Abelian varieties over finite fields

Frans Oort

May 2006

Preliminary version
Utrecht, Spring School on abelian varieties: May 2006

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 in this general, abstract theory it is often not easy to exhibit explicit examples, to construct abelian varieties with required properties.

A coarser classification is that of studying *isogeny classes of abelian varieties.* A wonderful and powerful theorem, the Honda-Tate theory, gives

a complete classification of isogeny classes of abelian varieties over a finite field,

see (1.1).

The basic idea starts with a theorem by A. Weil, a proof for the Weil conjecture for an abelian variety A over a finite field $K = \mathbb{F}_q$:

the geometric Frobenius π_A of A/K is an algebraic integer
which for every embedding $\psi : \mathbb{Q}(\pi_A) \to \mathbb{C}$ has absolute value $\mid \psi(\pi_A) \mid = \sqrt{q}$.

For an abelian variety A over $K = \mathbb{F}_q$ the assignment $A \mapsto \pi_A$ associates to A its geometric Frobenius π_A; the isogeny class of A gives the conjugacy class of the algebraic integer π_A, and

conversely such an algebraic integer, which is a Weil q-number,
determines an isogeny class, as J. Tate and T. Honda showed.

Geometric objects are constructed and 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, most of the times for a finite 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, fixed in these notes; we write ℓ for a prime number, which usually is different from the characteristic of the base field. We write $\mathbb{F} = \overline{\mathbb{F}_p}$.

In appendices we have gathered some information we need for statements and proofs of the main result. When reading these notes, anytime something seems unclear, please try to find the relevant notions in one of the appendices.

Instead of reading these notes it is much better to read the wonderful and clear [67]. Some proofs have been worked out in more detail in [68].

All material discussed below eventually will be contained in [GM]. That book by G. van der Geer and B. Moonen can be used as a reference for all material we need, and for all results we discuss. However, as a final version of this book is not yet available, we also give other references. In referring to [GM] we will usually not be precise as the final numbering can be different from the one available now.

Further recommended reading:
Abelian varieties: [40], [30], [9] Chapter V.
Honda-Serre-Tate theory: [67], [23], [68].
Abelian varieties over finite fields: [66], [69], [71].
Group schemes: [59], [46].
Endomorphism rings and endomorphism algebras: [66], [52], [69].

Contents:
§§ 1 – 8: material for this course,
§ 9: examples and exercises,
§§ 10 – 14: appendices giving definitions and background,
§ 15: questions and open problems.

1 Main topic/survey

(1) Below we will define: a Weil q-number, here $q = p^n$, see (2.1).

(2) 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 Weil q-number, a deep and important theorem by Weil, see (3.2).

(3) We will see, as Tate showed, that for simple abelian varieties A and B over a finite field K their Weil numbers π_A respectively π_B are conjugated, see (2.1), if and only if $A \sim_K B$, see (4.3).

(4) 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*

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

from the set of K-isogeny classes of K-simple abelian varieties defined over K and the set $W(q)$ of conjugacy classes of Weil q-numbers.
See [67]. The fact that the map is defined follows by Weil, the map is injective by Tate, and surjective by Honda.

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).

We sketch a proof of (1.1), which will be elaborated below. Write $K = \mathbb{F}_q$, with $q = p^n$. 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 $W(q)$.* Here $W(q)$ is the set of conjugacy classes of Weil q-numbers, see (2.1). This uses the Weil conjecture for abelian varieties over a finite field, see Section 3. We obtain the map

$$\{\text{simple AV over } \mathbb{F}_q\}/\sim \quad \longrightarrow \quad W(q).$$

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

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

See (4.3). 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. This shows that the map (A mod $\sim$) $\mapsto \pi_A$ is *injective.*

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 B' over K' with $\pi^N = \pi_{B'}$.*

Defintion: We say that π is *effective* if there exists A with $\pi \sim \pi_{A'}$. *In this step we prove that an appropriate power of a Weil q-number is effective.*

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

This result by Honda plus the last step shows that (A mod $\sim$) $\mapsto$ (π_A mod $\sim$) is *surjective.*

Hence the map

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

is bijective. This proves Theorem (1.1).

In 1966/1967 Serre wrote a letter to Tate in which he explained a proof of the Manin conjecture. That method proved the surjectivity result proved by Honda. Therefore, sometimes the theory discussed here is called the Honda-Serre-Tate theory. As Serre's proof was never published we can also use the terminology Honda-Tate theory.

2 Weil numbers and CM-fields

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

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

We say that π and π' are *conjugated* if there exists an isomorphism $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ mapping π to π'.

Equivalently: *the minimum polynomials of π and π' over $\mathbb{Q}$ are equal.*

Notation: $\pi \quad \sim \quad \pi'$. We write $W(q)$ for the set conjugacy classes of Weil q-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 on a CM-field corresponds with the restriction of complex conjugation on $\mathbb{C}$ to $\psi(L)$.

(2.3) Proposition. 3 *Let π be a Weil q-number. Then*

($\mathbb{R}$) *either for at least one $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \in \mathbb{R}$; in this case we have:*
 ($\mathbb{R}$e) *n is even, $\sqrt{q} \in \mathbb{Q}$, and $\pi = +p^{n/2}$, or $\pi = -p^{n/2}$; or*
 ($\mathbb{R}$o) *n is odd, $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$, and $\psi(\pi) = \pm p^{n/2}$.*
In particular in case (I) *we have $\psi(\pi) \in \mathbb{R}$ for every ψ.*

($\mathbb{C}$) *Or for every $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \not\in \mathbb{R}$* (equivalently: for at least one ψ we have $\psi(\pi) \not\in \mathbb{R}$). *In case* (II) *the field $\mathbb{Q}(\pi)$ is a* CM-*field.*

See (6.1), where we explain these cases in the Honda-Tate theory.

Proof. The claims in ($\mathbb{R}$) follow from the fact that $\pm p^{n/2}$ are precisely those real numbers with absolute value equal to $\sqrt{q}$.

If at least one embedding ψ gives $\psi(\pi) \not\in \mathbb{R}$, then we are not in case ($\mathbb{R}$), 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

$$\beta := \pi + \frac{q}{\pi}, \qquad (T - \psi(\pi))(T - \overline{\psi(\pi)}\ ) = T^2 - \beta T + q \in \mathbb{Q}(\beta)[T],$$

where β is a totally real integer. Hence $L_0 := \mathbb{Q}(\beta)$ is totally real. We are in the case that $\psi(\pi) \not\in \mathbb{R}$ for every ψ; hence L/L_0 is totally complex. □

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

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

and π 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 Weil q-numbers, see Section 9.

3 The Weil conjecture for abelian varieties over a finite field

(3.1) The geometric Frobenius. For a scheme $A \to S$ over a base $S \to \mathrm{Spec}(\mathbb{F}_p)$ in characteristic p there is the relative Frobenius

$$F_{A/S} : A \longrightarrow A^{(p)},$$

see (14.2). If moreover A/S is a group scheme this is a homomorphism. If $S = \mathrm{Spec}(\mathbb{F}_{p^n})$ there is a canonical identification $A^{(p^n)} \cong_S A$, and we obtain:

$$\left(A \quad \overset{F_{A/S}}{\longrightarrow} \quad A^{(p)} \quad \overset{F_{A^{(p)}/S}}{\longrightarrow} \quad \cdots \quad \longrightarrow \quad A^{(p^n)} = A\right) =: \pi_A,$$

called *the geometric Frobenius* of $A/\mathbb{F}_{p^n}$. Sometimes we will write (in abused notation) "$\pi_A = F^n$".

(3.2) Theorem (Weil). *Let A be a simple abelian variety over $K = \mathbb{F}_q$; consider the endomorphism $\pi_A \in \mathrm{End}(A)$, the geometric Frobenius of $A/\mathbb{F}_q$. The algebraic number π_A is a Weil q-number, i.e. for every embedding $\psi : \mathbb{Q}(\pi_A) \to \mathbb{C}$ we have*

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

See [72], page 70; [73], page 138; [40], Theorem 4 on page 206.

We indicate two facts which easily imply this result.

(3.3) Proposition. *For a simple abelian variety A over $K = \mathbb{F}_q$ we have*

$$\pi_A {\cdot} (\pi_A)^\dagger \quad = \quad q.$$

Here $\dagger : D \to D := \mathrm{End}^0(A)$ is the Rosati-involution.

One proof can be found in [40], formula (i) on page 206; also see [9], Coroll. 19.2 on page 144.

Another proof of (3.3) can be given by duality (see (14.9)):

$$\left(F_{A/S} : A \to A^{(p)}\right)^t \quad = \quad V_{A^t/S} : (A^{(p)})^t \to A^t.$$

From this we see that

$$\pi_{A^t} \cdot (\pi_A)^t = (F_{A^t})^n \cdot (V_{A^t})^n = p^n = q,$$

where we make the shorthand notation F^n for the n times iterated Frobenius morphism, and the same for V^n. See [GM], 5.21, 7.34 and Section 15. □(3.3)

(3.4) Proposition. *For any polarized abelian variety A over a field the Rosati-involution $\dagger : D \to D := \mathrm{End}^0(A)$ is positive definite bilinear form on D, i.e. for any non-zero $x \in D$ we have* $\mathrm{Tr}(x{\cdot}x^\dagger) > 0$.
See [40], Th. 1 on page 192, see [9], Th. 17.3 on page 138.

(3.5) We give a proof of (3.2) using (3.3) and (3.4). Note that $L = \mathbb{Q}(\pi_a)$ is the center of D, see (4.4) (1). Hence $\dagger$ on D induces an involution on L. Hence $\dagger$ induces an involution $\dagger_{\mathbb{R}}$ on $L \otimes_{\mathbb{Q}} \mathbb{R}$. This algebra is a finite product of copies of $\mathbb{R}$ and of $\mathbb{C}$. The involution $\dagger_{\mathbb{R}}$ is a positive definite $\mathbb{R}$-linear involution on this product. We see that this implies that $\dagger_{\mathbb{R}}$ is the identity on every real factor, stabilizes every complex factor, and is the complex conjugation on those factors. Conclusion:

$$\forall x \in L, \quad \forall\, \psi : L \to \mathbb{C} \quad \Rightarrow \quad \psi(x^{\dagger}) = \overline{\psi(x)}.$$

Hence

$$q = \pi_A{\cdot}(\pi_A)^{\dagger} = \psi\left(\pi_A{\cdot}(\pi_A)^{\dagger}\right) = \psi(\pi_A){\cdot}\overline{\psi(\pi_A)}.$$

Hence

$$\mid \psi(\pi_A) \mid \quad = \quad \sqrt{q}.$$

$\square$(3.2)

4 The structure of $\mathrm{End}^0(A)$: abelian varieties over finite fields by Tate

Main references: [66], [67].

(4.1) For a simple abelian variety over a field K the algebra $\mathrm{End}^0(A)$ is a division algebra. By the classification of Albert, see (13.1), we know the structure theorem of such algebras. Moreover, for any algebra in the list by Albert there is an abelian variety having this as endomorphism algebra. However over a finite field not all types do appear, there are restrictions.

(4.2) Tate described properties of the endomorphism algebra of a simple abelian variety over $K = \mathbb{F}_q$, with $q = p^n$. We write π_A for the geometric Frobenius of A, and f_A for the characteristic polynomial of π_A. We write Write Irr_{π_A} for the minimum polynomial of π_A over $\mathbb{Q}$.

The following theorems (and much more) are due to Tate, and can be found: [66], Theorem 1 on page 139, [66], Theorem 2 on page 140 and [67], Th. 1 on page 96.

(4.3) **Theorem** (Tate). *Let A be an abelian variety over the finite field $K = \mathbb{F}_q$. The characteristic polynomial $f_{A,\pi_A} = f_A \in \mathbb{Z}[T]$ of $\pi_A \in \mathrm{End}(A)$ is of degree $2{\cdot}\dim(A)$, the constant term equals $q^{\dim(A)}$ and $f_A(\pi_A) = 0$.*

The abelian variety A is K-simple if and only if f_A is a power of the minimum polynomial $\mathrm{Irr}(\pi_A) \in \mathbb{Z}[T]$.

Let A and B be abelian variety over $K = \mathbb{F}_q$. Then:

A is K-isogenous to an abelian subvariety of B iff f_A divides f_B.

