamma)$ denotes the φ_i-component of γ. Hence a character $\chi = \sum a_i\varphi_i^* + b_i\iota\varphi_i^*$ evaluates to 1 on $L(A)(\overline{\mathbb{Q}})$ if and only if for all $\gamma \in L(A)(\overline{\mathbb{Q}})$,

$$\chi(\gamma) = \prod \gamma_i^{a_i}\iota\gamma_i^{b_i} = 1.$$

This is clearly satisfied if $a_i = b_i$ for all i and $\sum a_i = 0$. Conversely, evaluating such a χ on the elements $\varphi_i + \iota\varphi_i$ gives $a_i = b_i$ for all i, and on $\sum \varphi_i + \iota\varphi_i$ gives $\sum a_i = 0$. This is what we wanted. □

Proposition 4.3.2. The character group $X^*(T^K)$ is a quotient of $\bigoplus_\Phi X^*(T^\Phi)$, where the product ranges over all Galois orbits of CM-types on K.

Proof. Combine Theorem 3.2.12 and Corollary 3.3.22. □

We will see that the above proposition is enough for our purposes: we don't need to know the exact structure of $X^*(T^K)$.

4.3.2 $X^*(L^K)$

Let Θ denote a Galois orbit in $W^K_{1,+}(p^\infty)$. Let A_Θ be an abelian variety over $\mathbb{F}$ corresponding to Θ, well-defined up to isogeny. Define $L^\Theta := L(A_\Theta)$. We can explicitly describe the characters of this group:

Proposition 4.3.3. The characters of L^Θ are given by

$$X^*(L^\Theta) = \frac{\{f\colon \Theta \to \mathbb{Z}\}}{\{f \mid f = f\iota \text{ and } \sum_{\alpha\in\Theta} f(\alpha) = 0\}}$$

with the natural Galois action.

Proof. Analogous to Proposition 4.3.1. In this case, we use the following identification: if A is a simple abelian variety over $\mathbb{F}$ and A_0 is a model for A, we have a $\mathrm{Gal}(\mathbb{Q})$-equivariant bijection

$$\mathrm{Hom}(\mathbb{Q}[\pi_{A_0}], \overline{\mathbb{Q}}) \longrightarrow \Theta,$$

where Θ is the Galois orbit of Frobenius eigenvalues of A_0 in $W_{1,+}(p^\infty)$ (cf. Remark 2.4.9). □

Proposition 4.3.4. The character group $X^*(L^K)$ is a quotient of $\bigoplus_\Theta X^*(L^\Theta)$, where the product ranges over all Galois orbits of elements from $W^K_{1,+}(p^\infty)$.

Proof. Combine Theorem 2.4.8 and Corollary 3.3.22. □

4.3.3 $X^*(S^K)$

We defined $\mathsf{CM}^K(\overline{\mathbb{Q}})$ to be the Tannakian subcategory of Hodge motives generated by CM abelian varieties with reflex field contained in K. The category of Hodge motives of CM abelian varieties is equivalent to the category of Hodge structures of CM type (induced by singular cohomology), which has a forgetful fibre functor. As an example of this, consider an abelian variety A of CM type over $\overline{\mathbb{Q}}$: in this case we have a Hodge structure of CM type on $H_1(A, \mathbb{Q})$, which we used in the classification of isogeny classes of such varieties.
The characters of S^K have the following description ([Mil99b, §3], or [Mil20, §4] for more details):

Proposition 4.3.5. The characters of the Serre group S^K are given by

$$X^*(S^K) = \{f\colon \mathrm{Hom}(K, \overline{\mathbb{Q}}) \to \mathbb{Z} \mid f(\tau) + f(\iota\tau) \text{ does not depend on } \tau\}$$

with the natural Galois action.

Remark 4.3.6. The proposition can be understood by looking at the example where $A/\overline{\mathbb{Q}}$ is simple of CM type with reflex field contained in K. Let $E = \mathrm{End}^0(A)$ be its field of endomorphisms. Denote by φ the CM-type defining the isogeny class of A as in Theorem 3.2.10, and define for each $\sigma\colon E \hookrightarrow \overline{\mathbb{Q}}$ a map $\psi_\sigma\colon \mathrm{Hom}(K, \overline{\mathbb{Q}}) \to \mathbb{Z}$, given by

$$\psi_\sigma(\tau) := \tilde{\tau}\varphi(\sigma) = \varphi(\tilde{\tau}^{-1}\sigma),$$

where $\tilde{\tau} \in \mathrm{Gal}(\mathbb{Q})$ is any extension of τ. This is well-defined by definition of the reflex field $K' \subset K$: indeed, $\tilde{\tau}\varphi = \varphi \iff \tau|_{K'} = \mathrm{id}$. Since φ is a CM-type, we have $\psi_\sigma(\tau) + \psi_\sigma(\iota\tau) = 1$ for all τ, and these ψ_σ are precisely the characters of S^K acting on $H_1(A, \mathbb{Q})$.
Note that the ψ_σ can be viewed as the elements of the Galois orbit of CM-types associated to A in Theorem 3.2.12. Thus, this gives a new interpretation of this theorem: two simple CM abelian varieties are isogenous if and only if S acts on their cohomology through the same characters.

4.3.4 The maps between the character groups

Finally, it remains to describe the maps between the character groups which are induced by the functors between the Tannakian categories.

Lemma 4.3.7. Let Φ be a Galois orbit of CM-types on K. Then the function $Z^\Phi \to X^*(S^K)$ sending

$$f \longmapsto \sum_{\varphi \in \Phi} f(\varphi)\varphi$$

factors through $X^*(T^\Phi)$, and is the map on characters corresponding to the functor $\mathsf{LCM}(\overline{\mathbb{Q}}) \to \mathsf{CM}(\overline{\mathbb{Q}})$.

Proof. The map $Z^\Phi \to X^*(S^K)$ is well-defined: as each $\varphi \in \Phi$ is a CM-type, we have $\varphi(\tau) + \varphi(\iota\tau) = 1$ for all $\tau \in \mathrm{Hom}(K, \overline{\mathbb{Q}})$. Hence

$$\sum f(\varphi)\varphi(\tau) + \sum f(\varphi)\varphi(\iota\tau) = \sum f(\varphi)$$

is independent of τ. Next, suppose $f = f\iota$ and $\sum f(\varphi) = 0$. Then for any $\tau : K \to \overline{\mathbb{Q}}$, we have

$$2\sum f(\varphi)\varphi(\tau) = \sum f(\varphi)\varphi(\tau) + \sum f(\varphi)\varphi(\iota\tau) = \sum f(\varphi) = 0,$$

so this is the zero function. Hence the map factors through $X^*(T^\Phi)$. To see that it is the map on characters corresponding to the functor, it suffices to check what happens to the Galois orbit of CM-types Φ of a simple abelian variety. By Remark 4.3.6, the CM-types in the orbit define the characters of S^K, so the given map is indeed correct. □

Combining these maps for all Galois orbits of CM-types on K gives a map $X^*(T^K) \to X^*(S^K)$.

