# Abelian varieties over finite fields

Frans Oort

March 2005

**Preliminary version**
**Gael: Luminy 21 - 25 March 2005**

## Introduction

We could try to classify *isomorphism classes of abelian varieties*. The theory of moduli spaces of polarized abelian varieties answers this question completely. This is a geometric theory. However it is sometimes not so easy to exhibit explicit examples.

A coarser classification is that of studying *isogeny classes of abelian varieties*. A wonderful and powerful theorem, the Honda-Serre-Tate theory gives a complete classification of isogeny classes of abelian varieties over a finite field, see (1.1). The idea is that for an abelian variety $A$ over $K = \mathbb{F}_q$ the assignment $A \mapsto \pi_A$ which associates to $A$ its geometric Frobenius $\pi_A$ identifies the isogeny class of $A$ with the conjugacy class of the algebraic integer $\pi_A$, and conversely such an algebraic integer, a $q$-Weil number, determines an isogeny class: geometric objects can be classified by a simple algebraic invariant. This arithmetic theory gives access to a lot of wonderful theorems. In these notes we describe this theory, we give some examples, applications and some open questions.

We use to write $K$ for an arbitrary field, and $k$ for an algebraically closed field. We write $g$ for the dimension of an abelian variety, unless otherwise stated. We write $p$ for a prime number; we write $\ell$ for a prime number, which usually is different from the characteristic of the base field. We write $m = \overline{\mathbb{F}_p}$; sometimes we also use $m$ for an integer; we hope this does not cause any confusion.

Instead of reading these notes it is much better to read [52]. Some proofs have been worked out in more detail in [53].

Recommended reading:
Abelian varieties: [28], [22], [6] Chapter V.
Honda-Serre-Tate theory: [52], [16], [53].
Abelian varieties over finite fields: [51], [54], [55].
Group schemes: [45], [34].
Endomorphism rings and endomorphism algebras: [51], [39], [54].

# 1 Main topic

Below we will define:
(1) An abelian variety and an isogeny between abelian varieties, see (3.1).
(2) A $q$-Weil number, here $q = p^a$, see (2.1).
(3) We remind the reader of the fact that for a simple abelian variety $A$ over $K = \mathbb{F}_q$ the geometric Frobenius $\pi_A : A \to A$ is a $q$-Weil number, see (5.4).
(4) We will see that for simple abelian varieties $A$ and $B$ over finite fields their Weil numbers $\pi_A$ respectively $\pi_B$ are conjugated, see (2.1), if and only if $A \sim B$.
(5) Thus we obtain a map $A \mapsto \pi_A$ defined on K-isogeny classes. Using these notions we have:

**(1.1) Theorem** (Honda, Serre and Tate). *Fix a finite field $K = \mathbb{F}_q$. The assignment $A \mapsto \pi_A$ induces a bijection from the set of $K$-isogeny classes of $K$-simple abelian varieties defined over $K$ and the set of conjugacy classes of $q$-Weil numbers.*
See [52].

This will be the main topic of these talks. On the road to these notions we will encounter various notions and results, which will be exposed below (sometimes in greater generality than strictly necessary to understand this beautiful theorem).

# 2 Weil numbers and CM-fields

**(2.1) Definition.** *Let $p$ be a prime number, $a \in \mathbb{Z}_{>0}$; write $q = p^a$. A $q$-Weil number is an algebraic integer $\pi$ such that for every embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have*

$$| \psi(\pi) | \quad = \quad \sqrt{q}.$$

We say that $\pi$ and $\pi'$ are *conjugated* if there exists an isomorphism $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ mapping $\pi$ to $\pi'$.
**Notation:** $\pi \quad \sim \quad \pi'$. We write $W(q)$ for the set conjugacy classes of $q$-Weil numbers.

**(2.2) Definition.** *A field $L$ is said to be a* CM*-field if $L$ is a finite extension of $\mathbb{Q}$* (hence $L$ is a number field), *there is a subfield $L_0 \subset L$ such that $L_0/\mathbb{Q}$ is totally real* (i.e. every $\psi_0 : L_0 \to \mathbb{C}$ gives $\psi_0(L_0) \subset \mathbb{R}$) *and $L/L_0$ is quadratic totally imaginary* (i.e. $[L : L_0] = 2$ and for every $\psi : L \to \mathbb{C}$ we have $\psi(L) \not\subset \mathbb{R}$).
**Remark.** The quadratic extension $L/L_0$ gives an involution $\iota \in \mathrm{Aut}(L/L_0)$. For every embedding $\psi : L \to \mathbb{C}$ this involution corresponds with the restriction of complex conjugation on $\mathbb{C}$ to $\psi(L)$.

**(2.3) Proposition.** *Let $\pi$ be a $q$-Weil number. Then*
**(I)** *either for at least one $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \in \mathbb{R}$; in this case we have:*
**(Ie)** *$a$ is even, $\sqrt{q} \in \mathbb{Q}$, and $\pi = +p^{a/2}$, or $\pi = -p^{a/2}$; or*
**(Io)** *$a$ is odd, $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$, and $\psi(\pi) = \pm p^{a/2}$. In particular in case* (I) *we have $\psi(\pi) \in \mathbb{R}$ for every $\psi$.*
**(II)** *Or for every $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \notin \mathbb{R}$* (equivalently: for at least one $\psi$ we have $\psi(\pi) \notin \mathbb{R}$). *In case* (II) *the field $\mathbb{Q}(\pi)$ is a* CM*-field.*
**Proof.** The claims in (I) follow form the fact that $\pm p^{a/2}$ are precisely those numbers with absolute value equal to $\sqrt{q}$.

If at least one embedding $\psi$ gives $\psi(\pi) \notin \mathbb{R}$, then we are not in case (I), hence all embeddings have this property. Then

$$\psi(\pi)\cdot\overline{\psi(\pi)} = q = \psi(\pi)\cdot\frac{q}{\psi(\pi)}.$$

Hence

$$\overline{\psi(\pi)} = \frac{q}{\psi(\pi)}.$$

This shows that

$$\beta := \pi + \frac{q}{\pi}$$

is totally real. Hence $L_0 := \mathbb{Q}(\beta)$ is totally real. We are in the case that $\psi(\pi) \notin \mathbb{R}$ for every $\psi$; hence $L/L_0$ is totally complex. □

**(2.4) Remark.** We see a characterization of $q$-Weil numbers:

$$\beta := \pi + \frac{q}{\pi} \quad \text{is totally real,}$$

and $\pi$ is a zero of

$$T^2 - \beta\cdot T + q, \quad \text{with} \quad \beta < 2\sqrt{q}.$$

In this way it is easy to construct $q$-Weil numbers, see Section 17.

# 3 Abelian varieties

For the theory of Abelian varieties we refer to [28], or to [6], Chapter V.

**(3.1) Definition.** Let $K$ be a field. An abelian variety $A$ over $K$ is a complete, absolutely irreducible group variety over $K$.
This implies that $A$ is a commutative group variety. However this was not the origin of the name. Abelian integrals on a Riemann surface have values well-defined up to periods; these values modulo periods, and in an abelian variety, only depend on beginning and end point; this gave the name.

*An isogeny $\varphi : A \to B$ between abelian varieties is a surjective homomorphism between abelian varieties of the same dimension.* Notation: $A \sim B$, or $A \sim_K B$ if we want to stress that we consider a $K$-isogeny between abelian varieties over $K$.

The kernel of an isogeny is a finite group scheme. If the degree of $\varphi$ equals $n$, then $\mathrm{Ker}(\varphi)$ is contained in the kernel of multiplication by $n$ on $A$. From this we deduce that isogeny between abelian varieties over a given field is *an equivalence relation.*

**(3.2) Exercise.** Let $A$ and $B$ be abelian varieties over a field $K$. Let $\varphi : A \to B$ be an isogeny. Show there exist an integer $N$ and an isogeny $\psi : B \to A$ such that $\psi\cdot\varphi = N\cdot 1_A$; show that $\varphi\cdot\psi = N\cdot 1_B$ in this case; show that $x \mapsto (\psi\cdot x\cdot\varphi)/N$ gives an isomorphism $\mathrm{End}^0(A) \to \mathrm{End}^0(B)$.

**(3.3) Notation.** *Let $G$ be an abelian group, additively written. Let $n \in \mathbb{Z}_{>0}$. We write $G[n]$ for the set of all elements $g \in G$ such that $n \cdot g = 0$.* Note that $G[n] \subset G$ is a subgroup.

Let $G \to S$ be a commutative group scheme. Let $n \in \mathbb{Z}_{>0}$. The fiber product of the diagram

$$G \xrightarrow{n} G \xleftarrow{0} S \quad \text{is denoted by} \quad S \leftarrow G[n] \subset G.$$

Note that $G[n] \subset G$ is a subgroup scheme.
Be careful! Say, $G$ is a commutative group scheme over a field $K$. In general one should not identify $G[n] \subset G$ with the set of rational points $G[n](K) \subset G(K)$.
**Exercise.** Describe $G[n]$ and $G[n](k)$ in case $G = \mathbb{G}_m$ (the multiplicative linear group) in case $n = 2$, or $n = 3$, and $K \in \{\mathbb{Q}, \mathbb{C}, \mathbb{F}_2, \overline{\mathbb{F}_2}\}$.

Let $N$ be a finite group scheme over a field $K$ suppose that as a scheme, $N \to \mathrm{Spec}(K)$ is étale. We can consider the $\mathrm{Gal}(K^s/K)$-module $N(K^s)$. Here $K^s$ stands for the separable closure of $K$.

**(3.4) Fact.** *The assignment $N \mapsto N(K^s)$ is an equivalence between* (finite group schemes over $K$) *and* (finite groups, with a continuous $\mathrm{Gal}(K^s/K)$-action).
**Exercise.** Prove this fact.

**(3.5) Simple abelian varieties.** A non-zero abelian variety $A$ over a field $K$ is called *simple* (or $K$-simple if confusion could occur) if for every abelian subvariety $B \subset A$ (over $K$) we have either $0 = B$ or $B = A$. We say $A$ is *absolutely simple* if $A \otimes \overline{K}$ is simple.
**Exercise.** *Choose a field $K$ and an abelian variety $A$ over $K$ which is simple but not absolutely simple.*

**Fact.** *For an abelian variety $A$ over a field $K$ the endomorphism ring* $\mathrm{End}(A)$ *has no torsion, and its rank over $\mathbb{Z}$ is finite.*

*The endomorphism algebra* $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a semi-simple algebra, finite-dimensional over $\mathbb{Q}$.*

*For every simple abelian variety $A$ over a field $K$ the endomorphism algebra* $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a division algebra of finite rank over $\mathbb{Q}$,* see [28], Cor. 3 on page 178.

**(3.6) Notation.** Let $A$ be a non-zero abelian variety over a field $K$. An isogeny

$$A \quad \sim \quad \prod_{1 \le i \le r} A_i^{\mu_i},$$

is called a *primary isogeny decomposition* if:

- $\mu_i \in \mathbb{Z}_{>0}$;
- for every $1 \le i \le r$ the abelian variety $A_i$ is simple;
- for $1 \le i < j \le r$ the abelian varieties $A_i$ and $A_j$ are non-isogenous.

*The Poincaré-Weil theorem says that every abelian variety over a field admits a primary isogeny decomposition.*

**(3.7)** For the definition of a polarization see [28]; [27], 6.2. A divisor $D$ on an abelian variety $A$ defines a homomorphism $\phi_D : A \to A^t$; in case this divisor is ample $\phi_D$ is an isogeny, and is called a *polarization*. In case this polarization is an isomorphism, we say it is a *principal polarization*. A polarization $\phi$ on $A$ defines an anti-involution $\iota$ on $\mathrm{End}^0(A)$ by $\iota(x) := \phi^{-1} \cdot x^t \cdot \phi$. we say we have a *principal polarization* if $\iota : \mathrm{End}(A) \to \mathrm{End}(A)$ is an isomorphism.