In particular

$$A \sim_K B \quad \Longleftrightarrow \quad f_A = f_B.$$

(4.4) Theorem (Tate). **(1)** *The algebra* $\mathrm{End}^0(A)$ *is semi-simple. Suppose A is simple; the center of* $\mathrm{End}^0(A)$ *equals* $L := \mathbb{Q}(\pi_A)$.
(2) *Suppose A is* simple; *then*

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

where g is the dimension of A. Hence: every abelian variety over a finite field admits smCM. See (10.9). *We have:*

$$f_A \quad = \quad (\mathrm{Irr}_{\pi_A})^{\sqrt{[D:L]}}.$$

(3) *Suppose A is* simple,

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

The central simple algebra D/L

- *does not split at every real place of L,*
- *does split at every finite place not above p,*
- *and for $v \mid p$ the invariant of D/L is given by*

$$\mathrm{inv}_v(D/L) = \frac{v(\pi_A)}{v(q)}\cdot[L_v:\mathbb{Q}_p] \mod 1,$$

where L_v is the local field obtained from L by completing at v.

(4.5) Remark. Using Brauer theory, see Section 12, and using this theorem by Tate we see that the structure of D follows once $\pi = \pi_A$ is given. In particular the dimension g of A follows from π. *We will say that D is the algebra determined by the Weil number π.*

(4.6) Remark. An abelian variety over a field of characteristic zero which admits smCM is defined over a number field.

(4.7) Remark. The converse of Tate's result (4.4) (2) is almost true. Grothendieck showed: *Let A be an abelian variety over a field which admits smCM; then A is isogenous with an abelian variety defined over a finite extension of the prime field*; see [48].

It is easy to give an example of an abelian variety,(over a field of characteristic p, with smCM which is not defined over a finite field.

(4.8) Exercise. *Give an example of a simple abelian variety A over a field such that $A\otimes\overline{K}$ is not simple.*

(4.9) Exercise. Let $A \neq 0$ be an abelian variety over a field K. (Suggestion, see (10.7), and see (6.1).)
(1) *Show that* $\mathrm{End}^0(A)$ *is a semisimple ring.*
(2) *Prove: if $A \sim B^s$, where B is simple and $s \in \mathbb{Z}_{>0}$, then* $\mathrm{End}^0(A)$ *is a simple ring.*
(3) *Prove: if A is simple, then* $\mathrm{End}^0(A)$ *is a division algebra.*

Assume Theorem (1.1) to be true. For any Weil number π consider a simple abelian variety A over a finite field with $\pi \sim \pi_A$. See (4.4), and see Section 13 for notation of invariants of $D = \mathrm{End}^0(A)$.

(4.10) Exercise. *For each of the numbers below show it is a Weil number, determine q, determine the invariants e_0, e, d, g, describe the structure of D, and describe the structure of* $\mathrm{End}^0(A \otimes_K K')$ *for any field extension $K \subset K'$.*
(1) $\pi = \sqrt{-p}$,
(2) $\zeta = \zeta_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}, \quad \pi = \zeta{\cdot}\sqrt{-p}$,
(3) π is a zero of $T^2 - \sqrt{2}{\cdot}T + 8$,

5 Injectivity

(5.1) Exercise/Construction. Let K be a field, and let A and B be abelian varieties over K. Assume there exists an isogeny $\varphi : A \to B$. Choose an isogeny $\psi : B \to A$ and an integer $N > 0$ such that $\psi{\cdot}\varphi = N{\cdot}1_A$. Construct

$$\Phi : \quad \mathrm{End}^0(A) \quad \longrightarrow \quad \mathrm{End}^0(B), \quad \Phi(x) := \frac{1}{N}{\cdot}\varphi{\cdot}x{\cdot}\psi.$$

(1) *Show that Φ is a homomorphism. Construct Ψ by $\Psi(y) = \psi{\cdot}y{\cdot}\varphi/N$. Show $\Psi{\cdot}\Phi = Id$ and $\Phi{\cdot}\Psi = Id$. Conclude that*

$$\Phi : \quad \mathrm{End}^0(A) \quad \xrightarrow{\sim} \quad \mathrm{End}^0(B)$$

is an isomorphism.
(2) *Show that Φ is independent of the choice of ψ and N.*
(3) *Show that $\varphi{\cdot}\psi = N{\cdot}1_B$.*

(5.2) Exercise. Let $A \sim B$ be a K-isogeny of simple abelian varieties over a finite field $K = \mathbb{F}_q$; *show: this isogeny gives an isomorphism $\mathbb{Q}(\pi_A) \cong \mathbb{Q}(\pi_B)$*, use (5.1). *Show that this maps π_A tot π_B.*

(5.3) By Theorem (3.2) by Weil we see that for a simple abelian variety A over $K = \mathbb{F}_q$ indeed π_A is a Weil q-number. If A and B are K- isogenous, π_A and π_B are conjugated. Hence

$$\boxed{\{\text{simple abelian variety over} \quad K\}/\sim_K \quad \longrightarrow \quad W(q), \qquad A \mapsto \pi_A,}$$

is well-defined.

We have seen in (4.3) (2) that Tate showed that A and B are K-isogenous if and only if $f_A = f_B$. Hence this map is *injective.*

6 Newton polygons, the Manin conjecture

In later sections we will indicate parts of a proof for Theorem (1.1). In this section we assume this theorem, we draw some conclusions, and we show an important application.

(6.1) Let π be a Weil q-number. Let $\mathbb{Q} \subset L \subset D$ be the central algebra determined by π. We remind the reader that

$$[L : \mathbb{Q}] =: e, \quad [D : L] =: d^2, \quad 2g := e{\cdot}d. \qquad \text{See Section 13.}$$

As we have seen in Proposition (2.3) there are three possibilities:

($\mathbb{R}$e) *Either $\sqrt{q} \in \mathbb{Q}$, and $q = p^n$ with n an* **even** *positive integer.* $\boxed{\text{Type III}(1), \quad g = 1}$
In this case $\pi = +p^{n/2}$, or $\pi = -p^{n/2}$. Hence $L = L_0 = \mathbb{Q}$. We see that $D/\mathbb{Q}$ has rank 4, with ramification exactly at ∞ and at p. We obtain $g = 1$, we have that $A = E$ is a supersingular elliptic curve, $\mathrm{End}^0(A)$ is of Type III(1), a definite quaternion algebra over $\mathbb{Q}$. This algebra was denoted by Deuring as $\mathbb{Q}_{p,\infty}$. Note that "all endomorphisms of E are defined over K", i.e. for any

$$\forall \quad K \subset K' \quad \text{we have} \quad \mathrm{End}(A) = \mathrm{End}(A \otimes K').$$

($\mathbb{R}$o) *Or $q = p^n$ with n an* **odd** *positive integer and $\sqrt{q} \notin \mathbb{Q}$.* $\boxed{\text{Type III}(2), \quad g = 2}$
In this case $L_0 = L = \mathbb{Q}(\sqrt{p})$, a real quadratic field. We see that D ramifies exactly at the two infinite placeswith invariants equal to $(n/2){\cdot}2/(2n) = 1/2$. Hence D/L_0 is a definite quaternion algebra over L_0, it is of Type III(2). We conclude $g = 2$. If $K \subset K'$ is an extension of odd degree we have $\mathrm{End}(A) = \mathrm{End}(A \otimes K')$. If $K \subset K'$ is an extension of even degree $A \otimes K'$ is non-simple, it is K'-isogenous with a product of two supersingular elliptic curves, and $\mathrm{End}^0(A \otimes K')$ is a 2×2 matrix algebra over $\mathbb{Q}_{p,\infty}$, and

$$\forall \quad 2 \mid [K' : K] \quad \text{we have} \quad \mathrm{End}(A) \neq \mathrm{End}(A \otimes K').$$

($\mathbb{C}$) *For at least one embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \notin \mathbb{R}$.* $\boxed{\text{IV}(e_0, d), \quad g := e_0{\cdot}d}$
In this case all conjugates of $\psi(\pi)$ are non-real. We can determine $[D : L]$ knowing all $v(\pi)$ by (4.4) (3); here d is the greatest common divisor of all denominators of $[L_v : \mathbb{Q}_p]{\cdot}v(\pi)/v(q)$, for all $v \mid p$. This determines $2g := e{\cdot}d$. The endomorphism algebra is of Type IV(e_0, d). For $K = \mathbb{F}_q \subset K' = \mathbb{F}_{q^m}$ we have

$$\mathrm{End}(A) = \mathrm{End}(A \otimes K') \quad \Longleftrightarrow \quad \mathbb{Q}(\pi) = \mathbb{Q}(\pi^m).$$

We recall an important corollary from the Honda-Tate theory, as observed independently by Serre.

(6.2) Let A be an abelian variety in positive characteristic, and let $\xi = \mathcal{N}(A)$ be its Newton polygon, see Section 14. Then ξ is *symmetric*. This means that the slopes β and $1 - \beta$ appear with the same multiplicity. Over a finite field this was proved by Manin. The general case follows from the duality theorem, see (10.3), see [46], Theorem 19.1.

Does the converse hold? I.e.:

Conjecture (Manin, see [33], Conjecture 2 on page 76).
Suppose given a prime number p and a symmetric Newton polygon ξ. Then there exists an abelian variety A over a field of characteristic p with $\mathcal{N}(A) = \xi$.

Actually if such an abelian variety does exist, then there exists an abelian variety with this Newton polygon over a finite field. This follows by a result of Grothendieck and Katz about Newton polygon strata being Zariski closed; see [27], Th. 2.3.1 on page 143.

(6.3) **Proof of the Manin Conjecture** (Serre, Honda), see [67], page 98. We recall that Newton polygons can be described by a sum of ordered pairs (d, c). A symmetric Newton polygon can be written as

$$\xi = f{\cdot}\left((1,0) + (0,1)\right) + s{\cdot}(1,1) + \sum_i \quad \left((d_i, c_i) + (c_i, d_i)\right),$$

with $f \geq 0, \quad s \geq 0$ and $d_i > c_i > 0$ being coprime integers. Note that $\mathcal{N}(A) \cup \mathcal{N}(B) = \mathcal{N}(A \times B)$. We know that for an ordinary elliptic curve E we have $\mathcal{N}(E) = (1,0) + (0,1)$, and for a sypersingular elliptic curve we have $\mathcal{N}(E) = (1,1)$, and both types exist. Hence the Manin Conjecture has been settled if we can handle the case

$$(d,c) + (c,d) \text{ with } \gcd(d,c) = 1 \text{ and } d > c > 0 \text{ being coprime integers.}$$

For such integers we consider a zero π of the poynomial

$$P = T^2 + p^c{\cdot}T + p^n, \qquad n = d + c, \quad q = p^n.$$

Clearly $(p^c)^2 - 4{\cdot}p^n < 0$, and we see that π is an imaginary quadratic Weil q-number. Note that

$$(T^2 + p^c{\cdot}T + p^n)/p^{2c} \quad = \quad (\frac{T}{p^c})^2 + \frac{T}{p^c} + p^{d-c}.$$

As $d > c$, we see that $L = \mathbb{Q}(\pi)/\mathbb{Q}$ is an imaginary quadratic extension in which p splits. Moreover, using (4.4) (3), the Newton polygon of P tells us the p-adic values of zeros of P; this shows that the invariants of D/L are c/n and d/n. This proves that $[D : L] = n^2$. Using Theorem (1.1) we have proved the existence of an abelian variety A over $\mathbb{F}_q$ with $\pi = \pi_A$, hence $\mathrm{End}^0(A) = D$. In particular the dimension of A equals $n = d + c$.

Claim. $\mathcal{N}(A) = (d,c) + (c,d)$

Note that $D \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong D_1 \times D_2$, where D_1 and D_2 are central division algebras over $\mathbb{Q}_p$ both of degree n^2. Note that $\mathrm{End}(A) = \mathcal{O}$ is an order in D; hence $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ acts on $A[p^\infty]$. The splitting of $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ induces a splitting up to isogeny $A[p^\infty] \sim X_1 \times X_2$; write $\pi = (\pi^{(1)}, \pi^{(2)}) \in \mathrm{End}^0(X_1) \times \mathrm{End}^0(X_2)$. We know that $\pi = \pi_A$, the geometric Frobenius of A, acts with slopes d respectively c; by this we mean that the component $\pi^{(1)} \in D_1 = \mathrm{End}^0(X_1)$ has the property that $p^d/\pi^{(1)}$ is a unit, i.e. has v_1-valuation zero, and the analogous statement for $\pi^{(2)} \in D_2 = \mathrm{End}^0(X_2)$ (order the choice of indices for the X_i in this way). Hence the F-slope of X_1 equals d/n and the F-slope of X_2 equals c/n. This proves $\mathcal{N}(A) = (d,c) + (c,d)$. Hence the Manin conjecture is proved. □

(6.4) Exercise. Let A be an elliptic curve over a local field in mixed characteristic zero/p, such that $\mathrm{End}(A) \supsetneqq \mathbb{Z}$. Let $E = \mathrm{End}^0(A)$. Note that $E/\mathbb{Q}$ is an imaginary quadratic extension. Suppose A has good reduction modulo p. Show:

If p is ramified or if p is inert in $\mathbb{Q} \subset E$ then A_0 is supersingular.