The map corresponding to $\mathsf{LMot}^K(\mathbb{F}) \to \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P^K)$ has the following description: we associated motives over $\mathbb{F}$ to the Galois orbit of their Frobenius, which we then sent to the representation with those eigenvalues. Thus, the $L^\Theta \to W^K(p^\infty)$ which is simply induced by sending $\alpha \in \Theta$ to $\alpha \in W^K(p^\infty)$. We check that it is well-defined:

Lemma 4.3.8. Let Θ be a Galois orbit in $W^K_{1,+}(p^\infty)$. Then the function $Z^\Theta \to W^K(p^\infty)$ sending

$$f \longmapsto \prod_{\alpha \in \Theta} \alpha^{f(\alpha)}$$

factors through $X^*(L^\Theta)$.

Proof. We need to show that if $f = f\iota$ and $\sum_{\alpha\in\Theta} f(\alpha) = 0$, then the product $\prod \alpha^{f(\alpha)}$ equals $1 \in W^K(p^\infty)$. For this, it is enough to show that its square is 1. Let $n \in \mathbb{N}$ be big enough so that every element in Θ lies in $W^K(p^n)$. They all have the same weight w, and so

$$\prod_{\alpha\in\Theta} \alpha^{2f(\alpha)} = \prod_{\alpha\in\Theta} \alpha^{f(\alpha)+f(\iota\alpha)} = \prod_{\alpha\in\Theta} ||\alpha||^{2f(\alpha)} = p^{nw\sum_{\alpha\in\Theta} f(\alpha)} = 1.$$

□

Combining these maps for all Galois orbits of CM-types on K gives the map $X^*(L^K) \to X^*(P^K)$.

Characters of the reduction functor

To describe the vertical character maps, we are again back to the following question: given a CM-type on K, what is the Galois orbit of the Frobenius of the reduction of the associated abelian variety over $\overline{\mathbb{Q}}$? We will use the theorem of Taniyama and Shimura (4.2.4) to give an explicit construction of the maps.

Let's have a closer look at the function f_π appearing in Theorem 4.2.4. Let Y denote the set of primes of K lying over p. Then for any $n \geq 1$, we have a $\mathrm{Gal}(\mathbb{Q})$-equivariant map

$$\begin{aligned} W^K(p^n) &\longrightarrow \mathbb{Z}[Y] \\ \pi &\longmapsto f_\pi \colon w \mapsto \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(p^n)}[K_w : \mathbb{Q}_p] \end{aligned}$$

which induces a well-defined map $W^K(p^\infty) \to \mathbb{Z}[Y]$.

Lemma 4.3.9. The map $W^K(p^\infty) \to \mathbb{Z}[Y]$ given by $[(\pi, n)] \mapsto f_\pi$ is injective.

Proof. In general, two elements of a number field K differ by a root of unity if and only if their quotient has norm 1 under every norm on K. For Weil p-numbers, this is trivially the case for norms coming from primes not lying over p.
Let $[(\pi, n)], [(\pi', n')] \in W^K(p^\infty)$, so that they have representatives $\pi^{n'}, \pi'^n \in W^K(p^{nn'})$. Then $f_\pi = f_{\pi'}$ implies that $\mathrm{ord}_w(\pi^{n'}) = \mathrm{ord}_w(\pi'^n)$ for all $w \mid p$, so $\pi^{n'}$ and π'^n differ by a root of unity, which implies $[(\pi, n)] = [(\pi', n')]$. □

We now construct a map $g \mapsto [g(\varpi)] \colon X^*(S^K) \to W^K(p^\infty)$ and prove that it is well-defined; afterwards we will show that this is the map on characters. Recall that $X^*(S^K)$ is the set of functions $g : \mathrm{Hom}(K, \overline{\mathbb{Q}})$ such that $g(\tau) + g(\iota\tau)$ is independent of τ. Fix a prime w_K of $\overline{\mathbb{Q}}$ lying over p. Let h be the order of w_K in the class group of K, and let $(\varpi) = w_K^h$.

Given any $g \in X^*(S^K)$, we can consider g as a function $K \to \overline{\mathbb{Q}}$ by defining

$$g(a) = \prod_{\tau : K \to \overline{\mathbb{Q}}} \tau(a)^{g(\tau)}.$$

Lemma 4.3.10. Fix $g \in X^*(S^K)$. Then $g(\varpi) \in W^K(p^n)$ for $n = fh$, where f denotes the inertia degree of w_K. Moreover, $[g(\varpi)] \in W^K(p^\infty)$ has weight $\mathrm{wt}(g) := g + \iota g$ and is independent of the choice of generator ϖ.

Proof. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We compute the norm of $\sigma(g(\varpi))$ as follows:

$$\begin{aligned} ||\sigma(g(\varpi))||^2 = \sigma(g(\varpi) \cdot \iota g(\varpi)) = \sigma \prod_{\tau : K \hookrightarrow \overline{\mathbb{Q}}} \tau(\varpi)^{g(\tau) + \iota g(\tau)} = \\ = \mathrm{Nm}_{K/\mathbb{Q}}(\varpi)^{\mathrm{wt(p)}} = p^{fh \cdot \mathrm{wt}(g)}. \end{aligned}$$

Thus $g(\varpi)$ is a Weil p^{fh}-number of weight $\mathrm{wt}(g)$. To show that it lies in $W^K(p^{fh})$, we compute, for any prime $w \mid p$ of K,

$$f_{g(\varpi)}(w) = \frac{\mathrm{ord}_w(g(\varpi))}{\mathrm{ord}_w(p^{fh})}[K_w : \mathbb{Q}_p] = \frac{\sum g(\tau)\mathrm{ord}_w(\tau(\varpi))}{\mathrm{ord}_w(p^{fh})}[K_w : \mathbb{Q}_p].$$