**(3.8) Duality for finite group schemes.** For a finite, locally free, *commutative* group scheme $N \to S$ there is a dual group scheme, denoted by $N^D$, called the Cartier dual of $N$; for $N = \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ we take $B^D := \mathrm{Hom}_A(B, A)$, and show that $N^D := \mathrm{Spec}(B^D)$ exists and is a finite group scheme over $S$. See [34].

**(3.9) Duality** (Here not enough definitions are given...) For an abelian scheme $\mathcal{A} \to S$ we define $\mathcal{A}^t := \underline{\mathrm{Pic}}^0_{\mathcal{A}/S}$, the *dual abelian scheme*.

**Duality theorem.** *Let $S$ be a locally noetherian base scheme. Let $\varphi : A \to B$ be an isogeny of abelian schemes over $S$, with kernel $N = \mathrm{Ker}(\varphi)$. The exact sequence*

$$0 \quad \to \quad N \quad \longrightarrow \quad A \quad \xrightarrow{\varphi} \quad B \quad \to \quad 0$$

*gives rise to an exact sequence*

$$0 \quad \to \quad N^D \quad \longrightarrow \quad B^t \quad \xrightarrow{\varphi^t} \quad A^t \quad \to \quad 0.$$

See [34]. Theorem 19.1. For the definition of $N^D$, see (3.8).

**(3.10) The characteristic polynomial of an endomorphism.**

Let $A$ be an abelian variety over a field $K$ of $\dim(A) = g$, and and let $\varphi \in \mathrm{End}(A)$; then there exists a polynomial $f_A \in \mathbb{Z}[T]$ of degree $2g$ called *the characteristic polynomial of $\varphi$*; it has the property that for any $t \in \mathbb{Z}$ we have $f_A(\varphi - t) = \deg(\varphi - t)$; see [6] page 125. See (4.1) for the definition of $T_\ell(A)$; for every $\ell \neq \mathrm{char}(K)$ the polynomial $f_A$ is the characteristic polynomial of $T_\ell(\varphi) \in \mathrm{End}(T_\ell(A))$.

**(3.11) Exercise.** Let $K$ be a field, and $A$ an abelian variety over $K$ of dimension $g$. *Show there is a natural homomorphism*

$$\mathrm{End}(A) \to \mathrm{End}(\mathfrak{t}_A) \cong \mathrm{Mat}(K, g)$$

*by $\varphi \mapsto d\varphi$. If $\mathrm{char}(K) = 0$, show this map is injective.*

Let $E$ be an elliptic curve over $\mathbb{Q}$. *Show that* $\mathrm{End}(E) = \mathbb{Z}$. *Construct an elliptic curve $E$ over $\mathbb{Q}$ with* $\mathrm{End}(E) \subsetneqq \mathrm{End}(E) \otimes \mathbb{C}$.

**Remark.** There does exist an abelian variety $A$ over $\mathbb{Q}$ with $\mathbb{Z} \subsetneqq \mathrm{End}(A)$.

**(3.12) Exercise.** Show that over a field of characteristic $p$, the kernel of $\mathrm{End}(A) \to \mathrm{End}(\mathfrak{t}_A) \cong \mathrm{Mat}(K, g)$ can be bigger than $\mathrm{End}(A) \cdot p$.

# 4 Complex abelian varieties.

Suppose $K = \mathbb{C}$. Let $\mathfrak{t}_A$ be the tangent space; note that $\mathfrak{t}_A \cong \mathbb{C}^g$, where $g = \dim(A)$. The exponential map in the theory of complex commutative Lie groups gives a surjective homomorphism

$$\exp_A : \mathfrak{t}_A \quad \twoheadrightarrow \quad A(\mathbb{C}).$$

As $A$ is complete, we conclude that $A(\mathbb{C})$ is compact, see [29], Th. 2 on page I.10. Hence $\mathrm{Ker}(\exp_A) = \Lambda \subset \mathfrak{t}_A$ is a *lattice*. Conversely it is known under which circumstances a lattice $\Lambda \subset \mathbb{C}^g$ defines an abelian variety $A$ over $\mathbb{C}$ such that $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$; e.g. see [28], I.3; [22], 4.2.

**Fact.** *Let $A$ be an abelian variety over a field $K$; let $n \in \mathbb{Z}_{>0}$. Then $A[n]$ is a finite group scheme over $K$ of rank $n^{2g}$, where $g := \dim(A)$. If $n$ is not divisible by the characteristic of $K$ then $A[n]$ is étale over $K$. In this case $A[n](\overline{K} \cong (\mathbb{Z}/m)^{2g}$.*
**Exercise.** *Let $\mathrm{char}(K) = p$. Show that multiplication by $n$ induces the zero on $\mathfrak{t}_A$ if and only if $n$ is divisible by $p$.*

**(4.1) Tate-$\ell$-groups.** Let $A$ be an abelian variety over a field $K$. Let $\ell$ be a prime number not equal to $\mathrm{char}(K)$. Define

$$T_\ell(A) \quad := \quad \lim_{\infty \leftarrow i} \; A[\ell^i].$$

Discussion: This can be seen as an "pro-group scheme". One can also, equivalently, consider $\lim_{\infty \leftarrow i} \; A[\ell^i](\overline{K}) \cong (\mathbb{Z}_l)^{2g}$, and consider this as a continuous $\mathrm{Gal}(K^s/K)$-module.

**(4.2) Exercise.** *Use the exact sequence $\mathbb{C}^g/\Lambda = A(\mathbb{C})$, and show that for every $n \in \mathbb{Z}_{>0}$ there is a canonical isomorphism $A(\mathbb{C})[n] \xrightarrow{\sim} \Lambda/n{\cdot}\Lambda$.* (Hint: use the "snake lemma".)

# 5 Abelian varieties in positive characteristic

In this section all base fields have characteristic $p$. We only give some definitions and facts.

**(5.1) Frobenius.** For a scheme $S$ over $\mathbb{F}_p$ (i.e. $p{\cdot}1 = 0$ in all fibers of $\mathcal{O}_S$), we define the absolute Frobenius morphism $\mathrm{fr} : S \to S$; if $S = \mathrm{Spec}(R)$ this is given by $x \mapsto x^p$ in $R$.

For a scheme $A \to S$ we define $A^{(p)}$ as the fiber product of $A \to S \xleftarrow{\mathrm{fr}} S$. The morphism $\mathrm{fr} : A \to A$ factors through $A^{(p)}$. This defines $F_A : A \to A^{(p)}$, a morphism over $S$; this is called *the relative Frobenius morphism.* If $A$ is a group scheme over $S$, the morphism $F_A : A \to A^{(p)}$ is a homomorphism of group schemes. For more details see [45], Exp. VII$_A$.4. The notation $A^{(p/S)}$ is maybe more correct.

**Example.** Suppose $A \subset \mathbb{A}^n_R$ is given as the zero set of a polynomial $\sum_I a_I X^I$ (multi-index notation). Then $A^{(p)}$ is given by $\sum_I a_I^p X^I$, and $A \to A^p$ is given, on coordinates, by raising these to the power $p$. Note that if a point $(x_1, \cdots, x_n) \in A$ then indeed $(x_1^p, \cdots, x_n^p) \in A^{(p)}$, and $x_i \mapsto x_i^p$ describes $F_A : A \to A^{(p)}$ on points.

**(5.2)** Let $S = \mathrm{Spec}(\mathbb{F}_p)$; for any $T \to S$ we have a canonical isomorphism $T \cong T^{(p)}$. In this case $F_T = \mathrm{fr} : T \to T$.

**The geometric Frobenius.** Suppose $K = \mathbb{F}_q$, with $q = p^a$. There is a canonical isomorphism $A^{(q)} = A$. "Iterating" the relative Frobenius $a$ times we obtain

$$\text{" } (F_A)^a \text{ "} = F_{A^{(p^{a-1})}} \cdots F_{A^{(p)}} \cdot F_A = \pi_A : (A \longrightarrow A^{(p)} \longrightarrow \cdots \longrightarrow A^{(q)} = A),$$

which is a $K$-morphism. In case $A$ is an abelian variety this is an endomorphism $\pi_A \in \mathrm{End}(A)$, which is an isogeny of degree $q^{\dim(A)}$.

Suppose $A$ is simple. Then $\mathrm{End}^0(A)$ is a division algebra. Hence $\pi_A$ is of finite degree over $\mathbb{Q}$, and $\mathbb{Q}(\pi_A)$ is a number field.

**Exercise.** Let $A \sim B$ be an isogeny of simple abelian varieties over a finite field; this isogeny gives an isomorphism $\mathbb{Q}(\pi_A) \cong \mathbb{Q}(\pi_B)$, see (3.3). *Show that this maps $\pi_A$ tot $\pi_B$.*

**Remark.** If $A$ is simple over a finite field $K$, and $K \subset K'$ is a finite extension, write $A' := A \otimes_K K'$, then $\pi_{A'} \in \mathbb{Q}(\pi_A)$ and from the definition of the geometric Frobenius we see:

$$\pi_{A'} \quad = \quad \pi_A^{[K':K]}.$$

**(5.3) Exercise.** Let $E$ be an elliptic curve over $\mathbb{F}_p$. Show that $\mathbb{Z} \subsetneqq \mathrm{End}(E)$. *Show that $E$ admits smCM.*

**(5.4) Theorem** (Weil). *Let $A$ be a simple abelian variety over $K = \mathbb{F}_q$; consider the endomorphism $\pi_A \in \mathrm{End}(A)$. The algebraic number $\pi_A$ is a $q$-Weil number.*
See [56], page 70; [57], page 138; [28], Theorem 4 on page 206.

**(5.5) Verschiebung.** Let $A$ be a *commutative* group scheme over a characteristic $p$ base scheme. In [45], Exp. VII$_A$.4 we find the definition of the "relative Verschiebung"

$$V_A : A^{(p)} \to A; \quad \text{we have:} \quad F_A \cdot V_A = [p]_{A^{(p)}}, \quad V_A \cdot F_A = [p]_A.$$

In case $A$ is an abelian variety we see that $F_A$ is surjective, and $\mathrm{Ker}(F_A) \subset A[p]$. In this case we do not need the somewhat tricky construction of [45], Exp. VII$_A$.4, but we can define $V_A$ by $V_A \cdot F_A = [p]_A$ and check that $F_A \cdot V_A = [p]_{A^{(p)}}$.

**(5.6)** Suppose that $A$ is an abelian variety over $\mathbb{F}_q$. Then $\pi_A \in \mathrm{End}(A)$. Moreover the "$a$ times iteration of $V_A$" gives an endomorphism $\nu_A \in \mathrm{End}(A)$. We see that $\pi_A \cdot \nu_A = q = \nu_A \cdot \pi_A$. Moreover we see, in case $\pi_A$ is not real, but also in case (I), that we have for every embedding $\psi$:

$$\psi(\nu_A) \quad = \quad \overline{\psi(\pi_A)} \quad = \quad \frac{q}{\psi(\pi_A)}.$$

**(5.7) Definition.** Let $A$ be an abelian variety over $K$. We write $f(A) = f$ for the number which satisfies $A[p](\overline{K}) \cong \mathbb{Z}/p^f$. *This integer is called the $p$-rank of $A$.*

As is easily seen: We have $0 \leq f(A) \leq \dim(A)$; for an elliptic curve $E$ we have either $f(E) = 1$ (definition: $E$ is ordinary), or $f(E) = 0$ (definition: $E$ is supersingular). For every $g$ and every $0 \leq f(A) \leq g$ we can find an abelian variety of $p$-rank $f$ and dimension $g$.