If p is is split in $\mathbb{Q} \subset E$ then A_0 is ordinary.

(Note that in the case studied $\mathrm{End}(A) \hookrightarrow \mathrm{End}(A_0)$; you may use this.)

(6.5) Exercise. Let A be a simple abelian variety over the finite field $K = \mathbb{F}_{p^n}$. Write $P_A := \mathrm{Irr}_{\pi_A}$ for the minimum polynomial over $\mathbb{Q}$ of the geometric Frobenius of A/K, and let f_A be the characteristic poloynomial of$\pi_A \in \mathrm{End}(A)$. (Note that $f_A = (P_A)^d$.) *Show that $\mathcal{N}(A)$ can be read off from P_A and from f_A.* By his we mean: let $\mathrm{NP}(P_A)$ be the Newton polygon of $P_A \in \mathbb{Z}[T] \subset \mathbb{Q}_p[T]$. Consider the polygon obtained from $\mathrm{NP}(P_A)$ by streching the horizontal axis by a factor d and compressing the vertical axis by a factor n. Starting from $\mathrm{NP}(P_A)$ *this process produces the Newton polygon $\mathcal{N}(A)$ of A.*

(6.6) Exercise. (1) Fix a prime number p, fix coprime positive integers $d > c > 0$. Consider all division algebras D such that there exists an abelian variety A of dimension $g := d + c$ over some finite field of characteristic p such that $[\mathrm{End}^0(A) : \mathbb{Q}] = 2g^2$ and $\mathcal{N}(A) = (d,c) + (c,d)$. *Show that this gives a infinite set of isomorphism classes of such algebras.* (E.g. see the second proof of [8]. 4.9).
(2) Fix a prime number p, and fix a symmetric Newton polygon $\xi \neq \sigma$. Consider all fields such that there exists an abelian variety A over some finite field of characteristic p such that $\mathcal{N}(A) = \xi$. *Show that this gives an infinite set of isomorphism classes of such fields.*
(If you prefer, do this exercise first for $\xi = (1,0) + (0,1)$, then for $\xi = (2,1) + (1,2)$.)

7 Liftings of abelian varieties

In this section, the heart of the proof of Theorem (1.1), we follow Honda's results as explained by Tate. Basic references: [23], and [67], §3.

We want to construct an abelian variety over a finite field with a given geometric Frobenius. We do not know a direct method to construct such an abelian variety. However over the complex numbers we have lattices, complex tori, algebraizebility at our disposal. The main idea of the proof is, to construct a complex abelian with CM, to show it is defined and has good reduction over a local p-adic field, in such a way that the reduction modulo p gives the required Weil number. We will see that this idea leads to success, however not directly...

(7.1) Definition *We say that a Weil q-number π is* effective *if there exists an abelian variety A over $\mathbb{F}_q$ such that $\pi = \pi_A$.* I.e. π is effective if it is in the image of the map $A \mapsto \pi_A$.

We intend to show in this section:

(7.2) Theorem. *Let A be a simple abelian variety over a finite field K. There exists a finite extension $K \subset K'$, an abelian variety B over K', and a K'-isogeny $A \otimes_K K' \sim B$ such that B adits a* CM-*lift to characteristic zero.*
See [67], Th. 2 on page 102.
For the definition of a CM-lift, see (15.1). here it means that there exists a field $L \subset E \subset D = \mathrm{End}^0(B)$, with $[E : \mathbb{Q}] = 2{\cdot}\dim(A)$ (hence E/L is a splitting field for D/L) and E is a CM-field and a lift of B to an abelian scheme over a characteristic zero domain with CM by E.

(7.3) Corollary. *For every Weil q-number π there exists an integer $N > 0$ such that π^N is effective.*

(7.4) Suppose $M \supset R \twoheadrightarrow K$, where R is a domain and $M = Q(R)$ the field of fractions, and K a residue field. Suppose $A \to \mathrm{Spec}(R)$ is an abelian scheme. Then

$$\mathrm{End}(A_M) \xrightarrow{\sim} \mathrm{End}(A) \hookrightarrow \mathrm{End}(A_K).$$

Exercise. *In case ℓ is a prime number not equal to the characteristic of K, show that* $\mathrm{End}(A_K)/\mathrm{End}(A)$ *has no ℓ-torsion.*

Exercise. *Give an example where* $\mathrm{End}(A_K)/\mathrm{End}(A)$ *does have torsion.*

We conclude that we obtain $\mathrm{End}^0(A) \hookrightarrow \mathrm{End}^0(A_K)$. In general this is not an equlity.

Exercise. *Give examples of A over R such that* $\mathrm{End}^0(A) \subsetneqq \mathrm{End}^0(A_K)$.

(7.5) In order to be able to lift an abelian variety from characteristic p to characteristic zero, and to have a good candidate in characteristic zero whose reduction modulo p gives the required Weil number we have to realize that in general an endomorphism algebra in positive characteristic does not appear for that dimension as an endomorphism algebra in characteristic zero. However "less structure" will do:

(7.6) Lemma. *Suppose given a Weil q-number π. Let $\mathbb{Q} \subset L = \mathbb{Q}(\pi) \subset D$ the algebra determined by π, see* (4.4) (3). *Then there exists a field $L \subset E \subset D$ such that $[E : L] = \sqrt{[D : L]}$* , hence E/L is a splitting field for D/L, *and such that E is a* CM*-field.*
See [67], Lemme 2 on page 100.

(7.7) Construction/Proposition. *Suppose given a Weil q-number π. Let $\mathbb{Q} \subset L = \mathbb{Q}(\pi) \subset E \subset D$ as in the previous lemma. Then there exists an integer $N \in \mathbb{Z}_{>0}$, a finite extension $\mathbb{Q}_p \subset M$ with residue class field $\mathbb{F}_{q^N}$, and an abelian variety B over M with* $\mathrm{End}(B) = L$*, such that B has good reduction, and such that the reduction B_0 modulo p satisfies $\pi_{B_0} = \pi^N$.*
See [67], Lemme 3 on page 100.

Clearly (7.6) and (7.7) give a proof for (7.2) and (7.3).

(7.8) Remark. Actually Theorem (7.2) can be formulated in a stronger way: for every E as in (7.6) there exists a CM-lift of B to characteristic zero having CM by the field E.

(7.9) Exercise *. Let E be an elliptic curve over a field $K \supset \mathbb{F}_p$. Let $X = E[p^\infty]$ be its p-divisible group. Show:

(1) For every $\beta \in End(X)$ the pair (X, β) can be lifted to characteristic zero.

For every $b \in$ $\mathrm{End}(E)$ *the pair (E, b) can be llifted to characteristic zero.* See [53], Section 14, in particular 14.7.

Remark/Exercise. *There exists an elliptic curve E over a local field M such that E has good reduction, such that* $\mathrm{End}(E) = \mathbb{Z}$ *and* $\mathrm{End}(E[p^\infty]) \supsetneqq \mathbb{Z}_p$.

Remark. We see that in order that the Tate conjecture holds for abelian varieties we better assume that the base field is of finite type over the prime field; therefore Grothendieck formulated his "anabelian conjecture" for hyperbolic curves over such fields; it came as a big surprise that this conjecture for curves actually is true over local fields, as Mochizuchi showed, see [34].

In a proof for (7.7) we will use:

(7.10) Lemma. *Let E be a number field, i.e. $[E : \mathbb{Q}] < \infty$. A root of unity $\zeta \in E$ has the properties:*
(i) for every $\psi : E \to \mathbb{C}$ we have $\mid \zeta \mid = 1$,

(ii) for every finite prime w we have $w(\zeta) = 0$.
Conversely an element $\zeta \in E$ satisfying (i) and (ii) is a root of unity.
See [22], page 402 (page 520 in the second printing).

8 Surjectivity

Warning. For a K-simple abelian variety A over $K = \mathbb{F}_q$ in general it can happen that for a (finite) extension $K \subset K'$ the abelian variety $A \otimes K'$ is not K'-simple.

(8.1) Exercise. *Notation and assumptions as above; in particular $K = \mathbb{F}_q$ is a finite field, $[K' : K] = N$. Write $A' = A \otimes K'$. Write $\pi' = \pi_A^N$.*

Show that $\mathrm{End}(A) = \mathrm{End}(A')$ *iff* $\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi')$.

Show that $\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi')$ implies that A' is K'-simple.

Construct K, A, K' such that $\mathbb{Q}(\pi_A) \neq \mathbb{Q}(\pi_{A'})$ and A' is K'-simple.

(8.2) Lemma. *Let π be a Weil q-number and $N \in \mathbb{Z}_{>0}$ such that π^N is effective. Then π is effective.*
See [67], Lemme 1 on page 100.

(8.3) The Weil restriction functor. Suppose given a finite extension $K \subset K'$ of fields (we could consider much more general stiuations, but we will not do that); write $S = \mathrm{Spec}(K)$ and $S' = \mathrm{Spec}(K')$. We have the base change functor

$$\mathrm{Sch}_{/S} \quad \longrightarrow \quad \mathrm{Sch}_{S'}, \qquad T \mapsto T_{S'} := T \times_S S'.$$

The *right adjoint functor* to the base change functor is denoted by

$$\Pi = \Pi_{S'/S} = \Pi_{K'/K} \ : \ \mathrm{Sch}_{S'} \quad \longrightarrow \quad \mathrm{Sch}_{/S}, \qquad \mathrm{Hom}_S(T, \Pi_{S'/S}(Z)) \cong \mathrm{Hom}_{S'}(T_{S'}, Z).$$

In this situation Weil showed that $\Pi_{S'/S}(Z)$ exists. In fact, consider $\times_{S'}^{[K':K]} = Z \times_{S'} \cdots \times_{S'} Z$, the self-product of $[K' : K]$ copies, and it can be shown that $\times_{S'}^{[K':K]}$ can be descended to K in such a way that it solves this problem. Note that $\Pi_{S'/S}(Z) \times_S S' = \times_{S'}^{[K':K]} Z$. For a more general situation, see [20], Exp. 195, page 195-13.

(8.4) Lemma. *Let B' be an abelian variety over a finite field K'. Let $K \subset K'$, with $[K' : K] = N$. Write*

$$B := \Pi_{K'/K}\ B'; \quad \textit{then} \quad f_B(T) = f_{B'}(T^N).$$

See [67], page 100.

Let π be Weil q-number. By (7.3) there exists $N \in \mathbb{Z}_{>0}$ such that $\pi^N = \pi_{B'}$ for some abelian variety B' over $K' = \mathbb{F}_{q^N}$. Write $B := \Pi_{K'/K}\ B'$. By the previous lemma we see that π is a zero of $f_B(T)$. By (4.3) we conclude that there is a simple abelian variety A over K isogenous to a subvariety B such that $\pi = \pi_A$; this proves (8.2), it shows that π is effective; hence $A \mapsto \pi_A$ is surjective. Hence Theorem (1.1) has been proved. $\square$(1.1)

(8.5) Exercise. *Show that for any prime number p there exists a supersingular curve over* $\mathbb{F}_p$; do not use Honda-Tate theory, do not use methods of characteristic zero.

9 Some examples

(9.1) 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 $B_0 \otimes_{K_0} K' \cong A \otimes_K K'$. – An exercise below shows that this does not imply in general that we can choose B_0 such that $B_0 \otimes_{K_0} K \cong A$.

(9.2) Exercise. We say that E an elliptic curve (an abelian variety of dimension one) defined over a field M of characteristic p is *supersingular* if $E[p](\overline{M}) = 0$.
(1) *Let E be a supersingular elliptic curve over some field $M \supset \mathbb{F}_p$. Show that*

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

(2) *Show that $j(E) \in \mathbb{F}_{p^2}$.*
(3) *Show that E can be defined over* $\mathbb{F}_{p^2}$.

(9.3) Remark. As Deuring showed, for any elliptic curve E we have $(j(E) \in K) \Rightarrow (E$ can be defined over $K)$. An obvious generalization for abelian varieties of dimension $g > 1$ does not hold; in general it is difficult to determine a field of definition for A, even if a field of definition for its moduli point is given.
In fact, as in formulas given by Tate, see [65] page 52, we see that for $j \in K$ an elliptic curve over K with that j invariant exists:

- $\mathrm{char}(K) \neq 3$, $j = 0$: $Y^2 + Y = X^3$;
- $\mathrm{char}(K) \neq 2$, $j = 1728$: $Y^2 = X^3 + X$;
- $j \neq 0$, $j \neq 1728$:
$$Y^2 + XY = X^3 - \frac{36}{j - 1728}X - \frac{1}{j-1728}.$$

Deuring showed that the endomorphism algebra of a supersingular elliptic curve over $\mathbb{F} = \overline{\mathbb{F}_p}$ is the quaternion algebra $\mathbb{Q}_{p,\infty}$; this is the division algebra, of degree 4, central over $\mathbb{Q}$ unramified outside $\{p, \infty\}$. This was an inspriration for Tate to prove his structure theorems for endomorphism algebras of abelian varieties defined over a finite field, and as Tate already remarked, it reproved Deuring's result.