Now note that $\mathrm{ord}_w(p) = e$, the ramification index of w_K (= the ramification index of any $w \mid p$), and that

$$\mathrm{ord}_w(\tau(\varpi)) = \begin{cases} h & \tau(w_K) = w; \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, $[K_w : K_w^{\mathrm{ur}}] = e$ and $[K_w^{\mathrm{ur}} : \mathbb{Q}_p] = f$, and hence $[K_w : \mathbb{Q}_p] = ef$. Thus the formula simplifies to

$$\frac{efh \sum_{\tau(w_K)=w} g(\tau)}{efh} = \sum_{\tau(w_K)=w} g(\tau) \in \mathbb{Z}. \tag{4.2}$$

From this last expression, it follows that $[g(\varpi)] \in W^K(p^\infty)$ is well-defined. Indeed, the map $W^K(p^\infty) \to \mathbb{Z}[Y]$, $\pi \mapsto f_\pi$ is injective, and clearly the above expression does not depend on the choice of ϖ. □

Thus, we get a morphism $X^*(S^K) \to W^K(p^\infty)$ sending $g \mapsto \pi(g) := [g(\varpi)]$. To see that it is the map on character groups corresponding to the reduction functor, we need to see that for any embedding $\rho : K \hookrightarrow \overline{\mathbb{Q}}$, we have $[g(\varpi)] = [\rho(\pi)]$. Note that both are Weil numbers of weight 1.

Proposition 4.3.11. The map $g \mapsto \pi(g) := [g(\varpi)]$ is the induced map on characters of the functor $\mathsf{CM}^K(\overline{\mathbb{Q}}) \to \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P^K)$.

Proof. Let $w_K \mid p$ be the prime of K used to define the reduction functor, and let $A/\overline{\mathbb{Q}}$ be a CM abelian variety such that $E := \mathrm{End}^0(A) \subset K$. In particular, the reflex field of A is contained in K. Let φ be the CM-type on E which corresponds to A as in Theorem 3.2.12. Fix an embedding $\rho : E \hookrightarrow \overline{\mathbb{Q}}$. By Theorem 4.2.4, there is some $\pi \in E$ realizing the Frobenius of the reduction of A, and at the same time, ρ induces a CM-type φ_ρ on K. We want to show that $[\rho(\pi)] = [\varphi_\rho(\varpi)]$.

By Lemma 4.3.9, it suffices to show that $f_{\rho(\pi)} = f_{\varphi_\rho(\varpi)}$. We have, for any $w \mid p$ of K,

$$f_{\rho(\pi)}(w) = [K_w : \rho(E)_v] f_{\rho(\pi)}(v) = [K_w : \rho(E)_v] \sum_{\tau^{-1}(w_K)=v} \varphi(\tau \circ \rho),$$

where v equals w_K restricted to $\rho(E)$, and where the last equality is the theorem of Shimura and Taniyama.
On the other hand, we saw in (4.2) that

$$f_{\varphi_\rho(\varpi)}(w) = \sum_{\tau(w_K)=w} \varphi_\rho(\tau) = [K_w : \rho(E)_v] \sum_{\tau(w_K)=v} \varphi_\rho(\tau),$$

and since by definition $\varphi_\rho(\tau) = \varphi(\tau|_E) = \varphi(\tau^{-1} \circ \rho)$, this finishes the proof. □

This completes the construction of the map of characters associated to the reduction of abelian varieties. The calculations from the previous sections are summarised in Figure 4.1.

- Φ : Γ-orbit of CM-types on K
- $\Theta = \pi(\Phi)$
- w_K : fixed prime of K over p

$$\begin{tikzcd}
& \mathbb{Z}^{\Phi} \arrow[dl, two heads] \arrow[dr, "f \mapsto \sum_{\varphi\in\Phi} f(\varphi)\varphi"] & \\
X^*(T^{\Phi}) = \dfrac{\{f : \Phi \to \mathbb{Z}\}}{\{f \mid f = f\iota \text{ and } \sum_{\varphi\in\Phi} f(\varphi) = 0\}} \arrow[rr] \arrow[d, "\sum_{\varphi\in\Phi} f(\varphi)\varphi \mapsto \sum_{\varphi\in\Phi} f(\varphi)\pi(\varphi)"'] & & X^*(S^K) = \{f : \mathrm{Hom}(K,\overline{\mathbb{Q}}) \to \mathbb{Z} \mid f(\tau) + f(\iota\tau) \text{ is independent of } \tau\} \arrow[d, "\pi"', "g \mapsto \pi(g) = {[g(\varpi)]}"] \\
X^*(L^{\Theta}) = \dfrac{\{f : \Theta \to \mathbb{Z}\}}{\{f \mid f = f\iota \text{ and } \sum_{\alpha\in\Theta} f(\alpha) = 0\}} \arrow[rr] & & X^*(P^K) = W^K(p^{\infty}) = \{[\alpha] \in W(p^{\infty}) : \alpha \in K \text{ and } f_{\alpha}(w) \in \mathbb{Z}\ \forall w \mid p\} \\
& \mathbb{Z}^{\Theta} \arrow[ul, two heads] \arrow[ur, "f \mapsto \prod_{\alpha\in\Theta} \alpha^{f(\alpha)}"'] &
\end{tikzcd}$$

where

- $(\varpi) = w_K^h$
- $g(\varpi) := \prod_{\tau : K \hookrightarrow \overline{\mathbb{Q}}} \tau(\varpi)^{g(\tau)}$

Figure 4.1: Overview of the character groups and maps between them.

4.4 $P = S \cap L$

Recall that we want to prove the following theorem:

Theorem 4.4.1. In the commutative square with injective maps

$$\begin{tikzcd}
T & S \arrow[l, hook'] \\
L \arrow[u, hook] & P \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

the image of P equals $S \cap L \subset T$.

There are convenient reformulations:

Lemma 4.4.2. The following are equivalent:

1) $P = S \cap L \subset T$.
2) The induced map $\operatorname{coker}(P \to L) \to \operatorname{coker}(S \to T)$ is injective.
3) The induced map $\operatorname{coker}(P \to S) \to \operatorname{coker}(L \to T)$ is injective.

Proof. We first extend the diagram to one with exact rows by taking cokernels:

$$\begin{tikzcd}
0 & Q' \arrow[l] & T \arrow[l] & S \arrow[l, hook'] & 0 \arrow[l] \\
0 & Q \arrow[l] \arrow[u] & L \arrow[l] \arrow[u, hook] & P \arrow[l, hook'] \arrow[u, hook] & 0 \arrow[l]
\end{tikzcd}$$

Now 1) $\implies$ 2) is a diagram chase starting at Q (after taking R-points, if one wishes). Conversely, if $Q \hookrightarrow Q'$, we find that any $t \in S \cap L$ comes from P.
The equivalence of 2) and 3) is seen immediately after applying the snake lemma to the above diagram. □

After moving to character groups, we want to show the dual statements. For that sake, we make the following definition:

Definition 4.4.3. A commutative square of abelian groups

$$\begin{tikzcd} A \arrow[r, "h_1"] \arrow[d, "v_1"'] & B \arrow[d, "v_2"] \\ C \arrow[r, "h_2"] & D \end{tikzcd}$$

is said to be *almost cartesian* if all maps are surjective and $\ker(v_1) \twoheadrightarrow \ker(v_2)$, or equivalently, $\ker(h_1) \twoheadrightarrow \ker(h_2)$.