**(5.8)** For an abelian variety $A$ and a prime number $p$ we define

$$X = A[p^\infty] := \cup_i \ \ X[p^i].$$

Note that the morphism $\times p : X[p^{i+1}] \to X[p^i]$ is an epimorphism.

A $p$-divisible group of height $h$ is an inductive system of finite commutative group schemes $G_i$ of rank $p^{hi}$, such that $(G_i \subset G_{i+1}) = G_{i+1}[p^i]$. We see that $A[p^\infty]$ is the $p$-divisible group associated with $A$ (this construction can also be given over for an abelian scheme over an arbitrary base). An isogeny $X \to Y$ between $p$-divisible groups is a surjective homomorphism with finite kernel.

**Exercise.** *Let $A$ be an abelian variety over a field $k$, let $\ell$ be a prime number different from* $\mathrm{char}(k)$. *Show that* $\cup_i X[\ell^i](k) \cong \mathbb{Q}_\ell/\mathbb{Z}_\ell$.
**Discussion.** Instead of $T_\ell(A)$ we could use $\cup_i X[\ell^i]$, and instead of $\cup_i X[p^i]$ we could use $\lim_{\leftarrow} X[p^i]$.

**(5.9) Dieudonné-Manin theory.** (We only give some definitions and facts.) For coprime integers $m \in \mathbb{Z}_{\geq 0}, n \in \mathbb{Z}_{\geq 0}$ one can define a $p$-divisible group $G_{m,n}$. In fact, $G_{1,0} = \mathbb{G}_m[p^\infty]$, and $G_{0,1} = (\mathbb{Q}_p/\mathbb{Z}_p)$. For $m > 0$ and $n > 0$ we have a formal $p$-divisible group $G_{m,n}$ of dimension $m$ and of height $h = m + n$. We do not give the construction here; see the first two chapters of Manin's thesis [25]; the definition of $G_{m,n}$ is on page 35 of [25]. The $p$-divisible group $G_{m,n}$ is defined over $\mathbb{F}_p$; we will use the same symbol for this group over any base field or base scheme over $\mathbb{F}_p$, i.e. we write $G_{m,n}$ instead of $G_{m,n} \otimes_{\mathbb{F}_p} K$.

Let $K = \mathbb{F}_{p^a}$, and $X = G_{m,n} \otimes_{\mathbb{F}_p} K$. Let $\pi_X \in \mathrm{End}(X)$ be the geometric Frobenius. Then

$$\boxed{v_p(\pi_X) = \tfrac{m \cdot a}{h}, \quad h := m + n, \quad q = p^a.}$$

In [25], Chapter II we find:
**Theorem.** *Let $k$ be an algebraically closed field of characteristic $p$. Let $X$ be a $p$-divisible group over $k$. Then there exists an isogeny*

$$X \quad \sim \quad \prod_i G_{m_i,n_i}.$$

see [M] Classification Theorem on page 35.

**(5.10) Newton polygons.** The isogeny class of $\sum_i G_{m_i,n_i}$ will be encoded in the form of a Newton polygon. The simple $p$-divisible group $G_{m,n}$ will be represented by $m + n$ slopes equal to $m/(m + n)$. The slopes of $\sum_i G_{m_i,n_i}$ will be ordered in non-decreasing order. For a $p$-divisible group of dimension $d$, height $h$ with $h = d + c$ together these slopes form a polygon in $\mathbb{Q} \times \mathbb{Q}$ with the following properties:
- it starts at $(0, 0)$,
- it ends at $(h, c)$,
- for every slope $\lambda$ we have $0 \leq \lambda \leq 1$,
- it is lower convex, and
- its breakpoints have integral coordinates.

**Definition.** Such a polygon is called a *Newton polygon.* For a $p$-divisible group over $K$ we

write $\mathcal{N}(X)$ for the Newton polygon constructed from $X \otimes_K k$. For an abelian variety $A$ over $K$ we write $\mathcal{N}(A) = \mathcal{N}(A[p^\infty])$.

**Example.** Suppose $A[p^\infty] = X \sim G_{m,n} \times G_{n,m}$. Then the Newton polygon $\mathcal{N}(A)$ of $A$ equals $(m,n)+(n,m)$; this has $m+n$ slopes equal to $n/(m+n)$ and $m+n$ slopes equal to $m/(m+n)$.

The theorem just cited reads: *there is a bijection between the set of k-isogeny classes of p-divisible groups over k and the set of Newton polygons:*

$$\{X\}/\sim_k \quad \stackrel{\sim}{\longrightarrow} \quad \{\text{Newton polygon}\}$$

**(5.11) The Serre dual of a $p$-divisible group.** For a $p$-divisible group $X = \{G_i\}$ we use the maps $G_{i+1} \to G_i$ ("multiplication by $p$ on $G_{i+1}$", dualize to get $G_{i+1}^D \leftarrow G_i^D$; using these we define a $p$-divisible group $X^t = \{G_i^D\}$; this is called the Serre dual of $X$.

Using (3.9) we show: *for an abelian scheme $A \to S$ we have a canonical isomorphism:*

$$(A[p^\infty])^t \quad \cong \quad A^t[p^\infty].$$

**(5.12) Definition.** *We say that a Newton polygon $\xi$ is symmetric if the slope $\lambda$ and the slope $1-\lambda$ appear with the same multiplicity.*

**Corollary of the duality theorem.** *For an abelian variety $A$ over a field, its Newton polygon $\xi = \mathcal{N}(A)$ is symmetric.* Use the fact that a polarization gives is an isogeny $A \to A^t$, hence $A \sim A^t$. Hence $X = A[p^\infty] \sim A^t[p^\infty]$. If $\mathcal{N}(X) = \{\lambda_1, \cdots, \lambda_h\}$, then $\mathcal{N}(X^t) = \{1-\lambda_h, \cdots, 1-\lambda_1\}$. □

**(5.13) A conjecture by Manin.** We have seen that every abelian variety in characteristic $p$ has a symmetric Newton polygon. The converse was conjectured by Manin:

**Conjecture.** *For every symmetric Newton polygon $\xi$ there exists an abelian variety with $\mathcal{N}(A) = \xi$.*

**Remark.** By a result of Grothendieck and Katz it follows that if such an abelian variety does exist, then also an abelian variety $A$ over a finite field exists with $\mathcal{N}(A) = \xi$. See [19], Th. 2.3.1 on page 143.

**(5.14)** The Newton polygon $\sigma$ with all slopes equal to $\frac{1}{2}$ is called the *supersingular* Newton polygon.

Define an abelian variety $A$ over a field $K \supset \mathbb{F}_p$ to be *supersingular* if $A \otimes_K k \sim E^g$, where $E$ is a supersingular elliptic curve.

**Theorem.** *Let $A$ be an abelian variety over $K$.*

$$\mathcal{N}(A) = \sigma \quad \Longleftrightarrow \quad A \text{ is supersingular.}$$

Various details were proved by: Tate, FO, Deligne, Shioda; for references see [24], 1.6.

**(5.15) Remarks.** Note that $f(A)$ is the number of times the slope $\lambda = 0$ appears in $\mathcal{N}(A)$, which is the same as the number of times the slope $\lambda = 1$ appears in $\mathcal{N}(A)$.

We have seen that a supersingular abelian variety $A$ with $\dim(A) > 1$ is not absolutely simple; indeed $A \otimes k \sim E^g$, where $E$ is a supersingular elliptic curve. However, for every symmetric Newton polygon $\xi \neq \sigma$ there exists an absolutely simple abelian variety $A$ having

this Newton polygon; see Section 14. In particular for every abelian variety $A$ over $k$ which is not supersingular the isogeny decomposition of $X = A[p^\infty]$ is strictly finer than the Poincaré-Weil primary decomposition.

If $A$ is a supersingular abelian variety over $k$, then $\mathrm{End}(A) \neq \mathbb{Z}$. However we can show that for every symmetric Newton polygon $\xi \neq \sigma$ there exists an abelian variety $A$ over some algebraically closed field $k$ having this Newton polygon with $\mathrm{End}(A) = \mathbb{Z}$; see Section 14.

# 6 Complex multiplication

**(6.1) Defintion.** *An abelian variety $A$ of dimension $g$ over a field $K$ is said to admit sufficiently many Complex Multiplications, abbreviated smCM, iff* $\mathrm{End}^0(A)$ *contains a commutative semi-simple algebra of rank $2g$ over $\mathbb{Q}$. An abelian variety which admits smCM we will call a CM abelian variety. If confusion could arise we will say "sufficiently many Complex Multiplications over $K$".*

Equivalently: write $A \sim \sum B_i$ up to isogeny as a direct sum of $K$-simple abelian varieties; $A$ is said to admit smCM iff every $\mathrm{End}^0(B_i)$ contains a number field of degree $2{\cdot}\dim B_i$ over $\mathbb{Q}$.

**(6.2) Remarks.** For an elliptic curve $E$ smCM is equivalent with $\mathrm{End}(E) \neq \mathbb{Z}$.

Confusion might arise when we say "$A$ has complex multiplications" because it might mean smCM, or it might mean $\mathrm{End}(A) \neq \mathbb{Z}$, different concepts for $\dim A > 1$.

For a simple abelian variety $A$ over $\mathbb{C}$ the notion smCM is equivalent with the fact that $\mathrm{End}^0(A) = L$ is a field of degree $2{\cdot}\dim A$ over $\mathbb{Q}$. In this case the field $L$ is a CM-field. The field $L$ together with the action $\iota : L \to \mathrm{End}(\mathfrak{t}_{A,0})$ on the tangent space is called a CM-type. The notions smCM and CM-type are related, but not the same.

In general $\mathrm{End}^0(A)$ is not a field; for example the endomorphism algebra of a supersingular elliptic curve $E$ over $m := \overline{\mathbb{F}_p}$ equals $Q_{p,\infty}$, the quaternion algebra over $\mathbb{Q}$ ramified precisely at $p$ and $\infty$. If $A$ (is simple and) has smCM, and $E = \mathrm{End}^0(A)$ is a field, then $E/\mathbb{Q}$ is a CM-field, and the Rosati involution is complex conjugation.

We will see in Section 14 that the endomorphism algebra of an a simple abelian variety in characteristic $p$ can be a field or a division algebra, and both cases do appear.

For an abelian variety over a field $K$, and an extension $K \subset L$ of fields it can happen that $\mathrm{End}(A) \subsetneqq \mathrm{End}(A \otimes_K L)$. It can happen that $A$ does not admit smCM (over $K$) and $A \otimes_K L$ does admit smCM (over $L$). Be careful, e.g. some people say "$E$ is an elliptic curve over $\mathbb{Q}$ with complex multiplications" meaning that $E$ is defined over $\mathbb{Q}$, and that there exists an extension $K \subset L$ such that $\mathrm{End}(E \otimes_K L)$ is an imaginary quadratic field.

An abelian variety over $\mathbb{C}$ has smCM, is of CM-type, iff its Mumford-Tate group is commutative; see [9], page 63; [26], page 347.

**(6.3)** It is not difficult to show: An abelian variety with smCM over $\mathbb{C}$ is defined over a finite extension of $\mathbb{Q}$ (i.e. over a number field).

It is easy to see: There are abelian varieties in positive characteristic with smCM which cannot be defined over a finite field.

**(6.4) Theorem** (Grothendieck). *Let $K$ be a field, let $A$ be an abelian variety over $K$ which admits* smCM. *We write $k = \overline{K}$. There exists a finite extension $L$ of the prime field of $K$, an abelian variety $B$ over $L$, and an isogeny $A \otimes k \sim B \otimes k$.*

See [35]. I.e. "*the isogeny class of $A$ with* smCM *can be defined over a finite extension $L$ of the prime field $\mathbb{P}$ of $K$*: either $\mathbb{P} = \mathbb{Q}$, with $[L : \mathbb{Q}] < \infty$, and $L$ is a number field, or $\mathbb{P} = \mathbb{F}_p$, and $L = \mathbb{F}_q$ is a finite field.