(9.4) Endomorphism algebras of eliptic curves. *Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$. We write $\mathbb{Q}_{p,\infty}$ for the quaternion algebra central over $\mathbb{Q}$, ramified exactly at the places ∞ and p. One of the following three (mutually exclusive) cases holds:*

(1) (2.1.s) $\boxed{E \textit{ is ordinary; then } \mathrm{End}^0(E) = L = \mathbb{Q}(\pi_E)}$
is an imaginary quadratic field in which p **splits**. *Conversely if* $\mathrm{End}^0(E) = L$ *is a quadratic*

field in which p splits, E is ordinary. In this case, for every field extension $K \subset M$ we have $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes M)$.

(2) (2.1.ns) $\boxed{\textit{E is supersingular, and } \mathrm{End}^0(E) \cong \mathbb{Q}_{p,\infty}.}$

This is the case if and only if $\pi_E \in \mathbb{Q}$. For every field extension $K \subset M$ we have $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes M)$.

(3) (1.2) $\boxed{\textit{E is supersingular, and } \mathrm{End}^0(E) = L \supsetneqq \mathbb{Q}.}$

In this case $L/\mathbb{Q}$ is an imaginary quadratic field in which p does **not split**. *There exists an integer N such that $\pi_e^N \in \mathbb{Q}$. In that case* $\mathrm{End}^0(E \otimes M) \cong \mathbb{Q}_{p,\infty}$ *for any field M containing* $\mathbb{F}_{q^N}$.

If E is supersingular over a finite field either (2.1.ns) *or* (1.2) *holds.*

A proof can be given using (9.6). Here we indicate a proof independent of that classification of all elliptic curves over a finite field.

Proof. By (4.4) we know that for an elliptic curve e over a finite field we have $L := \mathbb{Q}(\pi_E)$ and $D = \mathrm{End}^0(E)$ and

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

Hence $e = 2, d = 1$ or $e = 1, d = 2$. We obtain three cases:

(2.1.s) $[L:\mathbb{Q}] = e = 2$ and $D = L$, hence $d = 1$, and p is split in $L/\mathbb{Q}$.
(2.1.ns) $[L:\mathbb{Q}] = e = 2$ and $D = L$, hence $d = 1$, and p is not split in $L/\mathbb{Q}$.
(1.2) $L = \mathbb{Q}$, $[D:\mathbb{Q}] = 4$; in this case $e = 1$, $d = 2$ and $D \cong \mathbb{Q}_{p,\infty}$.

Moreover we have seen that either $\pi_E \in \mathbb{R}$, and we are in case (1.2) or $\pi_E \notin \mathbb{R}$ and $D = L := \mathbb{Q}(\pi_E) = \mathbb{Q}$ and $L/\mathbb{Q}$ is an imaginary quadratic field.

Write $\overline{E}$ for $E \otimes \mathbb{F}$. For a p-divisible group X write $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We have the natural maps

$$\mathrm{End}(E) \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Z}_p \hookrightarrow \mathrm{End}(E[p^\infty]) \hookrightarrow \mathrm{End}^0(E[p^\infty]) \hookrightarrow \mathrm{End}^0(\overline{E}[p^\infty]).$$

Indeed the ℓ-adic map $\mathrm{End}(A) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{End}(T_\ell(E))$ is injective, as was proved by Weil. The same arguments of that proof are valid for the injectivity of $\mathrm{End}(A) \otimes \mathbb{Z}_p \hookrightarrow \mathrm{End}(A[p^\infty])$ for any abelian variety over any field, see (11.7), see [71], Theorem 5 on page 56. Hence

$$\mathrm{End}^0(E) \hookrightarrow \mathrm{End}^0(E) \otimes \mathbb{Q}_p \hookrightarrow \mathrm{End}^0(E[p^\infty]).$$

Claim (One) (2.1.ns) or (1.2) $\Longrightarrow$ E is supersingular.

Proof. *Suppose* (2.1.ns) *or* (1.2), *suppose that E is ordinary, and arrive at a contradiction.* If E is ordinary we have

$$E[p^\infty] \otimes \overline{K} \quad = \quad \overline{E}[p^\infty] \otimes \overline{K} \quad \cong \quad \mu_{p^\infty} \times \underline{\mathbb{Q}_p/\mathbb{Z}_p}.$$

Moreover

$$\mathrm{End}^0(\mu_{p^\infty}) \quad = \quad \mathbb{Z}_p, \qquad \mathrm{End}^0(\underline{\mathbb{Q}_p/\mathbb{Z}_p}) \quad = \quad \mathbb{Z}_p$$

(over any base field). In case (2.1.ns) we see that $D_p = \mathrm{End}^0(E) \otimes \mathbb{Q}_p$ is a quadratic extension of $\mathbb{Q}_p$. In case (1.2) we see that $D_p = \mathrm{End}^0(E) \otimes \mathbb{Q}_p$ is a quaternion algebra over $\mathbb{Q}_p$. In both cases we obtain

$$\mathrm{End}(E) \to \mathrm{End}^0(E) \otimes \mathbb{Q}_p \to \mathrm{End}^0(\overline{E}[p^\infty] \otimes \overline{K}) = \mathrm{End}^0(\mu_{p^\infty} \times \underline{\mathbb{Q}_p/\mathbb{Z}_p}) = \mathbb{Q}_p \times \mathbb{Q}_p.$$

As $(D_p \to \mathbb{Q}_p) = 0$ we conclude that $(\mathrm{End}(E) \to \mathrm{End}(E[p^\infty])) = 0$; this is a constradiction with the fact that the map $\mathbb{Z} \hookrightarrow \mathrm{End}(E) \to \mathrm{End}(E[p^\infty])$ is non-zero. Hence Claim (One) has been proved. □

Claim (Two) (2.1.s) $\Longrightarrow$ E is ordinary.

Proof. *Suppose* (2.1.s), *suppose that E that E is supersingular, and arrive at a contradiction.* Note that $E'[p^\infty]$ is a simple p-divisble group for any supersingular curve E' over any field. Hence $\mathrm{End}^0(E[p^\infty])$ is a division algebra. Suppose that we are in case (2.1.s). Then $\mathbb{Q}(\pi_E) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p \times \mathbb{Q}_p$. This shows that if this were true we obtain an injective map

$$\mathbb{Q}(\pi_E) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p \times \mathbb{Q}_p \hookrightarrow \mathrm{End}^0(E) \otimes \mathbb{Q}_p \hookrightarrow \mathrm{End}^0(E[p^\infty])$$

from $\mathbb{Q}_p \cong \mathbb{Q}_p$ into a division algebra; this is a contradiction. This proves Claim (Two). □

By Claim (One) and Claim (Two) it follows that

$$E \text{ is ordinary} \Longleftrightarrow (2.1.s), \qquad E \text{ is supersingular} \Longleftrightarrow (\ (2.1.ns) \text{ or } (1.2)\ ).$$

Claim (Three) If E is supersingular then for some $N \in \mathbb{Z}_{>0}$ we have $\pi_E^N \in \mathbb{Q}$.

Proof. If we are in case (1.2) we know $\pi_E \in \mathbb{Q}$.

Suppose we are in case (2.1.ns), and write $L = \mathbb{Q}(\pi_E)$. Write $\pi = \pi_E$ and consider $\zeta = \pi^2/q \in L$.

- Note that ζ has absolute value equal to one for every complex embedding (by the Weil conjecture), see (3.2).
- Note that for any discrete valuation v' of L not dividing p the element ζ is a unit at v'. Indeed π factors p^n, so π is a unit at w.
- As we are in case (2.1.ns) there is precisely one prime v above p.

The product formula $\Pi_w \mid \zeta \mid_w = 1$, the product running over all places of L, in the number field L (see [22], second printing, §20, absolute values suitably normalized) then shows that ζ is also a unit at v. By (7.10) we conclude that ζ is a root of unity. This proves Claim (Three). □

We finish the proof. If E is ordinary, $\mathrm{End}^0(E \otimes M)$ is not of degree four over $\mathbb{Q}$, hence $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes M)$ for any ordinary eliptic curve over a finite field K , and any extension $K \subset M$.

If we are in case (1.2) clearly we have $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes M)$ for any extension $K \subset M$.

If we are in case (2.1.ns) we have seen in Claim (Three) that for some $N \in \mathbb{Z}_{>0}$ we have $\pi_E^N \in \mathbb{Q}$. Hence for every $K \subset \mathbb{F}_{q^N} \subset M$ we have

$$\mathrm{End}^0(E) = L = \mathbb{Q}(\pi_E) \subsetneqq \mathrm{End}^0(E \otimes M) \cong \mathbb{Q}_{p,\infty}.$$

□

(9.5) Definition/Remark/Exercise. (1) An abelian variety A of dimension g over a field $K \supset \mathbb{F}_p$ is called *supersingular* if there exists an isogeny $A \otimes k \sim E^g \sim k$, where E is a supersingular elliptic curve, and k is algebraically closed.
(2) Tate and Oort showed:

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

where $\sigma = g(1,1)$ is the Newton polygon having only slopes equal to zero.
(3) We see that $g > 1$ and $\mathcal{N}(A) = \sigma$ implies that A is not absolutely simple. This is an exceptional case. Indeed, for any symmetric Newton polygon $\xi \neq \sigma$ and any p there exists an absolutely simple abelian variety A in characteristic p with $\mathcal{N}(A) = \xi$; see [31].
(4) Let A be a simple abelian variety over the finite field $\mathbb{F}_q$. Show:

$$A \text{ is supersingular} \quad \Longleftrightarrow \quad \pi_A \sim \zeta{\cdot}\sqrt{q},$$

where ζ is a root of unity.

(9.6) Classification of all elliptic curves over finite fields.
See [69], Th. 4.1 on page 536.

Let E be an elliptic curve over a finite field $K = \mathbb{F}_q$, with $q = p^n$, and $\pi = \pi_E$. Then $\mid \pi \mid = \sqrt{q}$ (for every embedding into $\mathbb{C}$), hence $\pi + \overline{\pi} =: \beta \in \mathbb{Z}$ has the property $\mid \beta \mid \leq 2\sqrt{q}$. For every E over a finite field $\pi = \pi_E$ is a zero of

$$P = T^2 - \beta{\cdot}T + q, \qquad \beta^2 \leq 4q.$$

The Newton polygon of E equals the Newton polygon of P with the vertical axis compressed by n. Hence:

$$(p \text{ does not divide } \beta) \quad \Longleftrightarrow \quad (E \text{ is ordinary}),$$

and

$$(v_p(\beta) > 0) \quad \Longleftrightarrow \quad (E \text{ is supersingular}) \quad \Longleftrightarrow \quad v_p(\beta) \geq v_p(q)/2 = n/2.$$

We write $D = \mathrm{End}^0(E)$, $\quad L = \mathbb{Q}(\pi)$, $\quad e = [L : \mathbb{Q}]$, $\quad \sqrt{[D : \mathbb{Q}]} = d$. Note that $ed = 2$. Hence $L = \mathbb{Q}$ iff $D \cong \mathbb{Q}_{p,\infty}$. If $L/\mathbb{Q}$ is quadratic, then L is imaginary. Note that if L is quadratic over $\mathbb{Q}$ then E is supersingular iff p is non-split in $L/\mathbb{Q}$.

We have the following possibilities. Moreover,
using (1.1) we see that these cases do all occur for an elliptic curve over some finite field.

(1) $\boxed{p \text{ does not divide } \beta}$,
E is *ordinary*, $L = \mathbb{Q}(\pi_E)$ is imaginary quadratic over $\mathbb{Q}$, and p is split in $L/\mathbb{Q}$; no restrictions on p, no restrictions on n.

In all cases below p divides β and E is *supersingular*. We write either $q = p^{2j}$ or $q = p^{2j+1}$.

(2) $\beta^2 = 4q$ $\quad \boxed{\beta = \mp 2\sqrt{q} = \mp 2p^j, \quad n = 2j \text{ is even}}$.
Here $\pi = \pm p^j = \pm\sqrt{q}$, and $L = \mathbb{Q}$, $\quad D \cong \mathbb{Q}_{p,\infty}$.