Thus, we can reformulate Theorem 4.1.3 as follows:

Theorem 4.4.4. Let K be a sufficiently large CM field of finite degree over $\mathbb{Q}$. Then the diagram

$$\begin{tikzcd} X^*(T^K) \arrow[r] \arrow[d] & X^*(S^K) \arrow[d] \\ X^*(L^K) \arrow[r] & X^*(P^K) \end{tikzcd}$$

is almost cartesian.

The next few pages are devoted to the proof of this theorem. In a sense, the heavy theory is behind us: we have used this to describe the groups and maps appearing in the square of characters. The next step is to make everything explicit enough to calculate with. After that, the proof of the theorem comes down to elementary linear and homological algebra.

4.4.1 Set-up and notation

We make the following assumptions on K: it is a Galois CM field of degree $2g$ over $\mathbb{Q}$, which properly contains an imaginary quadratic extension $E/\mathbb{Q}$ in which p splits, and which contains a real subfield of degree at least 3 in which p is inert. Since the union of such fields K is $\mathbb{Q}^{cm}$, this is justified. Moreover, we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ so that for varying such K, we get primes $w_K \mid p$ in a compatible way.

We now make very explicit descriptions of our objects in order to calculate with them. Write $\Gamma := \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K/E) \times \langle \iota \rangle = \{\tau_0, \dots, \tau_{g-1}, \iota\tau_0, \dots, \iota\tau_{g-1}\}$. Denote by $D \subset \Gamma$ the decomposition group of w_K, and let $d = |D|$. Since p splits in E, we have $d \mid g$. On the other hand, $d > 2$ because we assume p is inert in a degree > 2 subfield.

We will assume that the elements of Γ are ordered such that

$$D = \{\tau_0, \ldots, \tau_{d-1}\} \qquad \text{and} \qquad \tau_{kd+i}D = \tau_{kd}D \;\; \forall k = 0, \ldots, \frac{g}{d} - 1, \; \forall i = 1, \ldots, d-1.$$

Note that we have a bijection $\Gamma/D \xrightarrow{\sim} \{\text{primes of } K \text{ lying over } p\}$ given by $[\tau] \mapsto \tau w_K$.

Lemma 4.4.5. We have a commutative diagram

$$\begin{tikzcd}
X^*(S^K) \arrow[r, hook] \arrow[d, "g \mapsto {[g(\varpi)]}"'] & \mathbb{Z}[\Gamma] \arrow[d] \\
W^K(p^\infty) \arrow[r, "\pi \mapsto f_\pi"] & \mathbb{Z}[\Gamma/D]
\end{tikzcd}$$

Here the vertical arrow on the right sends g to the map $[\tau] \mapsto \sum_{\sigma\in[\tau]} g(\sigma)$.

Proof. Comparing the two compositions, want to show that

$$f_{g(\varpi)} \colon w \longmapsto \sum_{\tau w_K = w} g(\tau).$$

But this is exactly what we showed in the proof of Lemma 4.3.10. □

Corollary 4.4.6. Suppose $f, g \in X^*(S^K)$ are in the same D-orbit. Then $\pi(f) = \pi(g)$.

Proof. By Lemma 4.4.5, the images of f and g are equal in $\mathbb{Z}[Y]$. But the map $W^K(p^\infty) \to \mathbb{Z}[Y]$ is injective, so $\pi(f) = \pi(g)$. □

We can now also describe the map $X^*(T^\Phi) \to X^*(L^\Theta)$: the map $g \mapsto [g(\varpi)]$ from above is Galois equivariant, so it sends an orbit Φ surjectively to an orbit $\pi(\Phi)$. The map on characters $X^*(T^\Phi) \to X^*(L^{\pi(\Phi)})$ then becomes the following:

$$\sum_{\varphi\in\Phi} f(\varphi)\varphi \longmapsto \sum_{\varphi\in\Phi} f(\varphi)\alpha(\varphi).$$

In order to calculate more efficiently with the characters of S, we prove the following easy lemma:

Lemma 4.4.7. A $\mathbb{Z}$-basis for $X^*(S^K) = \{f : \Gamma \to \mathbb{Z} \mid f(\tau) + f(\iota\tau) \text{ is independent of } \tau\}$ is given by the following CM-types on K:

$$\varphi_i := \tau_i^* + \sum_{j\neq i} \iota\tau_j^* \quad \text{for} \quad i = 0, \ldots, g-1;$$
$$\bar{\varphi} := \sum_{j=0}^{g-1} \iota\tau_j^*.$$

Here $\tau^* : \Gamma \to \mathbb{Z}$ denotes the function sending τ to 1 and everything else to 0.

Proof. We can explicitly write any function $f : \Gamma \to \mathbb{Z}$ such that $n = f(\tau) + f(\iota\tau)$ is independent of τ as the sum

$$f = \sum_{i=0}^{g-1} f(\tau_i)\varphi_i + \left(n - \sum_{i=0}^{g-1} f(\tau_i)\right)\bar{\varphi}.$$

For $\mathbb{Z}$-linear independence, note that $\sum n_i\varphi_i + n\bar{\varphi} = 0$ implies $n_i = 0$ for all i (evaluating at τ_i) and thus also $n = 0$. □

We see that the Galois orbits of CM-types $\Phi := \{\varphi_0, \ldots, \varphi_{g-1}, \iota\varphi_0, \ldots, \iota\varphi_{g-1}\}$ and $\bar{\Phi} := \{\bar{\varphi}, \iota\bar{\varphi}\}$ together cover the basis from the lemma.

Lemma 4.4.8. Let Ψ be either Φ or $\bar{\Phi}$, and let $\Theta = \pi(\Psi)$ be the Γ-orbit of Weil numbers obtained by applying $\pi = X^*(S^K \to P^K)$. Then the bottom map in the commutative square

$$\begin{tikzcd}
X^*(T^\Psi) \arrow[r] \arrow[d] & X^*(S^K) \arrow[d] \\
X^*(L^\Theta) \arrow[r] & W^K(p^\infty)
\end{tikzcd}$$

is injective.