**(6.5)** Let $M$ be a field with a discrete valuation $v$ with $R_v$ the ring of $v$-integers in $M$. Let $A$ be an abelian variety over $M$. We say that $A$ has *good reduction* at $v$ if there exists an abelian scheme $\mathcal{A} \to \mathrm{Spec}(R_v)$ and an isomorphism $\mathcal{A} \otimes_{R_v} M \cong A$. For more details see [47], of [38].

**(6.6)** Let $M$ be a field and let $A$ be an abelian variety which admits smCM over $M$. Then there exists a finite extension $M \subset M'$ such that $A' = A \otimes_M M'$ has good reduction for every discrete valuation of $M'$; see [47], page 482; see [38], Th. 4.1, and use the fact that an abelian variety which admits smCM, and which has stable reduction has good reduction.

# 7 Brauer theory

Some references: [3]; [4], CH. VI; [46], CH. XII; [7]. Here we only give a very brief survey of facts which we need.

**(7.1)** Abstract definitions can be given. As a result we have: a *simple algebra* finite dimensional over its center is a matrix algebra over a division ring, Wedderburn's theorem, see [44], page 91. A finite dimensional *semi-simple algebra* is a product of simple algebras.

Let $A$ be an abelian variety over a field, $A \sim \prod_{1 \leq i \leq r} A_i^{\mu_i}$ the primary decomposition given by the Poincaré-Weil theorem. Then

$$\mathrm{End}^0(A) \cong \mathrm{Mat}(D_i, \mu_i), \quad D_i = \mathrm{End}^0(A_i)$$

is a semi-simple algebra.

**(7.2)** Choose a field $L$. Consider all simple division algebras with center equal to $L$ of finite dimension over $L$. we say that two such algebras $A$ and $B$ are equivalent if there exists a central $L$-division algebra and integers $r, s \in \mathbb{Z}_{\geq 0}$ such that $A \cong \mathrm{Mat}(D, r)$ and $B \cong \mathrm{Mat}(D, s)$. The set of equivalence classes of finite dimensional central $L$-algebras has a group structure (using $\otimes$). This group is called the Brauer group of $L$, notation $\mathrm{Br}(L)$.

**Examples.**
($\infty$ real) $\mathrm{Br}(\mathbb{R}) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, generated by the class of the quaternion algebra over $\mathbb{R}$.
($v$ finite) Let $L$ be a local field. Then $\mathrm{Br}(L) \cong \mathbb{Q}/\mathbb{Z}$.
($\infty$ complex) $\mathrm{Br}(\mathbb{C}) = 0$.

Let $L$ be a number field, i.e. $[L : \mathbb{Q}] < \infty$. Let $D$ be a central simple algebra of finite dimension over its center $L$. Then, using the isomorphisms above, we define:
$\mathrm{inv}_v(D) \in \mathbb{Q}, 0 \leq \mathrm{inv}_v L(D) < 1$ if $v$ is a finite place; here we use $\mathrm{Br}(L_v) \cong \mathbb{Q}/\mathbb{Z}$.
$\mathrm{inv}_v(D) \in \{0, 1/2\}$ if $v$ is a real infinite place; here we use $\mathrm{Br}(\mathbb{R}) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.
$\mathrm{inv}_v(D) = 0$ if $v$ is a complex infinite place.
Note that $\mathrm{inv}_v(D) = 0$ if and only if $D \otimes L_v$ is isomorphic with a matrix algebra over $L_v$.

With these notations we have:

**(7.3) Theorem.** *Let $L$ be a number field. Then there is an exact sequence*

$$0 \quad \to \quad \mathrm{Br}(L) \quad \longrightarrow \quad \bigoplus_v \mathrm{Br}(L_v) \quad \longrightarrow \quad \mathbb{Q}/\mathbb{Z} \quad \to \quad 0,$$

$$[D] \mapsto \{\mathrm{inv}_v(D) \mid v\}, \qquad \{i_v \mid v\} \mapsto \sum_v i_v \bmod \mathbb{Z}.$$

More explicitly: For every $D$ as above,

there are only finitely many places with $\mathrm{inv}_v(D) \neq 0$,

the equivalence class $[D]$ is determined by this set of invariants,

the sum of these invariants is an integer,

and conversely for every finite set of rational numbers $i_v$ with $0 \leq i_v < 0$, respectively $i_v \in \{0, 1/2\}$ if $v$ is real, respectively $i_v = 0$ if $v$ is complex, such that $\sum i_v \in \mathbb{Z}$ there exists a central simple algebra with these invariants.

The least common multiple $d$ of the denominators of all $\mathrm{inv}_v(D)$ is the order of the class of $D$ in $\mathrm{Br}(L)$ and $[D : \text{Ł}] = d^2$.

**(7.4)** This is an abstract description of all possible central division algebras over a number field. A more concrete description of some cases in terms of generators and defining relations is to be found in [2].

**(7.5) Splitting fields.** Let $D$ be a finite dimensional simple algebra central over $L$. Let $L \subset L'$ be a finite extension. Suppose $v$ is a finite place of $L$ and $v'$ is a finite place of $L'$ above $v$. Then

$$\mathrm{inv}_v(D) = [L'_{v'} : L_v] \cdot \mathrm{inv}_v(D \otimes_L L'),$$

see [46], XIII.3, Prop. 7.

An extension $L \subset L'$ is called a splitting field of $D/L$ if $D_{L'} = D \otimes_L L'$ is a matrix algebra over $L'$ (note that for any $L' \supset L$, the algebra $D \otimes_L L'$ is central over $L'$). If $[D : L] = d^2$, every subfield $L \subset L \subset D$ has degree $[L' : L]$ dividing $d$; if moreover this degree equals $d$, the extension $L'/L$ splits $D$.

Note that $D \mapsto D_{L'}$ gives a homomorphism $\mathrm{Br}(L) \to \mathrm{Br}(L')$. From this we see necessary and sufficient conditions for an extension $L'/L$ to be splitting for $D$: suppose $D$ is given by $\{\mathrm{inv}_v(D) \mid v\}$; let $\delta_v$ be the denominator of $\mathrm{inv}_v(D)$ written in lowest terms (note that $\mathrm{inv}_v(D) = 0$ implies $\delta_v = 1$); then *$L'/L$ is splitting for $D$ iff for every place $v$ of $L$ and every $v'$ a place of $L'$ above $v$, we have that $\delta_i$ divides $[L'_{v'} : L_v]$*. Every splitting field of $D$ degree $\sqrt{[D : L]}$ over $L$ can be $L$-embedded into $D$.

For example an extension $L'/\mathbb{Q}$ is splitting for $D = K_{p,\infty}$ iff every place above $\infty$ is complex, and every place $v'$ above $p$ gives an extension $L'_{v'} \subset \mathbb{Q}_p$ of even degree. A quadratic extension over $\mathbb{Q}$ can be embedded into $D$ iff these conditions are fulfilled, i.e. above $\infty$ there is one (complex) place, and $p$ does not split into $L'/\mathbb{Q}$.

**(7.6)** CM-**splitting fields.** Let $D$ be an Albert division algebra. We know there exists a splitting field $L \subset L' \subset D$ for $D$. In this case even more can be said: there exists a splitting field $L \subset L' \subset D$ for $D$ which moreover is a CM-field; see [52], Lemma 2 on page 100.

# 8 Endomorphism algebras

**(8.1) Definition.** *An* Albert algebra $D$ *is a* $\mathbb{Q}$*-algebra of finite rank over* $\mathbb{Q}$*, which has an anti-involution* $\iota : D \to D$ *which is positive definite* i.e. the map $x \mapsto \mathrm{Tr}(x \cdot \iota(x))$ is a positive definite quadratic form on $D$.

**(8.2) Theorem.** *Let* $A$ *be an abelian variety over* $K$*, with Rosati involution* $\iota : D \to D$ *on the endomorphism algebra* $D := \mathrm{End}^0(A)$*. This anti-involution is positive definite; hence* $(D, \iota)$ *is an Albert algebra.*

**(8.3) Notation.** We will study situations where we have:

$$\mathbb{Q} \quad \subset \quad L_0 \quad \subset \quad L \quad \subset \quad D,$$

where $L_0/\mathbb{Q}$ is a totally real field of finite degree $e_0 = [L_0 : \mathbb{Q}]$,
either $L/L_0$ is a totally imaginary quadratic extension, $e = 2 \cdot e_0$, and $L/\mathbb{Q}$ is a CM field,
or $L = L_0$ and $e = e_0$,
$D$ is a division algebra with center equal to $L$, with $d^2 = [D : \mathbb{Q}]$.

**(8.4) Theorem** (classification of Albert algebras). *Suppose* $(D, \iota)$ *is an Albert algebra, such that* $D$ *is a division algebra. Then* $D$ *is one of the following four types:*
Type I($e_0$) $d = 1$*,* $e = e_0$*, and* $D = L = L_0$ *is a totally real field;*
Type II($e_0$) $d = 2$*,* $e = e_0$*, and* $\mathrm{inv}_v D = 0$ *for all* $v$ *at infinity; here* $D$ *is an indefinite quaternion algebra over the totally real field* $L = L_0$*;*
Type III($e_0$) $d = 2, e = e_0$ *and* $\mathrm{inv}_v D \neq 0$ *for all* $v$ *at infinity; here* $D$ *is a definite quaternion algebra over the totally real field* $L = L_0$*;*
Type IV($e_0, d_0$) $L \supset L_0 \supset \mathbb{Q}$ *is a* CM*-field,* $[L : \mathbb{Q}] = e = 2e_0$*, and* $[D : \mathbb{Q}] = d^2$*.*

**(8.5)** The classification of Albert algebras was given by Albert in a series of papers in 1934/1935; for references see [39] or [22]. For a proof of (8.4) see [28], pp. 21 – 203, or [22], 5.5.

**(8.6) CM abelian varieties.** Let $A$ be a simple abelian variety over $K$ which admits smCM. Then:
(0) either the characteristic $\mathrm{char}(K) = 0$, the abelian variety can be chosen to be defined over a number field, $L = D = \mathrm{End}^0(A)$ is commutative, and $D = L$ is of type Type IV$(g, 1)$, a CM-field with $[L : \mathbb{Q}] = 2g$;

(p) or the characteristic $\mathrm{char}(K) = p > 0$, the abelian variety is isogenous with an abelian variety defined over a finite field; for a simple abelian variety over a finite field $K = \mathbb{F}_q$, $q = p^a$ we have the following possibilities:

$\boxed{\pi = \pm\sqrt{q} \in \mathbb{Q};}$ here $a$ is even; in this case $\dim(A) = 1$, i.e. $A$ is an elliptic curve, all endomorphisms of $A$ are defined over $K$, i.e. $\mathrm{End}(A) = \mathrm{End}(A \otimes \overline{\mathbb{F}_q})$, and $\mathrm{End}^0(A) = K_{p,\infty}$, the unique algebra of Type III(1), a quaternion algebra central over $\mathbb{Q}$ ramified exactly at $p$ and at $\infty$;

$\boxed{\pi = \pm\sqrt{q} \in \mathbb{R}, \text{ but } \pi \notin \mathbb{Q};}$ here $a$ is odd; in this case $\dim(A) = 2$, and $\mathrm{End}(A)$ is of Type III(2), a quaternion algebra central over $\mathbb{Q}(\sqrt{p})$ ramified exactly at the two infinite places of $L = L_0 = \mathbb{Q}(\sqrt{p})$; in this case over the quadratic extension $K \subset K'$ the abelian variety $A \otimes_K K'$ is isogenous with the product of two supersingular elliptic curves of the type just described;

$$A' = A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2} \sim E^2, \qquad \mathrm{End}^0(A') \cong \mathrm{Mat}(K_{p,\infty}, 2).$$

$\boxed{\pi \notin \mathbb{R}}$ (for at least one , equivalently for all embeddings into $\mathbb{C}$); in this case $\mathrm{End}(A)$ is of Type IV$(e_0, d)$ with $e_0 \cdot d = g$; the cases $e_0 = g$ (and $D = L$ is a CM-field), respectively $d > 1$ (and $D$ is non-commutative) do appear; also intermediate cases, $e_0 < g$, hence $d > 1$, do appear; e.g. see (17.10).