In all cases below E is *supersingular*, $\pi_E \notin \mathbb{Q}$, hence $\mathbb{Q} \subsetneqq L = D \cong \mathbb{Q}_{p,\infty}$.

(3) $\beta^2 = 3q$ $\boxed{p = 3, \quad \beta = \pm 3^{j+1}}$, $q = 3^{2j+1}$.
Here $p = 3$, $n = 2j+1$ is odd, and $\pi \sim \zeta_3\sqrt{q}$ or $\pi \sim \zeta_6\sqrt{q}$; $L = \mathbb{Q}(\sqrt{-3})$.

(4) $\beta^2 = 2q$ $\boxed{p = 2, \quad \beta = \pm 2^{j+1}}$, $q = 2^{2j+1}$.
Here $p = 2$, $n = 2j+1$ is odd, and $\pi \sim \zeta_8\sqrt{q}$; $L = \mathbb{Q}(\sqrt{-1})$.

(5) $\beta^2 = q$ $\boxed{\beta = \pm\sqrt{q} = \pm p^j, \quad p \not\equiv 1 \pmod 3}$, $n = 2j$ is even, and $L = \mathbb{Q}(\sqrt{-3})$.
Here $\pi \sim \zeta_6\sqrt{q}$, respectively $\pi \sim \zeta_3\sqrt{q}$.

If we are not in one of the cases above we have $\beta = 0$.

(6) $\boxed{\beta = 0, \quad n \text{ is odd}}$, $\pi \sim \pm\sqrt{-q}$, no restrictions on p; $L = \mathbb{Q}(\sqrt{-p})$.

(7) $\boxed{\beta = 0, \quad n \text{ is even}, \quad p \not\equiv 1 \pmod 4}$, $\pi \sim \pm p^j\sqrt{-1}$, $q = p^{2j}$; $L = \mathbb{Q}(\sqrt{-1})$.

In particular we see:

if E is supersingular over a finite field, $\pi_E \sim \zeta_r\sqrt{q}$ with $r \in \{1,2,3,4,6,8,12\}$.

Proof. Let E be an elliptic curve over $\mathbb{F}_q$. We have seen restrictions on β. If p does not divide $\beta \in \mathbb{Z}$, we see that $\beta^2 - 4q < 0$, and (1) is clear.

If we are not in case (1) we see that p divides β and E is supersingular. If $\beta^2 = 4q$, we are in Case (2); this is clear, see (6.1).

If $\beta^2 = 3q$, we obtain $p = 3$ and we are in case (3)

If $\beta^2 = 2q$, we obtain $p = 2$ and we are in case (4).

If $\beta^2 = q$ we obtain $L = \mathbb{Q}(\zeta_3)$; because p is non-split in $L/\mathbb{Q}$ we obtain $p \not\equiv 1 \pmod 3$ in this case; this proves (5).

Claim. *Suppose we are not in one of the cases* (1) − (5); *then* $\beta = 0$.
Suppose p divides β, i.e. not case (1), and $\beta^2 < 4q$, i.e. not case (2). If $q = p^{2j}$ and $\beta \neq 0$, write $\beta = b{\cdot}p^j$; we see that $\beta^2 = (b{\cdot}p^j)^2 < 4p^{2j}$; hence $b^2 = 1$, and we are in case (5). If $q = p^{2j+1}$ and $\beta \neq 0$, write $\beta = b{\cdot}p^{j+1}$, we see that $\beta^2 = (b{\cdot}p^{j+1})^2 < 4p^{2j+1}$; hence $b^2{\cdot}p < 4$, and we are either in case (3) or in case (4). This proves the claim.

If $\beta = 0$ and n odd, we have $L = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$. We are in case (6), no restrictions on p.

If $\beta = 0$ and n is even, we have $L = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-1})$. As p is non-split in $L/\mathbb{Q}$ we see that $p \not\equiv 1 \pmod 4$. We are in case (7).

This ends the proof of the classification of all elliptic curves over a finite field as given in [69], pp. 536/7. □

(9.7) Exercise. Let p be a prime number, $p \equiv 3 \pmod 4$. Let $\pi := p^2 \cdot \sqrt{-1}$.
(1) *Show that π 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* $\mathrm{End}^0(A)$.
(2) *Show there does not exist an abelian variety B_0 over $K_0 := \mathbb{F}_{p^2}$ such that $B_0 \otimes_{K_0} K \cong A$.*
(3) *Show there exists a field extension $K \subset K'$ and and abelian variety B_0 over K_0 such that $B_0 \otimes_{K_0} K' \cong A \otimes_K K'$.* I.e. A can be defined over K_0.

(9.8) Remark/Exercise. It is interesting to study the behavior of isomorphism classes and of isogeny classes of abelian varieties over finite fields under field extensions. See [69], page 538:

(9.8).1 Example. Let $q = p^n$ with *n even.* Consider $\beta_+ = +2\sqrt{q}$, and $\beta_- = -2\sqrt{q}$. The polynomial $P = T^2 - \beta \cdot T + q$ in both cases gives a Weil q-number. The resulting (isogeny classes) E_+, respectively E_- consist of elliptic curves, with $\mathrm{End}^0(E)$ quaternionic over $\mathbb{Q}$, the case of "all endomorphisms are defined over the base field". These isogeny classes do not coincide over $\mathbb{F}_q$:

$$\beta_\pm = \pm 2\sqrt{q}, \qquad E_+ \not\sim_{\mathbb{F}_q} E_-; \quad \text{however} \quad E_+ \otimes K' \sim_{K'} E_- \otimes K'$$

for the quadratic extension $K = \mathbb{F}_q \subset K' := \mathbb{F}_{q^2}$.

Note that in these cases the characteristic polynomial $f_{E_\pm}$ of the geometric Frobenius equals P^2.
Waterhouse writes: "But the extension which identifies these two classes created also a new isogeny class ... It is this sort of non-stable behavior which is overlooked in a treatment like Deuring's which considers only endomorphism rings over $\overline{k}$..."

(9.8).2 Exercise/Example. *Classify all isogeny classes of elliptic curves, and their endomorphism algebras for every p, for every $q = p^n$.* See (9.6).

(9.8).3 Exercise. *Write* $\mathrm{EIsom}(q)$ *for the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$. Let $K = \mathbb{F}_q \subset K' = \mathbb{F}_{q^N}$ be an extension of finite fields. There is a natural map*

$$\mathrm{EIsom}(q) \quad \longrightarrow \quad \mathrm{EIsom}(q^N) \qquad [E] \mapsto [E \otimes_K K'].$$

Show that this map is not injective, and is not surjective.

(9.8).4 Exercise. *Write* $\mathrm{Isog}(q)$ *for the set of isogeny classes of abelian varieties over $\mathbb{F}_q$. Show that for $N \in \mathbb{Z}_{>1}$ the natural map* $\mathrm{Isog}(q) \to \mathrm{Isog}(q^N)$ *is not injective, and is not surjective.*

(9.9) Exercise. *Show that $h := Y^3 - 6Y^2 + 9T - 1 \in \mathbb{Q}[Y]$ is irreducible. Let β be a zero of h. Show that for any $\psi_0 : \mathbb{Q}(\beta) \to \mathbb{C}$ we have $\psi_0(\beta) \in \mathbb{R}$, i.e. β is totally real, and that $0 < \psi_0(\beta) < 5$, hence β is totally positive. Let π be a zero of $T^2 - \beta \cdot T + 3$. Determine the dimension of A such that $\pi_A = \pi$.*

(9.10) 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.*

(9.11) 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 π 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 π 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:

(9.12) 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 $m = \overline{\mathbb{F}_\mathrm{p}}$ with $D = \mathrm{End}^0(A)$ of* $\mathrm{Type}(e_0, d)$.

(9.13) 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 $\overline{\mathbb{F}_\mathrm{p}}$ with $D = \mathrm{End}_0(A))$ of* $\mathrm{Type}(e_0, d)$ *and $\mathcal{N}(A) = (m, n) + (n, m)$.*

(9.14) 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.*

(9.15) Exercise. Let p be a prime number, and let $P := T^{30} + pT^{15} + p^{15}$. Write $K_n = \mathbb{F}_{p^n}$.
(a) *Show that $P \in \mathbb{Q}[T]$ is irreducible.* Let π be a zero of g. *Show that π 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.

(9.16) Exercise. (See Section 6.) 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 π_b be a zero of g_b. *Show that π_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*

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

defines an infinite number of $\overline{\mathbb{F}_{\rm p}}$*-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* $\mathbb{F}_p$ *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: [28], Th. 3.1 in 8.3 on page 194.

10 Appendix 1: Abelian varieties

For the notion of abelian variety over a field, abelian scheme over a base scheme, isogenies, and much more we refer to the literature.

Warning. In most recent papers there is a distinction between an abelian variety defined over a field K on the one hand, and $A \otimes_K K'$ over $K' \supsetneqq K$ on the other hand. The notation $\mathrm{End}(A)$ stands for the ring of endomorphisms of A over K. This is the way Grothendieck taught us to choose our notation.

In pre-Grothendieck literature and in some modern papers there is a confusion between on the one hand A/K and "the same" abelian variety over any extension field. In such papers there is a confusion. Often it is not clear what is meant by "a point on A", the notation $\mathrm{End}_K(A)$ can stand for the "endomorphisms defined over K", but then sometimes $\mathrm{End}(A)$ can stand for the "endomorphisms defined over $\overline{K}$".

Please adopt the Grotendieck convention that a scheme $T \to S$ is what it is, and any scheme obtained by base extension $S' \to S$ is denoted by $T \times_S S' = T_{S'}$, etc.

(10.1) For the definition of a polarization see [40]; [38], 6.2; see [GM]. A divisor D on an abelian variety A defines a homomorphism $\phi_D : A \to A^t$; in case this divisor is ample ϕ_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 ϕ on A defines an anti-involution ι 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.

(10.2) 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 $N = \mathrm{Spec}(B) \to \mathrm{Spec}(A) = S$ 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 [46], I.2.

(10.3) 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 [46]. Theorem 19.1. For the definition of N^D, see (10.2).

(10.4) 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 $f_{A,\varphi} \in \mathbb{Z}[T]$ of degree $2g$ called *the characteristic polynomial of* φ; it has the property that for any $t \in \mathbb{Z}$ we have $f_A(\varphi - t) = \deg(\varphi - t)$; see [9] page 125. See (11.1) for the definition of $T_\ell(A)$; for every $\ell \neq \mathrm{char}(K)$ the polynomial $f_{A,\varphi}$ equals the characteristic polynomial of $T_\ell(\varphi) \in \mathrm{End}(T_\ell(A)(\overline{K})) \cong M_{2g}(\mathbb{Z}_\ell)$.

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

$$\mathrm{End}(A) \quad \longrightarrow \quad \mathrm{End}(\mathfrak{t}_A) \cong M_g(K)$$

by $\varphi \mapsto d\varphi$.

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

If $\mathrm{char}(K) = p > 0$, *show this map is not 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 $\mathbb{Z} \subsetneqq \mathrm{End}(A)$.

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

(10.7) We say an abelian variety $A \neq 0$ over a field K is *simple* or we say A is K-simple, if for any abelian subvariety $B \subset A$ we have either $0 = B$ or $B = A$.
Theorem (Poincaré-Weil). For any abelian variety $A \neq 0$ over a field K there exist simple abelian varieties B_i and integers $s_i \in \mathbb{Z}_{>0}$ and an isogeny $A \sim_K \Pi B_i^{s_i}$.

(10.8) Exercise. Give an example of a simple abelian variety A over a field such that $A \otimes \overline{K}$ is not simple.

(10.9) **smCM** We say that an abelian variety X over a field K *admits sufficiently many complex multiplications over* K, abbreviated by "smCM over K", if $\mathrm{End}^0(X)$ contains a commutative semi-simple subalgebra of rank $2{\cdot}\dim(X)$ over $\mathbb{Q}$. Equivalently: for every simple abelian variety Y over K which admits a non-zero homomorphism to X the algebra $\mathrm{End}^0(Y)$ contains a field of degree $2{\cdot}\dim(Y)$ over $\mathbb{Q}$. For other characterizations see [12], page 63, see [39], page 347.

Note that if a simple abelian variety X of dimension g over a field *of characteristic zero* admits smCM then its endomorphism algebra $L = \mathrm{End}^0(X)$ is a CM-field of degree $2g$ over $\mathbb{Q}$. We will use he notion "CM-type" in the case of an abelian variety X over $\mathbb{C}$ which admits smCM, and where the type is given, i.e. the action of the endomorphism algebra on the tangent space $T_{X,0} \cong \mathbb{C}^g$ is part of the data.