Proof. We first consider the case $\Psi = \bar{\Phi}$. Let $a := \pi(\bar{\varphi}) \in \Theta$. Suppose $f\colon \{a, \bar{a}\} \to \mathbb{Z}$ gets sent to $1 \in W^K(p^\infty)$, i.e.

$$a^{f(a)} \cdot \bar{a}^{f(\bar{a})} = 1.$$

By Lemma 4.3.10 and the fact that $\bar{\varphi}$ has weight 1, we see that the complex norm of any representative of a is not 1. Thus, after replacing $a, \bar{a}$ and 1 by representatives in some $W^K(p^n)$ and taking norms, the equation gives $f(a) = -f(\bar{a})$ and hence (again using the equation) a and $\bar{a}$ differ by a root of unity. This implies that $a = \bar{a}$ in $W^K(p^\infty)$, and hence $f \equiv 0$.

Next, we consider the case $\Psi = \Phi$. In order to show injectivity of the bottom map, we use some linear algebra. We will show that we have a bijection $\Gamma/D \xrightarrow{\sim} \Theta$ by showing that

$$\Theta = \{\pi_0, \ldots, \pi_{\frac{g}{d}-1}, \iota\pi_0, \ldots, \iota\pi_{\frac{g}{d}-1}\},$$

where $\pi_i := \pi(\varphi_{di})$. Note that Corollary 4.4.6 and our ordering on the τ_i imply that these elements cover $\Theta = \pi(\Phi)$, but it is for the moment not clear that they are distinct.

Consider now the composite map

$$A\colon \mathbb{Z}[\Gamma/D] \longrightarrow X^*(L^\Theta) \longrightarrow W^K(p^\infty) \longrightarrow \mathbb{Z}[\Gamma/D],$$

where the first map is defined using the function $\Gamma/D \to \Theta$, $[\tau_{di}] \mapsto \pi_i$. By Lemma 4.4.5, A sends $[\tau_{di}]^*$ to the function

$$[\tau_{dj}]^* \longmapsto f_{\pi_i}(\tau_j w_K) = \sum_{\tau w_K = \tau_j w_K} \varphi_{di}(\tau).$$

Recalling the definition of φ_i, we see that we get a contribution of 1 to this sum for every $\tau = \iota^\varepsilon \tau_k \in \tau_j D$ such that either $\varepsilon = 0$ and $k = di$, or $\varepsilon = 1$ and $k \neq di$. In other words, A is given by a matrix, and the i^{th} entry of the j^{th} row is

$$A_{ji} = A([\tau_{di}]^*)([\iota^\varepsilon \tau_{dj}]^*) = \begin{cases} 0 & \varepsilon = 0 \text{ and } i \neq j; \\ 1 & \varepsilon = 0 \text{ and } i = j; \\ d-1 & \varepsilon = 1 \text{ and } i = j; \\ d & \varepsilon = 1 \text{ and } i \neq j. \end{cases}$$

The Γ-equivariance gives a similar result for the columns $A([\iota\tau_{di}]^*)$. Thus, with respect to the basis $\{[\tau_0]^*, [\tau_d]^*, \dots, [\tau_{g-d}]^*, [\iota\tau_0]^*, [\iota\tau_d]^*, \dots, [\iota\tau_{g-d}]^*\}$, the matrix A looks as follows:

$$A = \begin{pmatrix} I_{\frac{g}{d}} & dE_{\frac{g}{d}} - I_{\frac{g}{d}} \\ dE_{\frac{g}{d}} - I_{\frac{g}{d}} & I_{\frac{g}{d}} \end{pmatrix}$$

where E_n denotes the $n \times n$ matrix all of whose entries are 1.

We can now conclude first of all that $\Gamma/D \to \Theta$ is a bijection. Indeed, the fact that the columns of A are pairwise distinct means that the elements of Θ all represent different elements in $W^K(p^\infty)$. This is the point where we need the assumption on K that $d > 2$.

Next, we consider the kernel of A. Using elementary row operations, we reduce it to

$$A' = \begin{pmatrix} I_{\frac{g}{d}} & dE_{\frac{g}{d}} - I_{\frac{g}{d}} \\ 0 & M \end{pmatrix}, \qquad M = \begin{pmatrix} (2-g)d & (2-g)d & \cdots & (2-g)d \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Thus, one easily checks that

$$\ker(A) = \ker(A') = \left\{ \sum a_i[\tau_{di}]^* + b_i[\iota\tau_{di}]^* \mid \sum a_i = 0 \text{ and } a_i = b_i \ \forall i \right\}.$$

But the first map in the composition defining A was

$$\mathbb{Z}[\Gamma/D] \xrightarrow{\sim} \mathbb{Z}[\Theta] \twoheadrightarrow X^*(L^\Theta) = \frac{\{f : \Theta \to \mathbb{Z}\}}{\{f \mid f = f\iota \text{ and } \sum_{\alpha\in\Theta} f(\alpha) = 0\}},$$

so the kernel of this map is precisely the kernel of A. Hence $X^*(L^\Theta) \to X^*(P^K)$ is injective, as claimed. □

Lemma 4.4.9. In the commutative diagram below, the outer square is almost cartesian.

$$\begin{tikzcd}
X^*(T^\Phi) \oplus X^*(T^{\bar\Phi}) \arrow[r] \arrow[d] & \mathbb{Z}[\Gamma]\varphi_0 \oplus \mathbb{Z}[\Gamma]\bar\varphi \arrow[r] \arrow[d, "\gamma"] & X^*(S^K) \arrow[d, "\delta"] \\
X^*(L^{\pi(\Phi)}) \oplus X^*(L^{\pi(\bar\Phi)}) \arrow[r] & \mathbb{Z}[\Gamma/D]\pi_0 \oplus \mathbb{Z}[\Gamma/D]\bar\pi \arrow[r] & W^K(p^\infty)
\end{tikzcd}$$

Proof. The previous lemma implies that the left-hand square is a direct sum of almost cartesian squares, since the kernel of the bottom map is zero. It remains to show that the right-hand square is almost cartesian. By Lemma 4.4.7, the top right map is surjective; hence so is the bottom right map. We will show that the map of kernels $\ker(\gamma) \to \ker(\delta)$ is surjective.