It may happen (depending on $A$ and on $K$) that for an extension $K \subset K'$ that $\mathrm{End}^0(A) \subsetneqq \mathrm{End}^0(A \otimes_K K')$.

**(8.7) Remark.** For every Albert algebra $(D, \iota)$ and every characteristic there exists a simple polarized abelian variety $(A, \lambda)$ over a field of that characteristic giving this Albert algebra.

In characteristic zero this was proved by Albert, and by Shimura, see [48]. It is precisely known, which values $\dim(A)$ can have for a given $(D, \iota)$ under the condition $\mathrm{End}^0(A) = D$, see [48], Th. 5 on page 176; [28], page 206.

In the arbitrary case this was proved by Gerritzen, see [13]. Indeed that methods works in any characteristic, see [39], Th. 3.3. However there is no complete information which possibilities there are for $\dim(A)$ for a given $(D, \iota)$ under the condition $\mathrm{End}^0(A) = D$.

Here is an example. Suppose that $D = K_{p,\infty}$. If $D = \mathrm{End}^0(A)$, where $A$ is simple over $K$, and $\mathrm{char}(K) = 0$, then $g = \dim(A)$ is an even number and $g \geq 4$. However if $\mathrm{char}(K) = p$ we can choose $g = 1$ or any value $g \in \mathbb{Z}_{\geq 5}$ and find a simple abelian variety $A$ in characteristic $p$ of dimension $g$ with $K_{p,\infty} \cong \mathrm{End}^0(A)$, see [39], Th. 4.8. In general it now known what are the necessary and sufficient conditions are relating $g$ and $D$ by the existence of $A$ with $\dim(A) = g$ and $D \cong \mathrm{End}^0(A)$.

**(8.8)** Consider the $p$-divisible group $G_{m,n}$ in the Manin classification, i.e $\dim(G_{m,n}) = m$ and $\dim(G^t_{m,n}) = n$. This is an absolutely simple $p$-divisible group. Hence for every base field $K$, the algebra $D := \mathrm{End}^0(G_{m,n} \otimes K) = \mathrm{End}(G_{m,n}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a division algebra. Suppose the base field contains $\mathbb{F}_{p^{m+n}}$. In that case $D := \mathrm{End}^0(G_{m,n} \otimes K)$ is a division algebra central over $\mathbb{Q}_p$, with $[D : \mathbb{Q}_p] = (m+n)^2$ and

$$\mathrm{inv}_p(\mathrm{End}^0(G_{m,n})/\mathbb{Q}_p) = \frac{n}{m+n}.$$

See [18], page 227.

# 9 Tate: abelian varieties over finite field

We recall some results of [51] and [52].

**(9.1)** Choose an abelian variety $A$ over a field $K$. Let $\ell$ be a prime number different from $\mathrm{char}(K)$. We have a homomorphism

$$\mathrm{End}(A) \quad \longrightarrow \quad \mathrm{End}(T_\ell(A)).$$

This homomorphism is *injective*. We obtain an injective homomorphism

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \hookrightarrow \quad \mathrm{End}(T_\ell(A)).$$

**Theorem** (Tate). *If $K$ is a finite field, this is an isomorphism*

$$\boxed{\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \xrightarrow{\sim} \quad \mathrm{End}(T_\ell(A)).}$$

See [51], Main Theorem on page 314.

**Exercise.** *Show that this map is bijective if and only if* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to \mathrm{End}(T_\ell A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ *is bijective.*

**(9.2) Theorem** (Tate). *Let $A$ be a simple abelian variety over $K = \mathbb{F}_q$, $q = p^a$ of dimension $\dim(A) = g$. Write $L = \mathbb{Q}(\pi_A)$, and $D = \mathrm{End}^0(A)$. For a discrete valuation of $L$ write $L_v$ for the $v$-adic completion of $L$, and $f_v$ for the degree of the residue class field at $v$ over its prime field. The structure of $D$ gives:*

**1.** *$L = \mathbb{Q}(\pi_A)$ is the center of the division algebra $D = \mathrm{End}^0(A)$.*

**2.** *$D/L$ is non-split at every real infinite place of $L$.*

**3.** *For every discrete valuation with residue characteristic not equal to $p$ we have* $\mathrm{inv}_v(D) = 0$.

**4.** *For every discrete valuation with residue characteristic equal to $p$ we have*

$$\mathrm{inv}_v(D) = \frac{v(\pi_A)}{v(q)}[L_v : \mathbb{Q}_p] = v(\pi_a)\frac{f_v}{a} \pmod 1.$$

**5.** *The abelian variety $A$ admits* smCM *over $K$; in particular*

$$2{\cdot}g \quad = \quad [L : \mathbb{Q}]{\cdot}\sqrt{[D : L]}.$$

**6.** *Let $f_A$ be the characteristic polynomial of $\pi_A \in \mathrm{End}^0(A)$, see (3.10). Let $I_\pi$ be the irreducible polynomial of $\pi = \pi_A$ over $\mathbb{Q}$. Let $d := \sqrt{[D : L]}$. Then*

$$f_A \quad = \quad I_\pi^d.$$

See [52], Th. 1 on page 96.

**(9.3) Exercise.** In the notation of the above theorem, part (4), show: $v(\pi_A){\cdot}f_v \in \mathbb{Z}$.

**(9.4) Exercise** (see [52], page 97). Let $\psi(\pi_A) \notin \mathbb{R}$. Let $\overline{v}$ be the complex conjugate of $v$. Show:

$$\mathrm{inv}_v(D) + \mathrm{inv}_{\overline{v}}(D) \equiv 0 \pmod{\mathbb{Z}}; \quad \text{in particular} \quad \mathrm{inv}_v(D) \equiv 0 \pmod{\mathbb{Z}} \quad \text{if} \quad \overline{v} = v.$$

**(9.5) Exercise.** Let $A$ be a simple abelian variety over $\mathbb{F}_p$. *Show that* $\mathrm{End}(A)$ *is* commutative (hence $\mathrm{End}^0(A)$ is a field). See [54], Th.6.1.

**(9.6) Remark.** Let $A$ be an abelian variety over some field $K$. The $p$-adic completion of Center(End$^0(A)$) need not split $A[p^\infty]$ into isoclinic factors. However:
**Exercise.** Let $A$ be a simple abelian variety over a finite field $K$, with $L = \mathbb{Q}(\pi_A) \subset D = \mathrm{End}^0(A)$. The set of primes above $p$ in $L/\mathbb{Q}$ gives a splitting up to isogeny:

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_p \quad \cong \quad \prod_{v|p} L_v, \qquad A[p^\infty] \quad \sim \quad \prod_{v|p} X_v.$$

Note that every isogeny factor $X_v$, determined by the action of $L_v$, is non-zero. *Show that $X_v$ is isoclinic*, i.e. $\mathcal{N}(X_v)$ is a straight line. Warning: different isogeny factors can have the same slope.

**(9.7) Theorem** (Tate). *Let $A$ and $B$ be abelian varieties over $K = \mathbb{F}_q$ and let $f_A$ respectively $f_B$ be the characteristic polynomial of $\pi_A$ respectively $\pi_B$. Then $A$ is isogenous to an abelian subvariety of $B$ if and only if $f_A$ divides $f_B$ in $\mathbb{Q}[T]$. In particular $A \sim B$ if and only if $f_A = f_B$.*
See [51], Theorem 1 on page 139.

# 10 Honda-Serre-Tate theory

In this section we sketch a proof of (1.1). We write $K = \mathbb{F}_q$, with $q = p^q$. Here are the steps in this proof:

**ONE (Weil)** *By $A \mapsto \pi_A$ we map the set of isomorphism classes of simple abelian varieties over $K$ to $W(q)$.*

**TWO (Tate)** *For simple abelian varieties $A$, $B$ defined over a finite field we have:*

$$A \sim B \quad \Longleftrightarrow \quad \pi_A \sim \pi_B.$$

Note that $A \sim B$ only makes sense if $A$ and $B$ are defined over the same field. Note that $\pi_A \sim \pi_B$ implies that $A$ and $B$ are defined over the same finite field.

**THREE (Honda)** *Suppose given $\pi \in W(q)$. There exists a finite extension $K = \mathbb{F}_q \subset K' := \mathbb{F}_{q^N}$ and an abelian variety $A'$ over $K'$ with $\pi^N = \pi_{A'}$.*
Defintion: We say that $\pi$ is *effective* if there exists $A$ with $\pi \sim \pi_{A'}$. In this step we prove that an appropriate power of a $q$-Weil number is effective.

**FOUR** *If $\pi \in W(q)$ and there exists $N \in \mathbb{Z}_{>0}$ such that $\pi^N$ is effective, then $\pi$ is effective.*

**(10.1) A proof of ONE.** Weil proved, see (5.4), that for every abelian variety over a finite field with $q$ elements, $\pi_A$ is a $q$-Weil number. We conclude that we have a map

$$\boxed{\{\text{simple abelian variety over} \quad K\} \quad \longrightarrow \quad W(q),}$$

from the set of simple abelian varieties defined over $K$ to the set of $q$-Weil numbers.

**(10.2) A sketch of a proof of TWO.** An isogeny between $A$ and $B$ gives an isomorphism on the endomorphism algebras; as moreover Frobenius commutes with homomorphisms we see that this isomorphism maps $\pi_A$ onto $\pi_B$.

Suppose conversely that $\pi_A \sim \pi_B$. Then $A$ and $B$ are defined over the same finite field $\mathbb{F}_q$, where $q$ is the square of the norm of either of these integers. Then, using the description by Tate of the endomorphism algebra of an abelian variety over a finite field (9.2), we see that $\mathrm{End}^0(A)$ and $\mathrm{End}^0(B)$ are isomorphic. we conclude that

$$f_A = (I_{\pi_A})^d = (I_{\pi_B})^d = f_B.$$

By (9.7) we conclude that $A$ and $B$ are isogenous. We conclude that the map

$$\boxed{\{\text{simple abelian variety over } \quad K\}/\sim_K \quad \hookrightarrow \quad W(q)}$$

is injective.

**(10.3) A sketch of a proof of THREE.** ((Here we only give references and short indications of proof. For details see [52], §3.))

Start with a given $q$-Weil number $\pi$. Determine $L = \mathbb{Q}(\pi) \subset D$ as described in (9.2), see [52]. Choose a splitting field

$$L = \mathbb{Q}(\pi) \quad \subset \quad E \quad \subset \quad D$$

such that $E$ is a CM-field, see (7.6), see [52], Lemma 2 on page 100.

We know that for a given CM-field and a given CM-type $\Phi$ we can construct an abelian variety over $\mathbb{C}$ having that CM-type. Then, by Shimura we know that such an abelian variety, because its admits smCM, can be defined over a number field. An abelian variety which admits smCM acquires good reduction at all places after a finite extension of the ground field. Thus we can choose a number field $M$ and an abelian variety $B$ of CM-type $\Phi$ with good reduction $B_0$ at a prime over $p$. The essence of the proof consists of proving:

**Lemma.** *We can choose $\Phi$, and $B$ over $M$ in such a way that there exists $N \in \mathbb{Z}_{>0}$ such that $\pi_{B_0} = \pi^N$.*

See [52], Lemma 3 and §4.

This construction finishes the proof of step THREE.