Note however that there exist (many) abelian varieties A admitting smCM (defined over a field of positive characteristic), such that $\mathrm{End}^0(A)$ is not a field.

By Tate we know that an abelian variety over a finite field admits smCM, see (4.4). By Grothendieck we know that an abelian variety which admits smCM up to isogeny is defined over a finite field, see (4.7).

Terminology. Let $\varphi \in \mathrm{End}^0(A)$. then $d\varphi$ is a K-linear endomorphism of the tangent space. If the base field is $K = \mathbb{C}$, this is just multplication by a complex matrix x, and every multplication by a complex matrix x leaving invariant the lattice Λ, where $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$, gives rise to an endomorphism of A. If $g = 1$, i.e. A is an elliptic curve, and $\varphi \notin \mathbb{Z}$ then $x \in \mathbb{C}$ and $x \notin \mathbb{R}$. Therefore an endomorphism of an elliptic curve over $\mathbb{C}$ which is not in $\mathbb{Z}$ is sometimes called "a complex multiplication". Later this terminology was extended to all abelian varieties.

Warning. Sometimes the terminology "an abelian variety with CM" is used, when one wants to say "admitting smCM". An elliptic curve E has $\mathrm{End}(E) \supsetneqq \mathbb{Z}$ if and only if it admits smCM. However it is easy to give an abelian variety A which "admits CM", meaning that $\mathrm{End}(A) \supsetneqq \mathbb{Z}$, such that A does not admit smCM. However we will use the termionology "a CM-abelian variety" for an abelian vareity which admits smCM.

(10.10) **Exercise.** *Show there exists an abelian variety A over a field k such that $\mathbb{Z} \subsetneqq \mathrm{End}(A)$ and such that A does not admit* smCM.

11 Appendix 2: Tate-ℓ and Tate-p conjectures for abelian varieties

Most important reference: [66].

(11.1) **Notation.** Let A be an abelian vareity over a scheme S, let ℓ be a prime number invertible in the sheaf of local rings on S. Write

$$T_\ell(A) = \mathrm{proj.lim.}_{\leftarrow i}\ A[l^i].$$

This is called the Tate-ℓ-group of A/S.

(11.2) Let G be a group scheme over a base scheme S such that the rank of G is prime to every residue characteristic of S, i.e. the rank of G is invertible in the sheaf of local rings on S. Then $G \to S$ is etale; citeFO-reduced.

(11.3) Etale finite group schemes as Galois modules. (Any characteristic.) Let K be a field, and let $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. The main theorem of Galois theory says that there is an equivalence between the category of algebras etale and finite over K, and the category of finite sets with a continuous G-action. Taking group-objects on both sides we arrive at:
Theorem. *There is an equivalence between the category of etale finite group schemes over K and the category of finite continuous G-modules.*
See [70], 6.4. Note that this equivalence also holds in the case of not necessarily commutative group schemes.

Naturally this can be generalized to: let S be a connected scheme, and let $s \in S(\Omega)$ be a base point, where Ω is an algebraically closed field; let $\pi = \pi_1(S, s)$. *There is an equivalence between the category of etale finite group schemes* (not necessarily commutative) *over S and the category of finite continuous π-systems.*

Exercise. *Write out the main theorem of Galois theory as a theory describing separable field extensions via sets with continuous action by the Galois group. Then formulate and prove the equivalent theorem for etale finite group scheme over an arbitrary base as above.*

Conclusion. The Tate-ℓ-group of an abelian scheme A/S such that ℓ is invertible on S either can be seen as a pro-finite group scheme, or equivalently it can be seen as a projective system of finite modules with a continuous action of the fundamental group of S.

(11.4) Exercise. For an abelian variety A over a field K and a prime number $\ell \neq \mathrm{char}(K)$ the natural map

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

is *injective*, as Weil showed. Prove this statement.

(11.5) Theorem (Tate, Faltings, and many others). *Suppose K is of finite type over its prime field.* (Any characteristic different from ℓ.) *The canonical map*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \xrightarrow{\sim} \quad \mathrm{End}(T_\ell(A)) \cong \mathrm{End}_{G_K}((\mathbb{Z}_\ell)^{2g})$$

is an isomorphism.
This was conjectured by Tate. In 1966 Tate proved this in case K is a finite field, see [66]. The case of function field in characteristic p was proved by Zarhin and by Mori, see [74], [75], [36]; also see [35], pp. 9/10 and VI.5 (pp. 154-161).

The case K is a number field this was open for a long time; it was finally proved by Faltings in 1983, see [16]. For the case of a function field in characteristic zero, see [17], Th. 1 on page 204.

(11.6) We like to have a p-adic analogue of (11.5). For this purpose it is convenient to have p-divisible groups instead of Tate-ℓ-groups:

Definition. Let A/S be an abelian scheme, and let p be a prime number (no restriction on p). We write

$$A[p^\infty] = \text{ind.lim.}_{\to i}\ A[p^i],$$

called the p-divisible group (or the Barsotti-Tate group) of A/S.

Remark. Historically a Tate-ℓ-group is defined as a projective system, and the p-divisible group as an inductive system; it turns out that these are the best ways of handling these concepts (but the way in which direction to choose the limit is not very important). We see that the p-divisible group of an abelian variety should be considered as the natural substitute for the Tate-ℓ-group. Note that $A[p^\infty]$ is defined over any base, while $T_\ell(A)$ is only defined when ℓ is invertible on the base scheme.

The notation $A[p^\infty]$ is just symbolic; there is no morphism "p^∞", and there is no kernel of this.

(11.7) Exercise. For an abelian variety A over a field K and a prime number p the natural map

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

is *injective*. Prove this statement. Or see [71], theorem 5 on page 56.

(11.8) Theorem (Tate and De Jong). *Let K be a field finitely generated over $\mathbb{F}_p$. Let A and B be abelian varieties over K. The natural map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{Hom}(A[p^\infty], B[p^\infty])$$

is an isomorphism.
This was proved by Tate in case K is a finite field; a proof was written up in [71]. The case of a function field over a finite field was proved by Johan de Jong, see [24], Th. 2.6. This case follows from the result by Tate and from the following result on extending homomorphisms (11.9).

(11.9) Theorem (Tate, De Jong). *Let R be an integrally closed, Noetherian integral domain with field of fractions K.* (Any characteristic.) *Let X, Y be p-divisible group over* $\mathrm{Spec}(R)$. *Let $\beta_K : X_K \to Y_K$ be a homomorphism. There exists (uniquely) $\beta : X \to Y$ over* $\mathrm{Spec}(R)$ *extending β_K.*
This was proved by Tate, under the extra assumption that the characteristic of K is zero. For the case $\mathrm{char}(K) = p$, see [24], 1.2 and [25], Th. 2 on page 261.

12 Appendix 3: Central simple algebras

Basic references: [6], [58], [7] Chapter 7, [60] Chapter 10. We will not give a full treatment of this theory here.

(12.1) A module over a ring is *simple* if it is non-zero, and it has no non-trivial submodules.

A module over a ring is *semisimple* if it is a direct sum of simple submodules.

A ring is called *semisimple* if it is non-zero, and if it is semisimpe as a left module over itself.

A ring is called *simple* if it is semisimple and if there is only one class of simple left ideals.

A finite product of simple rings is semisimple.

The matrix algebra $M_r(D)$ over a division algebra D for $r \in \mathbb{Z}_{>0}$ is simple.

Wedderburn's theorem says that for a central simple algebra (see below) R over a field L there is a central division algebra D over L and an isomorphism $R \cong M_r(D)$ for some $r \in \mathbb{Z}_{\geq 0}$.

Examples of rings which are not semisimple: $\mathbb{Z}$, $K[T]$, $\mathbb{Z}/p^2$.
Examples of rings which are simple: a field, a division algebra (old terminology: "a skew field"), a matrix algebra over a division algebra.

(12.2) Definition. Let L be a field. A *central simple algebra* over L is an L-algebra Γ such that
(1) Γ is finite dimensional over L,
(2) L is the center of Γ,
(3) Γ is a simple ring.
We say that $\Gamma = D$ is a central division algebra over L if moreover D is a division algebra.

The set of "similarity classes" of central simple algebras over L has the structure of an abelian group, called the Brauer group of L, denoted by $\mathrm{Br}(L)$; in this group Γ and $\Gamma \otimes_L M_r(L)$ are identified under the similarity equivalence. See the literature cited for definitions, and properties.

(12.3) Facts (Brauer theory).
(1) *For any local field L there is a canonical homomorphism*

$$\mathrm{inv}_L : \mathrm{Br}(L) \to \mathbb{Q}/\mathbb{Z}.$$

(2) *If L is non-archimedean, then* $\mathrm{inv}_L : \mathrm{Br}(L) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ *is an isomorphism.*
If $L \cong \mathbb{R}$ then $Br(L) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.
If $L \cong \mathbb{C}$ then $\mathrm{Br}(L) = 0$.
(3) *If L is a global field, there is an exact sequence*

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

Note the use of this last statement: any central simple algebra over a global field L is uniquely determined by a finite set of non-zero invariants at places of L. We will see that this gives us the possibility to describe endomorphism algebras of (simple) abelian varieties.

For explicit descriptions of some division algebras see [5]. Note that such explicit methods can be nice to have a feeling for what is going on, but for the general theory you realy need Brauer theory.

13 Appendix 4: Endomorphism algebras.

Basic references: [62], [40], [30] Chapt. 5, [52].
We will see: *endomorphism algebras* of abelian varieites can be classified. In many cases we know which algebras do appear. However we will also see that it is difficult in general to describe all orders in these algebras which can appear as the *endomorphism ring* of an abelian variety.

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. By Wedderburn's theorem every central simple algebra is a matrix algebra over a division algebra. If A is K-simple the algebra $\mathrm{End}^0(A)$ is a division algebra; in that case we write:

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

here L_0 is a totally real field, and either $L = L_0$ or $[L : L_0] = 2$ and in that case L is a CM-field. In case A is simple $\mathrm{End}^0(A)$ is one of the four types in the Albert classification. We write:

$$[L_0 : \mathbb{Q}] = e_0, \quad [L : \mathbb{Q}] = e, \quad [D : L] = d^2.$$

The Rosati involution $\dagger : D \to D$ is positive definite. A simple division algebra of finite degree over $\mathbb{Q}$ with a positive definite anti-isomorphism which is positive definite is called an Albert algebra. Applications to abelian varieties and the classification has been described by Albert, [1], [2], [3].

(13.1) Albert's classification.
Type I(e_0) Here $L_0 = L = D$ is a totally real field.

Type II(e_0) Here $d = 2$, $e = e_0$, $\mathrm{inv}_v(D) = 0$ for all infinite v, and D is an indefinite quaternion algebra over the totally real field $L_0 = L$.

Type III(e_0) Here $d = 2$, $e = e_0$, $\mathrm{inv}_v(D) \neq 0$ for all infinite v, and D is an definite quaternion algebra over the totally real field $L_0 = L$.

Type IV(e_0, d) Here L is a CM-field, $[F : \mathbb{Q}] = e = 2e_0$, and $[D : L] = d^2$.

(13.2) A more refined question is to study the *endomorphism ring* of an abelian variety.
Remark. Suppose A is an abelian variety over a finite field. Let π_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 case A is an abelian variety over a finite field. This is in sharp contrast with:

(13.3) 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 $\mathbb{C}$.

(13.4) Exercise. *Show there exists a polarized abelian variety (A, μ) over a field k such that the Rosati involution* $\dagger : \mathrm{End}^0(A) \to \mathrm{End}^0(A)$ *does not map* $\mathrm{End}(A) \subset \mathrm{End}^0(A)$ *into itself.*

(13.5) Exercise. Show there for every integer m and for every algebraically closed field $k \supset \mathbb{F}_p$ not isomorphic to $\mathbb{F}$ there exists a simple abelian surface over k such that $E := \mathrm{End}^0(A)$ and $[\mathcal{O}_E : \mathrm{End}(A)] > m$.

(13.6) Remark. For a simple *ordinary* abelian variety A over a finite field the orders contained in $\mathrm{End}^0(A)$ and containing π_A and ν_A are precisely all possible orders in the isogeny class of A, see [69], Th. 7.4.

However this may fail for a non-ordinary abelian variety, see [69], page 555/556, where an example is given of an order containing π_A and ν_A, but which does not appear as the endormorphism ring of any abelian variety.

We see difficulties indetermining the possible orders in $\mathrm{End}^0(A)$ which can apear as the endomorphism ring of some $B \sim A$.

Much more information on endomorphism rings of abelian varieties over finite fields can be found in [69].

(13.7) Exercise. Let A be a simple abelian variety over an algebraically closed field k *which admits* smCM.