Suppose $\sum a_i\varphi_i + a\bar\varphi \in \ker(\delta)$. Then $\sum a_i\pi(\varphi_i) + a\bar\pi = 0$. Note however that the elements $\{\pi_1, \dots, \pi_{\frac{g}{d}-1}, \bar\pi\}$ are $\mathbb{Z}$-linearly independent, since their images in $\mathbb{Z}[\Gamma/D]$ are: with notation from the previous proof, the column vector representing f_{π_i} is the only one with a non-zero entry (namely 1) in the i^{th} entry, and $f_{\bar\pi}$ has as j^{th} entry a zero for $0 \le j \le \frac{g}{d} - 1$ and a d for $\frac{g}{d} \le j \le \frac{2g}{d} - 1$.

Since $\pi(\varphi_i) = \pi_{[i/d]d}$, we obtain from this that $a = 0$ and

$$\sum_{j=0}^{d-1} a_{di+j} = 0, \qquad i = 0, \ldots, \frac{g}{d} - 1.$$

But this means exactly that $\sum a_i\varphi_i + a\bar{\varphi} \in \ker(\gamma)$, as we wanted. □

Corollary 4.4.10. The square

$$\begin{tikzcd}
X^*(T^K) \arrow[r] \arrow[d] & X^*(S^K) \arrow[d] \\
X^*(L^K) \arrow[r] & W^K(p^\infty)
\end{tikzcd}$$

is almost cartesian.

Proof. Let $I = \{\Gamma\text{-orbits of CM-types on } K\}$ and let $I' = \{\Gamma\text{-orbits of weight one Weil numbers in } K\}$. The outer rectangle in the diagram

$$\begin{tikzcd}
\bigoplus_{\Phi\in I} X^*(T^\Phi) \arrow[r] \arrow[d, "\alpha"] & X^*(T^K) \arrow[r] \arrow[d, "\beta"] & X^*(S^K) \arrow[d, "\delta"] \\
\bigoplus_{\Theta\in I'} X^*(L^\Theta) \arrow[r] & X^*(L^K) \arrow[r] & W^K(p^\infty)
\end{tikzcd}$$

is almost cartesian, by Lemma 4.4.9 and the fact from Honda-Tate theory that any isogeny class over $\mathbb{F}$ lifts to an abelian variety over $\overline{\mathbb{Q}}$. Hence $\ker\alpha \twoheadrightarrow \ker\delta$, so $\ker\beta \twoheadrightarrow \ker\delta$ is surjective too. □

This completes the proof of Theorem 4.1.3.

4.5 Proof of the main theorem

Theorem 4.1.1 now follows from the following two statements:

Proposition 4.5.1. If the Hodge conjecture holds for abelian varieties of CM type over $\mathbb{C}$, then $P = M$.

Proof. If the Hodge conjecture holds, we have Proposition 4.2.3 and can hence deduce Theorem 4.1.3. The existence of the square

$$\begin{tikzcd}
T & S \arrow[l, hook'] \\
L \arrow[u, hook] & M \arrow[l, hook'] \arrow[u, hook]
\end{tikzcd}$$

implies that $M \subseteq S \cap L = P$. On the other hand, $P \hookrightarrow M$ (Proposition 3.3.17), so $P = M$. □

Theorem 4.5.2. The following are equivalent:

1) The Tate conjecture holds for abelian varieties over the algebraic closure of a finite field.

2) $P = M$.

Proof. 1) $\Longrightarrow$ 2): This is [Mil94, Prop. 2.38]. The idea is as follows: suppose the Tate conjecture (0.0.1) holds. Then numerical equivalence equals l-adic homological equivalence, by definition of $\sim_{\text{hom}}$. Hence we obtain an l-adic fibre functor $\omega_l : \mathsf{Mot}_{\text{num}}(\mathbb{F})$, which one can exploit to deduce that the simple motives are all of rank one, and are classified by $W(p^\infty)$. In conjunction with the fact that $\mathsf{Mot}_{\text{num}}(\mathbb{F})$ is semisimple (Jannsen's theorem), this implies that M is of multiplicative type and $X^*(M) = W(p^\infty)$, i.e. $P = M$.

2) $\Longrightarrow$ 1): Suppose that $P = M$. We first show that then numerical equivalence equals l-adic homological equivalence. To do this, consider the category $\mathsf{Mot}_{\text{hom}}(\mathbb{F})_l$ of motives whose correspondences are the graded pieces of $\text{CH}^\bullet_{\text{hom}}(X \times Y)_{\mathbb{Q}_l}$ (cf. 3.3.1). Then there is a natural functor

$$F : \mathsf{Mot}_{\text{hom}}(\mathbb{F})_l \longrightarrow \mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \mathbb{Q}_l \tag{4.3}$$

which is the identity on objects, and is defined on morphisms via the composition

$$(\text{CH}^\bullet(X) \otimes \mathbb{Q}_l)/\sim_{\text{hom}} \twoheadrightarrow (\text{CH}^\bullet(X) \otimes \mathbb{Q}_l)/\sim_{\text{num}} \xrightarrow{\sim} \text{CH}^\bullet_{\text{num}}(X) \otimes \mathbb{Q}_l;$$

here the last isomorphism follows from [And04, Prop. 3.2.7.1]. We are using here that the categories $\mathsf{Mot}_{\text{num}}(\mathbb{F})_l$ and $\mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \mathbb{Q}_l$ are equivalent, which follows from the above isomorphism, the fact that both categories are semisimple, and that $\mathsf{Mot}_{\text{num}}(\mathbb{F})_l$ is generated by the motives of abelian varieties; cf. [Sta08, Prop. 1.1.4].

We will show that the functor F from (4.3) is faithful. Note that this suffices: it would imply that for any abelian variety A and integer r, the quotient map

$$(\mathbb{Q}_l \otimes \text{CH}^r(A))/\sim_{\text{hom}} \longrightarrow (\mathbb{Q}_l \otimes \text{CH}^r(A))/\sim_{\text{num}}$$

is injective. Thus if $\alpha \in \text{CH}^r(X)$ is numerically equivalent to zero, then so is $1 \otimes \alpha \in \mathbb{Q}_l \otimes \text{CH}^r(X)$, so $1 \otimes \alpha$ is homologically equivalent to zero, which means $1 \cdot \text{cl}^r(\alpha) = 0$.