**(10.4) A sketch of a proof of FOUR.** *For the proof of this step we need the notion of the Weil restriction functor.* Let $T \to S$ be a morphism of schemes; Then there exists a base change functor $Sch_S \to Sch_T$ by $X/S \mapsto (Z_T := Z \times_S T)/T$. The Weil restriction functor denoted by

$$\Pi_{T/S} : Sch_T \to Sch_S$$

is the right adjoint functor to the base change functor, i.e.

$$\mathrm{Hom}_S(Z, \Pi_{T/S}(Y)) = \mathrm{Hom}_T(Z_T, Y);$$

see [14], page 195-13. If $T \to S$ is flat and proper, and $Y \to T$ is quasi-projective, this functor is representable, see [14], page 221-20. In case $K$ is a field, $S = \mathrm{Spec}(K)$, and $K \subset K'$ is

a finite separable extension, $T = \mathrm{Spec}(K')$, then $\Pi_{T/S}(Y)$ can be obtained by descending $Y^{[K':K]}$ to $K$, as Weil proved.

Let $A'$ be a simple abelian variety over $K'$ such that $\pi_{A'} \sim \pi^N$. Let $B := \Pi_{\mathrm{Spec}(K')/\mathrm{Spec}(K)}(A')$. One can prove that in this case $f_B(T) = f_{A'}(T^N)$. This shows that $\pi$ is conjugated to a zero of $f_B$. By (9.7) this shows that there exists a simple factor $A$ of $B$ such that $\pi_A \sim \pi$. This proves the fourth step.

Hence the map

$$\boxed{\{\text{simple abelian variety over } \quad K\}/\sim_K \quad \xrightarrow{\sim} \quad W(q)}$$

is bijective. This proves (1.1). □

As a corollary of the proofs we obtain:

**(10.5) Theorem.** *Let $A$ be an abelian variety over $K = \mathbb{F}_q$. Then there exists a finite extension $K' = \mathbb{F}_{q^N}$, an isogeny $B_0 \sim A' := A \otimes_K K'$ and a* CM*-lifting of $B_0$ to characteristic zero.*

See [52], Th. 2 on page 102.

# 11 Base change

**(11.1) Exercise.** Let $A$ be an abelian variety over a field $K$. Let $K \subset K'$ be an extension of fields; write $A' = A \otimes_K K'$. *Show:* $\mathrm{End}(A) \to \mathrm{End}(A')$ *is injective, and* $\mathrm{End}(A')/\mathrm{End}(A)$ *is* torsion-free.

**(11.2) Exercise.** *Give examples with $A' = A \otimes_K K'$ in which* $\mathrm{End}(A) \subsetneqq \mathrm{End}(A')$.

**(11.3) Exercise.** Let $R$ be an integral domain, with $M := Q(R)$ its field of fractions. Let $\mathcal{A} \to \mathrm{Spec}(R)$ be an abelian scheme; write $A := \mathcal{A} \otimes_R M$.
**(a)** *Show that* $\mathrm{End}(\mathcal{A}) \to \mathrm{End}(A)$ *is an isomorphism.*

Let $R \to K$ be a ring homomorphism. Let $N$ be an integer not divisible by $\mathrm{char}(K)$. Write $A_0 = \mathcal{A} \otimes_R K$.
**(b)** *Show that* $\mathrm{End}(\mathcal{A}) \to \mathrm{End}(A_0)$ *has no $N$-torsion.*
**(c)** Let $\mathrm{char}(K) = p > 0$. *Give an example of $\varphi \in \mathrm{End}^0(\mathcal{A})$ such that $\varphi/p$ is integral over $\mathbb{Z}$ and $\varphi/p \notin \mathrm{End}(A_0)$.*
**(d)** Let $\mathrm{char}(K) = p > 0$. Let $\varphi \in \mathrm{End}^0(\mathcal{A})$ such that $\varphi/p$ is integral over $\mathbb{Z}$. Suppose $\dim(\mathcal{A}/R) = 1$, i.e. $\mathcal{A}$ is an elliptic curves over $r$. *Show that $\varphi/p \in \mathrm{End}(A_0)$.* See [39], Lemma 2.1 and Lemma 2.2.

**(11.4) Exercise.** Suppose $A$ is a simple abelian variety over a finite field $K$. Let $K \subset K'$ be a finite extension. *Show:*

$$\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi_A^{[K':K]}) \quad \Longleftrightarrow \quad \mathrm{End}(A) \xrightarrow{\sim} \mathrm{End}(A \otimes_K K').$$

## 12 Endomorphism algebras and endomorphism rings.

We write $\mathrm{End}(A)$ for the endomorphism ring of $A$ and $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ for the endomorphism algebra of $A$.

Suppose $A$ is an abelian variety over a finite field. Let $\pi_A$ be its geometric Frobenius, and $\nu_A = q/\pi_A$ its geometric Verschiebung. We see that $\pi_A, \nu_A \in \mathrm{End}(A)$. Hence the index of $\mathrm{End}(A)$ in a maximal order in $\mathrm{End}^0(A)$ is quite small, in sharp contrast with:

**(12.1) Exercise.** Let $L$ be a field quadratic over $\mathbb{Q}$ with ring of integers $\mathcal{O}_L$. Show that for any order $R \subset L$ there is a number $f \in \mathbb{Z}_{>0}$ such that $\mathcal{O}_L = \mathbb{Z} + f \cdot \mathcal{O}_L$ (and, usually, this number $f$ is called the conductor). *Show that for any imaginary quadratic $L$ and any $f \in \mathbb{Z}_{>0}$ there exists an elliptic curve $E$ over $\mathbb{C}$ such that* $\mathrm{End}(E) \cong \mathbb{Z} + f \cdot \mathcal{O}_L$.
Conclusion: the index of $\mathrm{End}(A)$ in a maximal order in $\mathrm{End}^0(A)$ is in general not bounded when working over $\mathbb{C}$.

**(12.2) Remark.** For a simple ordinary abelian variety $A$ over a finite field the orders contained in $\mathrm{End}^0(A)$ and containing $\pi_A$ and $\nu_A$ are precisely all possible orders in the isogeny class of $A$, see [54], Th. 7.4. However this may fail for a non-ordinary abelian variety, see [54], page 555. Much more information on endomorphism rings of abelian varieties over finite fields can be found in [54].

**(12.3)** Let $A$ be a simple abelian variety over $\mathbb{F}_p$. Suppose that $\psi(\pi_A) \notin \mathbb{R}$. *Show that* $\mathrm{End}(A)$ *is* commutative (hence $\mathrm{End}^0(A)$ is a field) (an easy exercise, or see [54], Th.6.1). In this case every order containing $pi_A$ and $\nu_A$ in $D = L = \mathrm{End}^0(A)$ is the endomorphism algebra of an abelian variety over $\mathbb{F}_p$.
**Remark.** There does exist a simple abelian variety over $\mathbb{F}_p$ such that $\mathrm{End}^0(A)$ is not commutative.

**(12.4)** *For abelian varieties over a finite field separable isogenies is an equivalence relation*, see [54], Th. 5.2.
**Exercise.** *Show that there exists an abelian variety $A$ over a field $K \supset \mathbb{F}_p$ such that separable isogenies do not give an equivalence relation in the isogeny class of $A$.*

**(12.5) Remark.** If $K \subset K'$ is an extension of fields, and $A$ is a simple abelian variety over $K$, then $A' := A \otimes_K K'$ may be $K'$-simple or non-$K'$-simple; both cases do appear, and examples are easy to give. The natural map $\mathrm{End}(A) \to \mathrm{End}(A')$ is en embedding which may be an equality, but also inequality does appear; examples are easy to give, see (3.11), (17.1), (17.10).

## 13 CM-liftings

**(13.1) Definition.** Let $A_0$ be an abelian variety over $K \supset \mathbb{F}_p$. Suppose $A_0$ admits smCM. We say that $A$ is a lift of $A_0$ if there exists an integral domain $R$ of characteristic zero with a surjective homomorphism $R \twoheadrightarrow K$, an abelian scheme $\mathcal{A} \to \mathrm{Spec}(R)$ such that $\mathcal{A} \otimes_R K \cong A_0$, with $A := \mathcal{A} \otimes_R M$, where $M = Q(R)$ is the field of fractions of $R$. Suppose $A_0$ admits smCM. We say that $A$ is a CM-lift if moreover $A$ admits smCM.

In this case the natural map $\mathrm{End}(\mathcal{A}) \to \mathrm{End}(A)$ is an isomorphism. Hence we obtain an injective ring homomorphism $\mathrm{End}(A) \to \mathrm{End}(A_0$, and hence an injective homomorphism $\mathrm{End}^0(A) \to \mathrm{End}^0(A_0)$. Even if $A$ is a CM-lifting, this last map need not be surjective.

**(13.2) Remark.** There does exist an abelian variety $A_0$ over a finite field $K$, such that there does exist an isogeny $B_0 \sim_K A_0$, such that $B_0$ admits a CM-lifting to characteristic zero, but $A_0$ does not admit a CM-lifting to characteristic zero; see [40].

**(13.3)** We have seen that up to a finite extension $K \subset K'$ of the base field, and up to an isogeny over $K'$ there does exist a CM-lifting if we start with an abelian variety over a finite field $K$. However the following problem seems open.

**(13.4) Open problem.** *Suppose $A_0$ is an abelian variety defined over a finite field $K$. Does there exist an isogeny $A_0 \sim_K B_0$ such that $B_0$ admits a CM-lifting to characteristic zero?* Probably the answer is negative in general.

**(13.5) Remark.** For an *ordinary* abelian variety $A_0$ over a perfect field of $\mathrm{char}(K) = p > 0$ Serre and Tate defined a canonical lifting $\mathcal{A} \to \mathrm{Spec}(W)$, where $W := W_\infty(K)$ is the ring of Witt vectors with field of fractions $M := Q(W)$. In that case

$$\mathrm{End}(A_0) \xleftarrow{\sim} \mathrm{End}(\mathcal{A}) \cong \mathrm{End}(\mathcal{A} \otimes_W M).$$

Deligne used this in order to describe all ordinary abelian varieties over a finite field in term of a lattice, with certain properties, which defines $A \otimes_M \mathbb{C}$. See [8].

## 14 Existence of endomorphism fields

Let $A$ be an abelian variety which admits smCM over a field $K$ If $\mathrm{char}(K) = 0$ and $A$ is simple then $D := \mathrm{End}^0(A)$ is a field. However if $\mathrm{char}(K) = p > 0$, the ring $\mathrm{End}(A)$ need not be commutative. For examples see Section 17.

Suppose $k$ is an algebraically closed field of $\mathrm{char}(k) = p$, and let $A$ be a supersingular abelian variety, i.e. $\mathcal{N}(A) = \sigma$; then $A \otimes k \sim E^g$, where $E$ is a supersingular elliptic curve. We have $D := \mathrm{End}^0(A) = \mathrm{Mat}(K_{p,\infty}, g)$; in particular $D$ is *not commutative* and for $g > 1$ the abelian variety $A$ is *not simple*. However this turns out to be the only exceptional case in characteristic $p$ where such a general statement holds.

**(14.1) Theorem** (Lenstra and FO). *Let $\xi$ be a symmetric Newton polygon, and let $p$ be a prime number. Suppose that $\xi \neq \sigma$, i.e. not all slopes in $\xi$ are equal to $1/2$. Then there exists an abelian variety $A$ over $m = \overline{\mathbb{F}_p}$ such that $D = L = \mathrm{End}^0(A)$ is a field.* Necessarily $A$ is simple and $L$ is a CM-field of degree $2{\cdot}\dim(A)$ over $\mathbb{Q}$.
See [23].