(1) *If the characteristic of* k *equals zero,* $\mathrm{End}^0(A)$ *is commutative.*

(2) *If* A *is simple and ordinary over* $\mathbb{F}$ *then* $\mathrm{End}^0(A)$ *is commutative.*

(3) However if A is simple and non-ordinary over $\mathbb{F}$ there are many examples showing that $\mathrm{End}^0(A)$ may be non-commutative. *Give examples.*

(4) *Show there exists an ordinary abelian variety* B *over an algebraically closed field of positive characteristic such that* $\mathrm{End}(B)$ *is not commutative.* (Hence $k \not\cong \mathbb{F}$, and B does not admit smCM.)

(13.8) Exercise. *Let* $K \subset K'$ *be a an extension of finite field. Let* A *be an ordinary abelian variety over* K *such that* $A \otimes K'$ *is simple. Show that* $\mathrm{End}^0(A) \to \mathrm{End}^0(A \otimes K')$ *is an isomorphism.*

In [69], Theorem 7.2 we read that for simple and ordinary abelian vareities "$\mathrm{End}(A)$ is commutative and unchanged by base change". Some care has to be take in understanding this.

(13.9) Exercise. Choose a prime number p, and let π be a zero of the polynomial $T^4 - T^2 + p^2$. Show that π is a Weil p-number; let A be an abelian variety over $\mathbb{F}_p$ (determined up to isogeny) which has π as geometric Frobenius. Show that A is a simple, ordinary abelian surface. Show that $\mathrm{End}^0(A) \to \mathrm{End}^0(A \otimes \mathbb{F}_{p^2})$ is not an isomorphism.

(13.10) Remark/Exercise. *Choose* $p > 0$, *choose a symmetric Newton polygon* ξ *which is not supersingular. Then there exists a simple abelian variety* A *over* $\mathbb{F}$ *with* $\mathcal{N}(A) = \xi$ *such that* $\mathrm{End}^0(A)$ *is commutative*; see [31]. For constructions of other endomorphism algebras see [8], Th. 5.4 of an abelian variety over $\mathbb{F}$

(13.11) 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 [69], Th.6.1). In this case every order containing π_A and ν_A in $D = L = \mathrm{End}^0(A)$ is the endomorphism algebra of an abelian variety over $\mathbb{F}_p$.
Exercise. Show *there does exist a simple abelian variety over* $\mathbb{F}_p$ *such that* $\mathrm{End}^0(A)$ *is not commutative.*

(13.12) For abelian varieties over a *finite field* separable isogenies give an equivalence relation, see [69], 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.*

(13.13) 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 (10.5), (9.15).

(13.14) Exercise. *Let g be an odd prime number, and let A be a simple abelian variety over a finite field of dimension g. Show:*

- *either* $\mathrm{End}(A)$ *is commutative,*
- *or* $\mathrm{End}^0(A)$ *is of* $\mathrm{Type}(1, g)$, *and* $\mathcal{N}(A)$ *has exactly two slopes and the p-rank of A is equal to zero.*

See [52], (3.13).

(13.15) 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 9.

Suppose k is an algebraically closed field of $\mathrm{char}(k) = p$, and let A be a supersingular abelian variety, i.e. $\mathcal{N}(A) = \sigma$, all slopes are equal to $1/2$; 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.

(13.16) Theorem (Lenstra and FO). *Let ξ be a symmetric Newton polygon, and let p be a prime number. Suppose that $\xi \neq \sigma$, i.e. not all slopes in ξ are equal to $1/2$. Then there exists an abelian variety A over $m = \overline{\mathbb{F}_{\mathrm{p}}}$ 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 [31].

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

For more general constructions of endomorphism algebra with given invariants of an abelian variety over a finite field, see [8], Section 5.

14 Appendix 5: Some properties in characteristic p

For information on group schemes see [46], [59], [70].

In characteristic zero we have strong tools at our disposal: besides algebraic-geometric theories we can use analytic and topological methods. It seems that we are at a loss in positive characteristic. However the opposite is true. Phenomena, only occurring in positive characteristic provide us with strong tools to study moduli spaces. And, as it turns out again and again, several results in characteristic zero can be derived using reduction modulo p. These tools in positive characteristic will be of great help in this talk.

(14.1) A finite group scheme in characteristic zero, of more generally a finite group scheme of rank prime to all residue characteristics, is etale over the base; e.g. see [47]. However if the rank of a finite group scheme is not invertible on the base, it need not be etale.

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

For a scheme $A \to S$ over $\mathrm{Spec}(\mathbb{F}_p)$ 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 $F_{A/S} = F_A : A \to A^{(p)}$, 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 [59], 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.

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

(14.3) Verschiebung. Let A be a *commutative* group scheme over a characteristic p base scheme. In [59], Exp. VII_A.4 we find the definition of the "relative Verschiebung"

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

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 [59], Exp. VII_A.4, but we can define V_A by $V_A{\cdot}F_A = [p]_A$ and check that $F_A{\cdot}V_A = [p]_{A^{(p)}}$.

(14.4) Examples of finite group scheme of rank p. Let $k \supset \mathbb{F}_p$ be an algebraically closed field, and let G be a commutative group scheme of rank p over k. Then we are in one of the folowing three cases:

$G = \underline{\mathbb{Z}/p}_k$. This is the scheme $\mathrm{Spec}(k^p)$, with the group structure given by $\mathbb{Z}/p$. Here $V_G = 0$ and F_G is an isomorphism.

$G = \alpha_p$. We write $\alpha_p = \mathbb{G}_{a,\mathbb{F}_p}[F]$ the kernel of the Frobenis mophism on the linear group $\mathbb{G}_{a,\mathbb{F}_p}$. This group scheme is defined over $\mathbb{F}_p$, and we have the habit to write for any scheme $S \to \mathrm{Spec}(\mathbb{F}_p)$ just α_p, although we should write $\alpha_p \times_{\mathrm{Spec}(\mathbb{F}_p)} S$. For any field $K \supset \mathbb{F}_p$ we have $\alpha_{p,K} = \mathrm{Spec}(K[\tau]/(\tau^p))$ and the group sctructure is given by the comultiplication $\tau \mapsto \tau \otimes 1 + 1 + \tau$ on the algebra $K[\tau]/(\tau^p)$. Here $V_G = 0 = F_G$.

$G = \mu_{p,k}$. We write $\mu_{t,K} = \mathbb{G}_{m,K}[t]$ for any field K and any $t \in \mathbb{Z}_{>1}$. Note that the algebras defining $\alpha_{p,\mathbb{F}_p}$ and $\mu_{p,\mathbb{F}_p}$ are isomorophic, but the comultiplications are different. Here $F_G = 0$ and V_G is an isomorphism.

Any finite commutative group scheme over k of rank a power of p is a successive extension of group schemes of these three types. for an arbitrary field $K \supset \mathbb{F}_p$ the first and the last example can be "twisted" by a Galois action. However if $G \otimes_K k \cong \alpha_{p,k}$ then $G \cong \alpha_{p,K}$.

For duality, and for the notion of "local" and "etale" group scheme see [46].

Commutative group scheme of p-power rank over a perfect base fiedl can be classified with the help of Dieudonné modules, not dicussed here, but see [33], see [13].

(14.5) For an abelian variety A over a field $K \supset \mathbb{F}_p$ we define its p-rank $f(A) = f$ as the integer such that $A[p](\overline{K}) \cong (\mathbb{Z}/p)^f$.

We say A is *ordinary* iff $f(A) = \dim(A) =: g$.

(14.6) For a classification of ordinary abelian varieteis over finite fields (using Serre-Tate canonical lifts, and classical theory) see the wonderful paper [11].

(14.7) Examples. If E is an elliptic curve in characteristic p then:

$$E \quad \text{is ordinary} \quad \Leftrightarrow \quad E[p](\overline{K}) \neq 0 \quad \Leftrightarrow \quad E[F] := \mathrm{Ker}(F : E \to E^{(p)}) \otimes k \cong \mu_p.$$

In this case $E[p] \otimes k \cong \mu_p \times \underline{\mathbb{Z}/p}$.

$$E \quad \text{is supersingular} \quad \Leftrightarrow \quad E[p](\overline{K}) = 0 \quad \Leftrightarrow \quad E[F] := \mathrm{Ker}(F : E \to E^{(p)}) \cong \alpha_p.$$

In this case $E[p]$ is a non-trivial extension of α_p by α_p.

Warning. For a higher dimensional abelian varieties $A[F]$ and $A[p]$ can be quite complicated.

(14.8) Exercise. *Show that the following properties are equivalent:*
(1) *A is ordinary,*
(2) $\mathrm{Hom}(\alpha_p, A) = 0$,
(3) *the kernel of $V : A^{(p)} \to A$ is etale,*
(4) *the rank of the group* $\mathrm{Hom}(\mu_p, A \otimes \overline{K})$ *equals p^g.*
(5) $\mathrm{Hom}(\mu_p, A \otimes \overline{K}) \cong (\mathbb{Z}/p)^g$.

(14.9) Duality; see [GM], Chapter V. For a finite locally free group scheme $G \to S$ over a base $S \to \mathrm{Spec}(\mathbb{F}_p)$ we study $F_{G/S} : G \to G^{(p)}$. We can apply Cartier-duality.

Fact.

$$\left(F_{G/S} : G \to G^{(p)}\right)^D \quad = \quad \left(V_{G^D} : (G^{(p)})^D = (G^D)^{(p)} \to G^D\right).$$

In the same way Cartier duality gives $(V_G)^D = F_{G^D}$.

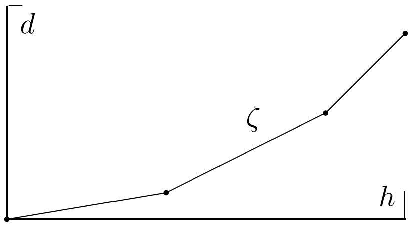
Using duality of abelian varieties, in particular see [46], Theorem 19.1, we arrive at:
For an abelian scheme $A \to S$ over a base $S \to \mathrm{Spec}(\mathbb{F}_p)$ we have

$$\left(F_{A/S} : A \to A^{(p)}\right)^t \quad = \quad \left(V_{A^t} : (A^{(p)})^t = (A^t)^{(p)} \to A^t\right), \quad \text{and} \quad (V_A)^t = F_{A^t}.$$

(14.10) Newton polygons. In order to being able to handle the isogeny class of $A[p^\infty]$ we need the notion of Newton polygons.

Suppose given integers $h, d \in \mathbb{Z}_{\geq 0}$; here $h =$ "height", $d =$ "dimension", and in case of abelian varieties we will choose $h = 2g$, and $d = g$. A Newton polygon γ (related to h and d) is a polygon $\gamma \subset \mathbb{Q} \times \mathbb{Q}$ (or, if you wish in $\mathbb{R} \times \mathbb{R}$), such that:

- γ starts at $(0, 0)$ and ends at (h, d);
- γ is lower convex;
- any slope β of γ has the property $0 \leq \beta \leq 1$;
- the breakpoints of γ are in $\mathbb{Z} \times \mathbb{Z}$; hence $\beta \in \mathbb{Q}$.



Note that a Newton polygon determines (and is determined by)

$$\beta_1, \cdots, \beta_h \in \mathbb{Q} \text{ with } 0 \leq \beta_1 \leq \cdots \leq \beta_h \leq 1 \quad \leftrightarrow \quad \zeta.$$

Sometimes we will give a Newton polygon by data $\sum_i \ (d_i, c_i)$; here $d_i, c_i \in \mathbb{Z}_{\geq 0}$, with $\gcd(d_i, c_i) = 1$, and $d_i/(d_i + c_i) \leq d_j/(d_j + c_j)$ for $i \leq j$, and $h = \sum_i \ (d_i + c_i)$, $\ d = \sum_i d_i$. From these data we construct the related Newton polygon by choosing the slopes $d_i/(d_i + c_i)$ with multiplicities $h_i = d_i + c_i$. Conversely clearly any Newton polygon can be encoded in a unique way in such a form.