Because of the diagram

$$\begin{tikzcd}
\text{Hom}(X, Y) \arrow[r, hook] \arrow[d] & \text{End}(X \times Y) \arrow[d] \\
\text{Hom}(F(X), F(Y)) \arrow[r, hook] & \text{End}(F(X \times Y))
\end{tikzcd}$$

we may reduce to endomorphism rings. Let $X \in \mathsf{Mot}_{\text{hom}}(\mathbb{F})_l$. Since the l-adic realisation functor is faithful and the Frobenius endomorphism commutes with correspondences, we have

$$\dim_{\mathbb{Q}_l} \text{End}(X) \leq \dim_{\mathbb{Q}_l} \text{End}_{\mathbb{Q}_l[\pi_X]}(\omega_l(X)).$$

As we saw in Lemma 2.3.3, we may compute the dimension of the right-hand side via the formula

$$\dim_{\mathbb{Q}_l} \text{End}_{\mathbb{Q}_l[\pi_X]}(\omega_l(X)) = \sum_P a(P)^2 \deg(P) =: r(\pi_X),$$

where $\prod_P P^{a(P)}$ is the decomposition of the characteristic polynomial of π_X into irreducible factors (cf. Remark 3.1.16). Here we use semisimplicity of the Frobenius action.

Now suppose Y is a motive in $\mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \mathbb{Q}_l$, and consider the composition

$$\mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \mathbb{Q}_l \longrightarrow \mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \overline{\mathbb{Q}}_l \xrightarrow{\omega} \mathsf{Vec}_{\overline{\mathbb{Q}}_l},$$

where ω was our abstract fibre functor. Then

$$\overline{\mathbb{Q}}_l \otimes \operatorname{End}(Y) \cong \operatorname{End}_{\overline{\mathbb{Q}}_l}(\omega(Y))^M.$$

If $P = M$, the right-hand side is the space fixed by the Frobenius endomorphism of Y, or more precisely, the class of the Frobenius endomorphism of a model of Y. By Proposition 3.3.14, Frobenius again acts semisimply, so the dimension of this space equals $r(\pi_Y)$.

Now let $X \in \mathsf{Mot}_{\text{hom}}(\mathbb{F})_l$, and let $F(X)$ be its image in $\mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \mathbb{Q}_l$. The above shows that

$$r(\pi_{F(X)}) = \dim_{\overline{\mathbb{Q}}_l} \operatorname{End}(F(X)) \leq \dim_{\mathbb{Q}_l} \operatorname{End}(X) \leq r(\pi_X),$$

but $r(\pi_{F(X)}) = r(\pi_X)$ because the characteristic polynomials of X and $F(X)$ are equal. Hence equality holds, so we conclude that $\sim_{\text{hom}} = \sim_{\text{num}}$.

Since $\sim_{\text{num}} = \sim_{\text{hom}}$, we get an l-adic realisation functor $\omega_l : \mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \overline{\mathbb{Q}}_l \to \mathsf{Vec}_{\overline{\mathbb{Q}}_l}$, and a commutative diagram

$$\begin{tikzcd}
\mathsf{Mot}_{\text{num}}(\mathbb{F}) \otimes \overline{\mathbb{Q}}_l \arrow[r] \arrow[dr] & \mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P) \arrow[d] \\
& \mathsf{Vec}_{\overline{\mathbb{Q}}_l}
\end{tikzcd}$$

where now the horizontal functor is defined by sending a motive X to the class of representations $[(\omega_l(X), \omega_l(\pi_X))]$. Since P and M depend on their fibre functors only up to an isomorphism, we still have $P = M$ under the map $P \to M$ induced by this diagram. In particular, a motive is fixed by M if and only if its image in $\mathsf{Rep}_{\overline{\mathbb{Q}}_l}(P)$ is fixed by P. Now for any object X in a Tannakian category $\mathcal{T}$, the largest subobject of X fixed by $\pi_1(\mathcal{T})$ is isomorphic to $\mathbb{1} \otimes \operatorname{Hom}(\mathbb{1}, X)$. In particular, we obtain for every $r \in \mathbb{Z}$ and every abelian variety $X/\mathbb{F}$,

$$\begin{aligned}
\overline{\mathbb{Q}}_l \otimes \mathrm{CH}^r_{\text{num}}(X) = \operatorname{Hom}(\mathbb{1}, hX(r)) &\cong (hX(r))^M \\
&\cong [(H^\bullet(X, \overline{\mathbb{Q}}_l(r)), \pi_{X_q(r)})]^P \\
&\cong \bigcup_{X_q/\mathbb{F}_q} H^{2r}(X, \overline{\mathbb{Q}}_l(r))^{\operatorname{Gal}(\mathbb{F}_q)}.
\end{aligned}$$

The last isomorphism holds because the space fixed by P is the largest subspace of $H^\bullet(X, \overline{\mathbb{Q}}_l(r))$ which becomes a trivial subrepresentation in the colimit; that is, the space of elements fixed by some power of Frobenius. Equivalently, the Frobenius of some finite base extension acts trivially, which is the same as the Galois-theoretic Frobenius acting trivially. The twist by r ensures that this space is contained in $H^{2r}(X, \overline{\mathbb{Q}}_l(r))$: indeed, $\pi_{X_q(r)} = \pi_{X_q} \otimes \pi_{\mathbb{L}}^{-r}$ acts on $H^n(X, \overline{\mathbb{Q}}_l) \otimes \overline{\mathbb{Q}}_l(r)$ through some Weil q^n-number on the first factor, and through q^{-r} on the second factor. Of course this yields a trivial action if and only if π_{X_q} acts by q^r, which in particular forces $n = 2r$.

To conclude, we showed that the cycle class map

$$\mathbb{Q}_l \otimes \mathrm{CH}^r_{\mathrm{num}}(X) \longrightarrow \bigcup_{X_q/\mathbb{F}_q} H^{2r}(X, \mathbb{Q}_l(r))^{\mathrm{Gal}(\mathbb{F}_q)} \tag{4.4}$$

is an isomorphism after tensoring with $\overline{\mathbb{Q}}_l$. Since this is faithfully flat over $\mathbb{Q}_l$, (4.4) was an isomorphism already. Thus the Tate conjecture holds for abelian varieties over $\mathbb{F}$. □

Bibliography

[And04] Yves André. *Une Introduction aux Motifs*, volume 17 of *Panoramas et Synthèses.* Société Mathématique de France, 2004.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models.* A Series of Modern Surveys in Mathematics. Springer-Verlag, first edition, 1990.

[Cha13] François Charles. The Tate conjecture for K3 surfaces over finite fields. *Inventiones Mathematicae*, 194:119–145, 2013.

[Del] Pierre Deligne. Letter to A. Viascu on November 30, 2011. Available at `https://publications.ias.edu/book/export/html/2582`.

[Del90] Pierre Deligne. Catégories tannakiennes. *Progress in Mathematics*, 87:111–195, 1990. The Grothendieck Festschrift II, A Collection of Articles in honor of the 60$^{\text{th}}$ birthday of Alexander Grothendieck.