**(14.2) Corollary.** *For any $p$ and for any $\xi \neq \sigma$ there exists a simple abelian variety $A$ over $\overline{\mathbb{F}_p}$ with $\mathcal{N}(A) = \xi$.*

## 15 The Tate-$\ell$-conjecture and Tate-$p$-conjecture.

**(15.1) Theorem** (Tate, Zarhin, Mori, Faltings). *Let $K$ be a field of finite type over its prime field. Let $A$ be an abelian variety over $K$. Let $\ell$ be a prime number different from* $\mathrm{char}(K)$. *The homomorphism*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \xrightarrow{\sim} \quad \mathrm{End}(T_\ell(A))$$

*is an isomorphism.*
This was proved by Tate for $K$ a finite field, and conjectured by Tate in general, see [51]. For functions fields of positive characteristic this was proved by Zarhin and Mori. For number fields this was proved by Faltings in 1983, see [11]. For function fields in characteristic zero see [12], Theorem 1 on page 211.

**(15.2) Theorem** (Tate). *Let $K$ be a finite field,* $\mathrm{char}(K) = p$. *Let $A$ be an abelian variety over $K$. Then*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{End}(A[p^\infty])$$

*is an isomorphism.* See [55].

**(15.3) Exercise.** Let $E$ be an elliptic curve over $\mathbb{F}_p[[t]]$ such that $j(E) = t$ and $E_0 = E \otimes_{\mathbb{F}_p[[t]]} \mathbb{F}_p$ ordinary. Show that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{End}(E[p^\infty])$ is an isomorphism.

**(15.4) Theorem** (A. J. de Jong). *Let $K$ be a field of finite type over $\mathbb{F}_p$. Let $A$ be an abelian variety over $K$. Then*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{End}(A[p^\infty])$$

*is an isomorphism.* See [17], Th. 2.6.

## 16 Hypersymmetric abelian varieties

In the statement that $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{End}(T_\ell(A))$ is an isomorphism we see $\mathrm{End}(T_\ell(A))$. This can be interpreted as $\mathrm{End}(T_\ell(A)) = \mathrm{End}_G(T_\ell(A \otimes_K \overline{K}))$, where $G = \mathrm{Gal}(K^s/K)$, the absolute Galois group of $K$. In general the action of $G$ on $\mathrm{End}_G(T_\ell(A \otimes_K \overline{K}))$ is not in "diagonal form", i.e. in general

$$\mathrm{End}(T_\ell(A)) = \mathrm{End}_G(T_\ell(A \otimes_K \overline{K})) \quad \subsetneq \quad \mathrm{End}(T_\ell(A \otimes_K \overline{K})).$$

**(16.1) Definition** (Chai). *Let $A$ be an abelian variety over a finite field $K$; write $m = \overline{\mathbb{F}_p}$. We say that $A$ is* hypersymmetric *if*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \xrightarrow{\sim} \quad \mathrm{End}(T_\ell(A \otimes_K m))$$

*is an isomorphism.*

**(16.2) Exercise.** **(a)** Let $E$ be an elliptic curve over $m = \overline{\mathbb{F}_p}$. *Show that $E$ is hypersymmetric.*
**(b)** Let $E_1$ and $E_2$ be elliptic curves over an algebraically closed field $k$ such that $E_1$ and $_2$ are non-isogenous. *Show that $E_1 \times E_2$ is not hypersymmetric.*
**(c)** Let $A$ and $B$ be hypersymmetric abelian varieties such that $\mathcal{N}(A)$ and $\mathcal{N}(B)$ have no slopes in common. *Show that $A \times B$ is hypersymmetric.*
**(d)** Let $A$ be a hypersymmetric abelian variety, and let $\mu \in \mathbb{Z}_{>0}$. *Show that $A^\mu$ is hypersymmetric.*
**(e)** Let $m > n \geq 0$ be coprime integers. Let $\pi$ be a zero of the polynomial $T^2 + p^n T + p^g$ with $g = m + n$. *Show that $\pi$ is a $p^g$-Weil number.* Let $A$ be such that $\pi_A = \pi$. *Show that $A$ is hypersymmetric.*
**(f)** *Show that for any given symmetric Newton polygon $\xi$ there exists a hypersymmetric abelian variety $A$ with $\mathcal{N}(A) = \xi$.*
For details see [5].

# 17 Some examples

**(17.1) Exercise.** Choose relatively prime integers $m, n \in \mathbb{Z}_{\geq 0}$ with $m > n \geq 0$. Write $h = m + n$. Consider the polynomial $T^2 + p^n \cdot T + p^h$.
**(a)** *Show that the discriminant of this polynomial is negative. Show that a zero $\pi$ of this polynomial is a $p^h$-Weil number.*

Hence we know there exists a simple abelian variety $A$ over $K = \mathbb{F}_{p^h}$ with $\pi_A = \pi$.
**(b)** *Compute the dimension of $D := \mathrm{End}^0(A)$, and compute the dimension of $A$.*
**(c)** *Show that under the field extension $K \subset m := \overline{K}$ we obtain an isomorphism* $\mathrm{End}(A) \xrightarrow{\sim} \mathrm{End}(A \otimes_K m)$.
**(d)** *Compute the Newton polygon of the $p$-divisible group of $A$.*

**(17.2) The Manin Conjecture** [25], Conjecture 2 on page 76. The above exercise shows that the Manin conjecture is true, see [52], page 98.

We have seen that in the proof of the Honda-Serre-Tate theorem we need a construction over the complex numbers (in step three). However, there does exist a pure characteristic $p$-proof of the Manin Conjectures, see [42]. But I do not know a pure characteristic $p$-proof of the Honda-Serre-Tate theorem.

**(17.3) Exercise.** Let $\mathrm{char}(K) = p > 0$. Let $A$ be a simple abelian variety over a finite field; suppose that the $p$-rank $f = f(A)$ is maximal ($f = g$, $A$ is ordinary), or $f(A) = g - 1 > 0$ (and we say $A$ is 'almost ordinary"). *Show that* $\mathrm{End}(A)$ *is commutative.*

**(17.4) Remark.** There does exist an abelian variety $A$ over a field $K$, where $K$ is *not finite*, such that $A$ is ordinary and $\mathrm{End}(A)$ is *not commutative.*

**(17.5) Exercise.** Let $E$ be an elliptic curve over a field of characteristic $p > 0$, and let $L \subset \mathrm{End}^0(E)$ be a field quadratic over $\mathbb{Q}$. *Show that $L$ is imaginary. Show there exists a* CM-*lifting of $(E, L)$ to characteristic zero.*

**(17.6) Exercise.** Let $L_0 = \mathbb{Q}(\sqrt{2})$. Choose a rational prime number $p$ inert in $L_0/\mathbb{Q}$. Let $\beta := (2-\sqrt{2})\cdot p$. Let $\pi$ be a zero of the polynomial

$$g := T^2 - \beta T + p^4.$$

**(a)** *Show that the discriminant of $g$ is negative.*
**(b)** *Show that $\pi$ is a $q$-Weil number with $q = p^4$.*
**(c)** Let $A$ be an abelian variety over $\mathbb{F}_q$ with $\pi_A = \pi$. Let

$$\mathbb{Q} \quad \subset \quad L_0 = \mathbb{Q}(\beta) \quad \subset \quad L = \mathbb{Q}(\pi) \quad \subset \quad D := \mathrm{End}^0(A).$$

*Determine: $g = \dim(A)$, the structure of $D$ and the Newton polygon $\mathcal{N}(A)$.*

This can be generalized to:

**(17.7) Exercise.** Let $g \in \mathbb{Z}_{>0}$. Let $e_0, d \in \mathbb{Z}_{>0}$ with $e_0 \cdot d = g$. *Show there exists an abelian variety $A$ over $m = \overline{\mathbb{F}_p}$ with $D = \mathrm{End}^0(A)$ of* Type$(e_0, d)$.

**(17.8) Exercise.** Let $m, n \in \mathbb{Z}_{>0}$ be coprime integers. Let $g = m+n$. Let $e_0, d \in \mathbb{Z}_{>0}$ with $e_0 \cdot d = g$. *Show there exists an abelian variety $A$ over $\overline{\mathbb{F}_p}$ with $D = \mathrm{End}_0(A))$ of* Type$(e_0, d)$ *and $\mathcal{N}(A) = (m,n) + (n,m)$.*

**(17.9) Exercise.** *Give a counterexample to the statement*: Let $A$ be an ordinary, simple abelian variety over a finite field $K$; let $K \subset K'$ be a field extension; then $\mathrm{End}(A \otimes_K K')$ is commutative (hence [54], Th. 7.2 on page 553 needs careful reading).

**(17.10) Exercise.** Let $p$ be a prime number, and let $g := T^{30} + pT^{15} + p^{15}$. Write $K_n = \mathbb{F}_{p^n}$.
**(a)** *Show that $g \in \mathbb{Q}[T]$ is irreducible.* Let $\pi$ be a zero of $g$. *Show that $\pi$ is a $p$-Weil number.* Let $A$ be an abelian variety over $\mathbb{F}_p$ such that $\pi_A \sim \pi$.
**(b)** *Describe the structure of* $\mathrm{End}(A)$ *and compute* $\dim(A)$.
**(c)** *Show that*

$$\mathrm{End}(A) \quad \subsetneqq \quad \mathrm{End}(A \otimes K_3) \quad \subsetneqq \quad \mathrm{End}(A \otimes K_{15}),$$

*and describe the structures of these endomorphism algebras. Show that $A$ is absolutely simple.*

**(17.11) Exercise.** Let $m$ and $n$ be coprime integers, $m > n \geq 0$. Write $h := m+n$. For every $b \in \mathbb{Z}_{>1}$ write

$$g_b := T^2 + p^{2bn}(1 - 2p^{be}) + p^{2bh}, \quad e := h - 2n = m_n.$$

**(a)** *Show that the discriminant of $g_b$ is negative; conclude that $g_b \in \mathbb{Q}[T]$ is irreducible.* Let $\pi_b$ be a zero of $g_b$. *Show that $\pi_b$ is a $p^{2bh}$-Weil number.* Let $A_b$ be an abelian variety with $\pi_{A_b} \sim \pi_b$.
**(b)** *Describe the structure of* $\mathrm{End}(A_b)$ *and determine the Newton polygon $\mathcal{N}(A_b)$.*
**(c)** *Show that*

$$\#\Big(\{\ell \mid \ell \text{ is a prime number and } \exists b \in \mathbb{Z}_{>0} \text{ such that } \ell \text{ divides } (4p^{be}-1)\}\Big) = \infty.$$

[Hint: you might want to use the reminder below.]
**(d)** *Show that the set $\{\mathbb{Q}(\pi_b) \mid b \in \mathbb{Z}_{>0}\}/\cong_{\mathbb{Q}}$ is an infinite set of isomorphism classes of*

*quadratic fields.*
**(e)** *Conclude that*

$$\{A_b \otimes \overline{\mathbb{F}_p} \mid b \in \mathbb{Z}_{>1}\}$$

*defines an infinite number of* $\overline{\mathbb{F}_p}$*-isogeny classes with Newton polygon equal to* $(m,n)+(n,m)$.
**(f)** *Show that for any symmetric Newton polygon* $\xi \neq \sigma$ *which is not supersingular, there exists infinitely many isogeny classes of hypersymmetric abelian varieties over* $\overline{\mathbb{F}_p}$ *having that Newton polygon.*

**Reminder.** Let $S$ be a set of primes, and $\mathbb{Z}_S$ the ring of rational numbers with denominators using only products of elements of $S$; write $(\mathbb{Z}_S)^*$ for the multiplicative group of units in this ring. A conjecture by Julia Robinson, later proved as a corollary of a theorem by Siegel and Mahler says:

$$\#\left(\{\lambda \mid \lambda \in (\mathbb{Z}_S)^*, \quad \lambda - 1 \in (\mathbb{Z}_S)^*\}\right) < \infty;$$

this is a very special case of: [20], Th. 3.1 in 8.3 on page 194.