Remark. The Newton polygon of a polynomial. Let $g \in \mathbb{Q}_p[T]$ be a monic polynomial of degree h. We are interested in the p-adic values of its zeroes (in an algebraic closure of $\mathbb{Q}_p$). These can be computed by the Newton polygon of this polynomial. Write $g = \sum_j \gamma_j T^{h-j}$. Plot the pairs $(j, v_p(\gamma_j))$ for $0 \leq j \leq h$. Consider the lower convex hull of $\{(j, v_p(\gamma_j)) \mid j\}$. This is a Newton polygon according to the definition above. *The slopes of the sides of this polygon are precisely the p-adic values of the zeroes of g, ordered in non-decreasing order.*
Exercise. Prove this.
Hint. Write $g = \Pi \ (T - z_i)$, with $z_i \in \overline{\mathbb{Q}_p}$. Write $\beta_i := v_p(z_i) \in \mathbb{Q}_{\geq 0}$. Suppose the order of the $\{z_i\}$ chosen in such a way that

$$0 \leq \beta_1 \leq \beta_2 \leq \cdots \leq \beta_i \leq \beta_{i+1} \leq \cdots \leq \beta_h.$$

Let σ_j be the elementary symmetric functions in z_i. Show that:

$$\sigma_j = \gamma_j, \quad v_p(\sigma_j) \geq \beta_1 + \cdots + \beta_j, \quad \beta_h = v_p(\gamma_h),$$

and

$$N < h, \quad \beta_N < \beta_{N+1} \quad \Longrightarrow \quad \sigma_N = \beta_1 + \cdots + \beta_N.$$

□

(14.11) *A p-divisible group X over a field of characteristic p determines uniquely a Newton polygon.* The general definition can be found in [33]. The isogeny class of a p-divisible group over and algebraically closed field k uniquely determines (and is uniquely determined by) its Newton polygon:

(14.12) **Theorem** (Dieudonné and Manin), see [33], "Classification theorem " on page 35 .

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

(14.13) We sketch the construction of a Newton polygon of a p-divisible group X, or of an abelian variety.

(**Incorrect.**) Here we indicate what the Newton polygon of a p-divisible group is (in a slightly incorrect way ...). Consider "the Frobenius endomorphism" of X. This has a "characteristic polynomial". This polynomial determines a Newton polygon, which we write as $\mathcal{N}(X)$, the Newton polygon of X. For an abelian variety A we write $\mathcal{N}(A)$ instead of $\mathcal{N}(A[p^\infty])$.

Well, this "definition" is correct over $\mathbb{F}_p$ as ground field. However over any other field $F : X \to X^{(p)}$ is not an endomorphism, and the above "construction" fails.

Over a finite field there is a method which repairs this. Let A be an abelian variety over $\mathbb{F}_q$. The geometric Frobenius $\pi_A \in \mathrm{End}(A)$ has a characteristic polynomial $f = f_A = f_{A,\pi_A} \in \mathbb{Z}[T] \subset \mathbb{Q}_p[T]$. Take $\mathrm{NP}(f_A)$ the Newton polygon of f_A. That is: write $f = \sum_{0 \leq i \leq 2g} b_i T^{2g-i}$; consider all points $\{(i, v_p(b_i))\}$ in the plane, and let $\mathrm{NP}(f_A)$ be the lower convex hull of this set of points. Note that $(0, v_p(b_0)) = (0,0)$, because the polynomial is monic, and $(2g, v_p(b_{2g})) = (2g, n{\cdot}2g)$, because $b_{2g} = q^{2g} = p^{n \cdot 2g}$. We define $\mathcal{N}(A)$, the Newton polygon of A to be the lower convex hull of the set of $\{(i, \frac{1}{n}{\cdot}v_p(b_i))\}$.

However one can define the Newton polygon of an abelian variety over an arbitrary field in positive characteristic. we can work with the "explanation" given above: $\mathcal{N}(X)$ is the "Newton polygon of the Frobenius on X".

(14.14) **Dieudonné-Manin theory.** (We only give some definitions and facts.) For coprime integers $d, c \in \mathbb{Z}_{\geq 0}$ one can define a p-divisible group $G_{d,c}$. In fact, $G_{1,0} = \mathbb{G}_m[p^\infty]$, and $G_{0,1} = \underline{(\mathbb{Q}_p/\mathbb{Z}_p)}$. For $d > 0$ and $c > 0$ we have a formal p-divisible group $G_{d,c}$ of dimension d and of height $h = d + c$. We do not give the construction here; see the first two chapters of Manin's thesis [33]; the definition of $G_{d,c}$ is on page 35 of [33]. The p-divisible group $G_{d,c}$ 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 $G_{d,c}$ instead of $G_{d,c} \otimes_{\mathbb{F}_p} K$.

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

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

In [33], 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*

$$X \quad \sim \quad \prod_i G_{d_i,c_i}.$$

see [33], Classification Theorem on page 35.

The isogeny class of $\sum_i G_{d_i,c_i}$ will be encoded in the form of a Newton polygon. The simple p-divisible group $G_{d,c}$ will be represented by $d+c$ slopes equal to $d/(d+c)$. The slopes of $\sum_i G_{d_i,c_i}$ 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 $\mathbb{Q} \times \mathbb{Q}$.

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

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:*

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

Verify that this more general definition of Dieudonné and Manin coincides with the definition given above in case A is defined over a finite field.

15 Some questions

In this section we gather some remarks, questions and open problems.

(15.1) Definition. Let B_0 be an abelian variety over a field K of characteristic $p > 0$. We say B is a CM-lift of B_0 if there exists an integral domain R of characteristic zero with a surjective homomorphism $R \twoheadrightarrow K$ with field of fractions $Q(R)$ and an abelian scheme $B \to \mathrm{Spec}(R)$ such that $B \otimes K \cong B_0$ and such that $B \otimes Q(R)$ admits smCM.

Remarks. (1) If A_0 admits a CM-lift, then $A_0 \otimes K$ admits smCM.
(2) By Tate we know that any abelian variety over a finite field admits smCM, [66].
(3) If A_0 is an *ordinary* abelian variety over a finite field K, then by using the canonical Serre-Tate lift we see that A_0 admits a CM-lift.
(4) Deuring has proved that any elliptic curve over a finite field admits a CM-lift; see [14], pp. 259 – 263; for a proof also see [53], Section 14, in particular 14.7.
(5) The previous method can be used to show that any abelian variety of dimension g defined over a finite field of p-rank equal to $g-1$ admits a CM-lift; use [53], 14.6.
(6) We have seen that for an abelian variety A_0 over a finite field K there exists a finite extension $K \subset K'$, and a K'-isogeny $A_0 \otimes K' \sim B_0$ such that B_0 admits a CM lift. *Do we really need the finite extension and the isogeny to assure a CM-lift ?*
(7) (We need the isogeny.) In [54], Theorem B we find: *suppose $g \geq 3$, and let f be an integer, $0 \leq f \ \leq g-2$. Then there exists an abelian variety A_0 over $\mathbb{F} := \overline{\mathbb{F}_p}$ of dimension g with p-rank equal to f such that A_0 does not admit a CM-lift.*

(15.2) Expectation. (Do we need a finite extension?) *We expect that there exist a finite field K and an abelian variety A_0 over K such that any B_0 over K isogenous overt K with A_0 does not admit a* CM-*lift.*

(15.3) In the proof of the Honda-Tate theorem analytic tools are used. Indeed we construct CM abelian varieties over $\mathbb{C}$ in order to prove surjectivity of the map $A \mapsto \pi_A$. As a corollary of the Honda-Tate theory we have seen a proof of the Manin Conjecture. However it turns out that for the Manin Conjecture we now have a purely geometric proof, indeed a proof which only uses characteristic p methods, see [56], Section 5.

(15.4) Open Problem. *Does there exist a proof of the Honda-Tate theorem* (1.1) *only using methods in characteristic p ?*

(15.5) Over an algebraically closed field k of characteristic zero for a given g it is exactly known which algebras can appear as the endomorphism algebra of a simple abelian variety over k; see [62], pp. 175/176; also see [40] pp. 202/203; see [30], 5.5.

For any Albert algebra (an algebra of finite dimension over $\mathbb{Q}$, with a positive definite anti-involution, equivalently: a finite product of algebras in the classification list of Albert), and any characteristic, there exists a simple abelian variety over an algebraically closed field of that characteristic having that endomorphism algebra; see [62], pp. 175/176 and [40] pp. 202/203 for characteristic zero; for arbitrary characteristic see [19]; for a discussion see [52], Theorem 3.3 and Theorem 3.4.

(15.6) Open Problem. *Suppose a prime number $p > 0$ given. Determine for every $g \in \mathbb{Z}_{>0}$ the possible endomorphism algebras appearing for that g in characteristic p.*

(15.7) Open Problem. *For every characteristic and every $g \in \mathbb{Z}_{>0}$ determine all possible endomorphism rings of an abelian variety over an algebraically closed field in that characteristic.*

(15.8) Exercise. *For an abelian variety of dimension g over a field K of characteristic zero we have*

$$m(X) := \frac{2g}{[\mathrm{End}^0(A) : \mathbb{Q}]} \quad \in \quad \mathbb{Z}.$$

Give examples of an abelian variety A in positive characteristic where

$$\frac{2g}{[\mathrm{End}^0(A) : \mathbb{Q}]} \quad \not\in \quad \mathbb{Z}.$$

(15.9) Expectation. *For every $\gamma \in \mathbb{Q}_{>0}$ and every prime number $p > 0$ there exists a field k in characteristic p, and an abelian variety A over k such that*

$$\frac{2g}{[\mathrm{End}^0(A) : \mathbb{Q}]} \quad = \quad \gamma.$$

See [55], Section 2.

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

References

[1] A. A. Albert – *On the construction of Riemann matrices, I, II.* Ann. Math. **35** (1934), 1 – 28; **36** (1935), 376 – 394.

[2] A. A. Albert – *A solution of the principal problem in the theory of Riemann matrices.* Ann. Math. **35** (1934), 500 – 515.

[3] A. A. Albert – *Involutorial simple algebras and real Riemann matrices.* Ann. Math. **36** (1935), 886 – 964.

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

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

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

[7] 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.

[8] C.-L. Chai & F. Oort – *Hypersymmetric abelian varieties.* [To appear: Quarterly Journal of Pure and Applied Mathematics]. See
http://www.math.uu.nl/people/oort/

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

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

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

[12] 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.

[13] M. Demazure – *Lectures on p-divisible groups.* Lecture Notes Math. 302, Springer – Verlag 1972.

[14] M. Deuring – *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem.Hamburg **14** (1941), 197 – 272.

[15] 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/

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

[17] G. Faltings & G. Wüstholz – *Rational points.* Seminar Bonn / Wuppertal 1983/84. Asp. Math. E6, Vieweg 1984.

[18] G. van der Geer & B. Moonen – *Abelian varieties.* [In preparation] This will be cited as [GM].

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

[20] A. Grothendieck – *Fondements de la géométrie algébrique.* Extraits du Séminaire Bourbaki 1957 - 1962. Secr. math., Paris 1962.

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

[22] H. Hasse - *Zahlentheorie.* Akad. Verlag, Berlin 1949 (first printing, second printing 1963).

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

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

[25] A. J. de Jong – *Barsotti-Tate groups and crystals.* Documenta Mathematica, Extra Volume ICM 1998, II, 259 – 265.

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

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

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

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

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

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

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

[33] 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.

[34] S. Mochizuki – *The local pro-p anabelian geometry of curves.* Invent. Math. **138** (1999), 319 – 423.

[35] L. Moret-Bailly – *Pinceaux de variétés abéliennes.* Astérisque 129. Soc. Math. France 1985.

[36] S. Mori – *On Tate's conjecture concerning endomorphisms of abelian varieties.* Itl. Sympos. Algebr. Geom. Kyoto 1977 (Ed. M. Nagata). Kinokuniya Book-store 1987, pp. 219 - 230.

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

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

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

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

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

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

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

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

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

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

[47] F. Oort – *Algebraic group schemes in characteristic zero are reduced.* Invent. Math. **2** (1966), 79 - 80.

[48] 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.

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

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

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

[52] 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.

[53] F. Oort – — *Lifting algebraic curves, abelian varieties and their endomorphisms to characteristic zero.* Algebraic Geometry, Bowdoin 1985 (Ed. S. J. Bloch). Proceed. Sympos. Pure Math. **46** Part 2, AMS 1987; pp. 165 -195.

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

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

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

[57] 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.

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

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

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

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

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

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

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

[65] J. Silverman – *The arithmetic of elliptic curves.* Grad. Texts Math. 106, Springer – Verlag, 1986.

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

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

[68] 2005-05 VIGRE number theory working group. Organized by Brian Conrad and Chris Skinner. On: http://www.math.Isa.umich.edu/ bdconrad/vigre04.html

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

[70] W. C. Waterhouse – *Introduction to affine group schemes.* Grad. Texts Math. 66, Springer – Verlag, 1979.

[71] 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.

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

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

[74] J. G. Zarhin – *Isogenies of abelian varieties over fields of finite characteristic.* Math. USSR Sbornik **24** (1974), 451 – 461.

[75] J. G. Zarhin – *A remark on endomorphisms of abelian varieties over function fields of finite characteristic.* Math. USSR Izv. **8** (1974), 477 – 480.

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