[DM82] Pierre Deligne and James S. Milne. Hodge cycles on abelian varieties, 1982. Available at `www.jmilne.org/math/`.

[DM18] Pierre Deligne and James S. Milne. Tannakian categories, 2018. Available at www.jmilne.org/math/.

[EvdGM] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. *Abelian Varieties.* not yet published. Preliminary version available at `http://van-der-geer.nl/~gerard/AV.pdf`.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones Mathematicae*, 73(3):349–366, 1983.

[FGI$^+$00] Barbara Fantechi, Lothar Göttsche, Luc Illusie, Steven L. Kleiman, Nitin Nitsure, and Angelo Vistoli. *Fundamental Algebraic Geometry: Grothendieck's FGA Explained*, volume 123 of *Mathematical Surveys and Monographs.* American Mathematical Society, 2000.

[Ful98] William Fulton. *Intersection Theory.* Springer-Verlag, second edition, 1998.

[GS06] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*, volume 101 of *Cambridge studies in advanced mathematics.* Cambridge University Press, 2006.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1977.

[Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20,1-2:83–95, 1968.

[Jan92] Uwe Jannsen. Motives, numerical equivalence, and semi-simplicity. *Inventiones mathematicae*, 107:447–452, 1992.

[Jav10] Ariyan Javanpeykar. The Grothendieck-Riemann-Roch theorem, with an application to covers of varieties. Master's thesis, 2010. Available from `https://www.math.leidenuniv.nl/scripties/MasterJavanpeykar.pdf`.

[Kü93] Klaus Künnemann. A Lefschetz decomposition for Chow motives of abelian schemes. *Inventiones Mathematicae*, 113:85–102, 1993.

[Kle70] Steven L. Kleiman. Motives. In Frans Oort, editor, *Algebraic Geometry, Oslo 1970*, Proceedings of the 5th Nordic Summer-School in Mathematics, pages 53–82. Wolters-Noordhoff, 1970.

[KM74] Nicholas Michael Katz and William Messing. Some consequences of the Riemann hypothesis for varieties over finite fields. *Inventiones Mathematicae*, 23:73–77, 1974.

[KMP16] Wansu Kim and Keerthi Madapusi Pera. 2-adic integral canonical models. *Forum Math. Sigma*, 4:e28, 2016.

[Leo17] Marius Leonhardt. The main theorems of complex multiplication, 2017. Essay submitted for the Smith-Knight & Rayleigh-Knight Prizes 2017.

[Lic10] Sam Lichtenstein. Tate's isogeny theorem for abelian varieties over finite fields, 2010. Notes from a Number Theory learning seminar at Stanford.

[Mil94] James S. Milne. Motives over finite fields. In Uwe Jannsen, Steven Kleiman, and Jean-Pierre Serre, editors, *Motives*, Proc. Symp Pure Math. 55, pages 401–459. AMS, 1994.

[Mil99a] James S. Milne. Lefschetz classes on abelian varieties. *Duke Math. J.*, 96:3:639–675, 1999. Available at `www.jmilne.org/math/`.

[Mil99b] James S. Milne. Lefschetz motives and the tate conjecture. *Compositio Math.*, 117:47–81, 1999. Available at `www.jmilne.org/math/`.

[Mil15a] James S. Milne. Algebraic groups (v2.00), 2015. Available at `www.jmilne.org/math/`.

[Mil15b] James S. Milne. Divisors and intersection theory, 2015. Available at `www.jmilne.org/math/`.

[Mil19] James S. Milne. On the Tate and standard conjectures over finite fields, 2019. Available at `www.jmilne.org/math/`.

[Mil20] James S. Milne. Complex multiplication, 2020. Available at `www.jmilne.org/math/CourseNotes/`.

[MM65] John Willard Milnor and John Coleman Moore. On the structure of Hopf algebras. *Annals of Mathematics*, 81, no.2:211–264, 1965.

[Moo19] Ben Moonen. A remark on the Tate conjecture. *Journal of Algebraic Geometry*, 28:559–603, 2019.

[MP15] Keerthi Madapusi Pera. The Tate conjecture for K3 surfaces in odd characteristic. *Inventiones Mathematicae*, 201:625–668, 2015.

[Mum74] David Mumford. *Abelian Varieties.* Tata Institute of Fundamental Research, Bombay, second edition, 1974.

[Oor] Frans Oort. Abelian varieties over finite fields. Lectures at the summer school "Higher-dimensional varieties over finite fields" in Göttingen, June 2007.

[Rio06] Joël Riou. Realizations functors, 2006. Written version of a lecture at the summer school *Motives and related topics* at the I.H.É.S.

[Sch94] Anthony J. Scholl. Classical motives. In Uwe Jannsen, Steven Kleiman, and Jean-Pierre Serre, editors, *Motives*, Proc. Symp Pure Math. 55, pages 163–187. AMS, 1994.

[SD74] Henry Peter Francis Swinnerton-Dyer. *Analytic Theory of Abelian Varieties*, volume 14 of *London Mathematical Society Lecture Notes.* Cambridge University Press, Cambridge, 1974.

[Ser65] Jean-Pierre Serre. Zeta and L functions. *Arithmetical algebraic geometry*, pages 82–92, 1965. Proceedings of a conference held at Purdue University, December 5-7, 1963.

[Sou84] Christophe Soulé. Groupes de chow et K-théorie de variétés sur un corps fini. *Mathematische Annalen*, 268:317–345, 1984.

[ST61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan.* Tokyo, 1961.

[ST68] Jean-Pierre Serre and John Torrence Tate. Good reduction of abelian varieties. *The Annals of Mathematics*, 88:492–517, 1968.

[Sta08] Nicolas Stalder. Scalar extension of abelian and Tannakian categories, 2008. Preprint, available from: `https://arxiv.org/abs/0806.0308`.

[Sti09] Jakob Stix. A course on finite flat group schemes and p-divisible groups, 2009. Lecture notes, available from: `https://www.uni-frankfurt.de/52288632/Stix_finflat_Grpschemes.pdf`.

[Tat65] John Torrence Tate. Algebraic cycles and poles of zeta functions. *Arithmetical algebraic geometry*, pages 93–110, 1965. Proceedings of a conference held at Purdue University, December 5-7, 1963.

[Tat66] John Torrence Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones math.*, 2:134–144, 1966.

[Vak17] Ravi Vakil. *The Rising Sea.* 2017. Draft, available from: `http://math.stanford.edu/~vakil/216blog/`.

[Zar75] Yuri G. Zarhin. Endomorphisms of abelian varieties over fields of finite characteristic. *Math. USSR Izvestija*, 9(2):255–260, 1975.