**(17.12) Exercise.** Let $p$ be a prime number, $p \equiv 3 \pmod 4$. Let $\pi := p^2 \cdot \sqrt{-1}$.
**(a)** *Show that* $\pi$ *is a* $p^4$*-Weil number.* Let $A$ be an abelian variety over $K := \mathbb{F}_{p^4}$ such that $\pi_A \sim \pi$. *Determine* $\dim(A)$. *Describe* $\mathrm{End}^0(A)$.
**(b)** *Show there does not exist an abelian variety* $B_0$ *over* $K_0 := \mathbb{F}_{p^2}$ *such that* $B_0 \otimes_{K_0} K \cong A$.
**(c)** *Let* $E$ *be a supersingular elliptic curve over some field* $M \supset \mathbb{F}_p$. *Show that*

$$\mathrm{Ker}(E \xrightarrow{F_E} E^{(p)} \xrightarrow{F_{E^{(p)}}} E^{(p^2)}) = E[p].$$

*Show that* $j(E) \in \mathbb{F}_p$.
**(d)** *Show there exists a field extension* $K \subset K'$ *and and abelian variety* $B_0$ *over* $K_0$ *such that* $B_0 \otimes_{K_0} K' \cong A \otimes_K K'$.

**(17.13) Definition / Remark.** Let $A$ be an abelian variety over a field $K$ and let $K_0 \subset K$. We say that $A$ *can be defined over* $K_0$ if there exists a field extension $K \subset K'$ and and abelian variety $B_0$ over $K_0$ such that $B_0 \otimes_{K_0} K' \cong A \otimes_K K'$. - The previous exercise shows that this does not imply that we can choose $B_0$ such that $B_0 \otimes_{K_0} K \cong A$.

# 18 Some questions

**(18.1) Open problem.** Determine all $(p, g, T)$ such that $p > 0$ is a prime number, $g \in \mathbb{Z}_{>0}$ and $T$ is the Type of an Albert algebra, such that there exists an algebraically closed field $k$ of characteristic $p$, and there exists an abelian variety $A$ over $k$ with $\mathrm{End}^0(A)$ of that type. Restrictions are known; which triples satisfying these conditions indeed do appear?

**(18.2) Open problem.** *Does there exist an abelian variety* $A$ *over a finite field* $K$ *such that there does not exist an isogeny* $A \sim_K B_0$ *where* $B_0$ *admits a* CM*-lifting to characteristic zero* ? See (13.4).
**Remarks.** We expect that there does exist such an isogeny class over a finite field.
Note that does exist $A \sim_K B_0$ over a finite field such that $A$ does not, and $B_0$ does admit a CM-lifting to characteristic zero.
Note that for any given $A$ over a finite field $K$ there does exist a finite extension $K'/K$ and an abelian variety $B_0 \sim_{K'} (A \otimes K')$ such that $B_0$ admits a CM-lifting to characteristic zero.

**(18.3) Open problem.** Note that the proof of (1.1) described above uses a construction of CM-abelian varieties over $\mathbb{C}$. *Does there exist a pure characteristic p proof of the Honda-Serre-Tate theorem ?*
**Remark.** We have seen there does exist a pure characteristic $p$ proof of the Manin conjecture, see [42].

Not all references below are needed for this talk, but I include relevant literature for completeness sake.

# References


[1] C. Birkenhake & H. Lange – *Complex tori.* Progr. Math. 177, Birkhäuser 1999.

[2] A. Blanchard - *Les corps non commutatifs.* Coll. Sup, Presses Univ. France, 1972.

[3] N. Bourbaki – *Algèbre.* Chap.VIII: *modules et anneaux semi-simples.* Hermann, Paris 1985.

[4] J. W. S. Cassels & A. Fröhlich (Editors) – *Algebraic number theory.* Academic press 1967. Chapter VI: J-P. Serre – *Local class field theory* pp. 129–161.

[5] C.-L. Chai & F. Oort – *Hypersymmetric abelian varieties.* [In preparation] For a preliminary version, see http://www.math.uu.nl/people/oort/

[6] G. Cornell, J. H. Silverman (Editors) – *Arithmetic geometry.* Springer – Verlag 1986.

[7] C. W. Curtis & I. Reiner – *Representation theory of finite groups and associative algebras.* Intersc. Publ.1962.

[8] P. Deligne – *Variétés abéliennes sur un corps fini.* Invent. Math. **8** (1969), 238 – 243.

[9] P. Deligne – *Hodge cycles on abelian varieties.* Hodge cycles, motives and Shimura varieties (Eds P. Deligne et al). Lect. Notes Math. **900**, Springer – Verlag 1982; pp. 9 - 100.

[10] S. J. Edixhoven, B. J. J. Moonen & F. Oort (Editors) – *Open problems in algebraic geometry.* Bull. Sci. Math. **125** (2001), 1 - 22.
See: http://www.math.uu.nl/people/oort/

[11] G. Faltings – *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349 – 366.

[12] G. Faltings & G. Wüstholz – *Rational points.* Seminar Bonn / Wuppertal 10983/84. Asp. Math. E6, Vieweg 1984.

[13] L. Gerritzen – *On multiplications of Riemann matrices.* Math. Ann **194** (1971), 109 – 122.

[14] A. Grothendieck – *Fondements de la géomtétrie algébrique.* Extraits du Séminaire Bourbaki 1957 - 1962. Secr. math., Pairs 1962.

[15] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux de Dieudonné.* Sém. Math. Sup. **45**, Presses de l'Univ. de Montreal, 1970.

[16] T. Honda – *Isogeny classes of abelian varieties over finite fields.* Journ. Math. Soc. Japan **20** (1968), 83 – 95.

[17] A. J. de Jong – *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristics.* Invent. Math. **134** (1998) 301-333, Erratum **138** (1999) 225.

[18] A. J. de Jong & F. Oort – *Purity of the stratification by Newton polygons.* J. Amer. Math. Soc. **13** (2000), 209-241. See: http://www.ams.org/jams/2000-13-01/

[19] N. M. Katz – *Slope filtration of F–crystals.* Journ. Géom. Alg. Rennes, Vol. I, Astérisque **63** (1979), Soc. Math. France, 113 - 164.

[20] S. Lang – *Fundamentals of diophantine geometry.* Springer – Verlag 1983.

[21] S. Lang – *Complex multiplication.* Grundl. math. Wissensch. 255, Springer – Verlag 1983.

[22] H. Lange & C. Birkenhake - *Complex abelian varieties.* Grundl. math. Wissensch. 302, Springer – Verlag 1992.

[23] H. W. Lenstra jr & F. Oort – *Simple abelian varieties having a prescribed formal isogeny type.* Journ. Pure Appl. Algebra **4** (1974), 47 - 53.

[24] K.-Z. Li & F. Oort – *Moduli of supersingular abelian varieties.* Lecture Notes Math. 1680, Springer - Verlag 1998.

[25] Yu. I. Manin – *The theory of commutative formal groups over fields of finite characteristic.* Usp. Math. **18** (1963), 3-90; Russ. Math. Surveys **18** (1963), 1-80.

[26] D. Mumford – *A note of Shimura's paper "Discontinuous groups and abelian varieties".* Math. Ann. **181** (1969), 345 - 351.

[27] D. Mumford – *Geometric invariant theory.* Ergebn. Math. Vol. 34, Springer – Verlag 1965 (second version 1982, 1994).

[28] D. Mumford – *Abelian varieties.* Tata Inst. Fund. Research and Oxford Univ. Press 1970 (2nd printing 1974).

[29] D. Mumford – *The red book of varieties and schemes.* Lect. Notes Math. 1358, Springer – Verlag 1988.

[30] P. Norman – *An algorithm for computing moduli of abelian varieties.* Ann. Math. **101** (1975), 499 - 509.

[31] P. Norman – *Lifting abelian varieties.* Invent. Math. **64** (1981), 431 - 443.

[32] P. Norman & F. Oort – *Moduli of abelian varieties.* Ann. Math. **112** (1980), 413 - 439.

[33] A. Ogus – *Supersingular K3 crystals.* Journ. Géom. Algébr., Rennes 1978, Vol. II. Astérisque **64**, Soc. Math. France 1979, 3 - 86

[34] F. Oort – *Commutative group schemes.* Lect. Notes Math. 15, Springer - Verlag 1966.

[35] F. Oort – *The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field.* Journ. Pure Appl. Algebra **3** (1973), 399 - 408.

[36] F. Oort – *Subvarieties of moduli spaces.* Invent. Math. **24** (1974), 95 - 119.

[37] F. Oort – *Which abelian surfaces are products of elliptic curves?* Math. Ann. **214** (1975), 35 - 47.

[38] F. Oort – *Good and stable reduction of abelian varieties.* Manuscr. Math. **11** (1974), 171 - 197.

[39] F. Oort – *Endomorphism algebras of abelian varieties.* Algebraic Geometry and Commut. Algebra in honor of M. Nagata (Ed. H. Hijikata et al), Kinokuniya Cy Tokyo, Japan, 1988, Vol II; pp. 469 - 502.

[40] F. Oort – *CM-liftings of abelian varieties.* Journ. Algebraic Geometry **1** (1992), 131 - 146.

[41] F. Oort – *Some questions in algebraic geometry,* preliminary version. Manuscript, June 1995. http://www.math.uu.nl/people/oort/

[42] F. Oort — *Newton polygons and formal groups: conjectures by Manin and Grothendieck.* Ann. Math. **152** (2000), 183 - 206.

[43] F. Oort – *Newton polygon strata in the moduli space of abelian varieties.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 417 - 440.

[44] I. Reiner – *Maximal orders.* London Math. Soc. Monographs Vol. 28. Oxford 2003.

[45] *Schémas en groupes, Séminaire de géométrie algébrique, SGA3.* M. Demazure & A. Grothendieck. Vol I: Lect. Notes Math. 151, Springer – Verlag 1970.

[46] J-P. Serre – *Corps locaux.* Hermann Paris 1962.

[47] J-P. Serre & J. Tate – *Good reduction of abelian varieties.* Ann. Math. **88** (1968), 492 – 517.

[48] G. Shimura – *On analytic families of polarized abelian varieties and automorphic functions.* Ann. Math. **78** (1963), 149 – 193.

[49] G. Shimura & Taniyama – *Complex multiplication of abelian varieties and its applications to number theory.* Publ. Math. Soc. Japan **6**, Tokyo 1961.

[50] T. Shioda – *Supersingular K3 surfaces.* In: *Algebraic Geometry,* Copenhagen 1978 (Ed. K. Lønsted). Lect. Notes Math. 732, Springer - Verlag (1979), 564 - 591.

[51] J. Tate – *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134-144.

[52] J. Tate – *Classes d'isogénies de variétés abéliennes sur un corps fini (d'àpres T. Honda).* Sém. Bourbaki **21** (1968/69), Exp. 352.

[53] 2005-05 VIGRE number theory working group. Organized by Brian Conrad and Chris Skinner. On: http://www.math.Isa.umich.edu/ bdconrad/vigre04.html

[54] W. C. Waterhouse – *Abelian varieties over finite fields.* Ann. Sc. Ec. Norm. Sup. 4.Ser, **2** (1969), 521 – 560).

[55] W. C. Waterhouse & J. S. Milne – *Abelian varieties over finite fields.* Proc. Sympos. pure math. Vol. XX, 1969 Number Theory Institute (Stony brook), AMS 1971, pp. 53 – 64.

[56] A. Weil – *Sur les courbes algébriques et les variétés qui s'en déduisent.* Hermann 1948.

[57] A. Weil – *Variétés abéliennes et courbes algébriques.* Hermann 1948.

Frans Oort
Mathematisch Instituut
P.O. Box. 80.010
NL - 3508 TA Utrecht
The Netherlands
email: oort@math.uu.nl