Abelian varieties over finite fields

Frans Oort

Higher-dimensional varieties over finite fields,
Summer school in Göttingen, June 2007

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 Theorem 1.2.

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 $K = \mathbb{F}_q$, see 3.2:

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

Geometric objects are constructed and classified up to isogeny 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.

Instead of reading these notes it is much better to read the wonderful and clear [73]. Some proofs have been worked out in more detail in [74].

In §§ 1 $\sim$ 15 material discussed in the course is described. In the appendices §§ 16 $\sim$ 22 we have gathered some information we need for statements and proofs of the main result. I hope all relevant notions and information needed for understanding the main arguments of these notes can be found in the appendices.

Material discussed below will be contained eventually 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: [47], [35], [15] Chapter V.
Honda-Tate theory: [73], [29], [74].
Abelian varieties over finite fields: [72], [75], [77], [64].
Group schemes: [62], [49].
Endomorphism rings and endomorphism algebras: [68], [24], [72], [75], [54].
CM-liftings: [56], [11].

Contents:

Some notation. In definitions and proofs below we need various fields, in various disguises. We use $K,\ L,\ M,\ P,\ k,\ \mathbb{F}_q,\ \overline{\mathbb{F}_p} = \mathbb{F},\ \mathbb{P},\ m$.

We write K for an arbitrary field, usually the base field, in some cases of arbitrary characteristic, however most of the times a finite field. We write k for an algebraically closed field. We write g for the dimension of an abelian variety, unless otherwise stated. We write p for a prime number. We write ℓ for a prime number, which usually is different from the characteristic of the base field, respectively invertible in the sheaf of local rings of the base scheme. We write $\mathbb{F} = \overline{\mathbb{F}_p}$. We use the notation M for a field, sometimes a field of definition for an abelian variety in characteristic zero.

We will use L as notation for a field, usually the center of an endomorphism algebra; we will see that in our cases this will be a totally real field or a CM-field. We write P for a CM-field, usually of degree $2g$ over $\mathbb{Q}$. We write $\mathbb{P}$ for a prime field: either $\mathbb{P} = \mathbb{Q}$ or $\mathbb{P} = \mathbb{F}_p$.

A discrete valuation on a base field usually will be denoted by v, whereas a discrete valuation on a CM-field usually will be denoted by w. If w divides p, the normalization chosen will be given by $w(p) = 1$.

For a field M we denote by Σ_M the set of discrete valuations (finite places) of M. If moreover M is of characteristic zero, we denote by $\Sigma_M^{(p)}$ the set of discrete valuations with residue characteristic equal to p.

We write $\lim_{\leftarrow i}$ for the notion of "projective limit" or "inverse limit".

We write $\mathrm{colim}_{i\rightarrow}$ for the notion of "inductive limit" or "direct limit".

1. Main topic/survey

1.1. Definition. Let p be a prime number, $n \in \mathbb{Z}_{>0}$; write $q = p^n$. A Weil q-number π is an *algebraic integer* 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'.
Notation: $\pi \quad \sim \quad \pi'$.
Equivalently: *the minimum polynomials of π and π' over $\mathbb{Q}$ are equal.* We write $W(q)$ for the set conjugacy classes of Weil q-numbers.

In this definition $| \cdot |$ denotes the *complex absolute value* given by $| a + b\sqrt{-1} |= \sqrt{a^2 + b^2}$ for $a, b \in \mathbb{R}$. We will show that for any Weil q-number π there exists an element $\overline{\pi} = \rho(\pi) \in \mathbb{Q}(\pi)$ such that for any $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ the number $\psi(\overline{\pi})$ is the complex conjugate of $\psi(\pi)$; moreover we show that $\pi{\cdot}\overline{\pi} = q$.

As Weil proved, we will see that the geometric Frobenius π_A, see 3.1, of a simple abelian variety over the finite field $\mathbb{F}_q$ is a Weil q-number, see Theorem 3.2. We will see that

$$A \sim B \quad \Rightarrow \quad \pi_A \sim \pi_B,$$

i.e. abelian varieties defined over the same finite field K isogenous over K define conjugated Weil numbers. We will write

$$\{ \text{ simple abelian variety over } \quad K\}/\sim_K \quad =: \quad \mathcal{M}(K, s)$$

for the set of isogeny classes of simple abelian varieties over K.

1.2. Theorem (Honda, Serre and Tate). *Fix a finite field $K = \mathbb{F}_q$. The assignment $A \mapsto \pi_A$ induces a bijection*

$$\boxed{\{\text{simple abelian variety over } \quad K\}/\sim_K = \mathcal{M}(K, s) \quad \xrightarrow{\sim} \quad W(q), \quad A \mapsto \pi_A}$$

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 [73].

The fact

- that the map is defined follows by Weil,
- the map is injective by Tate, and
- surjective by Honda and Tate.

This map will be denoted by

$$\mathcal{W} : \mathcal{M}(K, s) \quad \longrightarrow \quad W(q).$$

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

1.3. Definition. We say that a Weil q-number π is *effective* if there exists an abelian variety A simple over $\mathbb{F}_q$ such that $\pi \sim \pi_A$. I.e. π is effective if it is in the image of the map $\mathcal{W} : A \mapsto \pi_A / \sim$.

We indicate the steps in a proof of 1.2, which will be elaborated below. Write $K = \mathbb{F}_q$, with $q = p^n$.

ONE (Weil) *For a simple abelian variety A over a finite field $K = \mathbb{F}_q$ the Weil conjecture implies that π_A is a Weil q-number, see* Section 3, especially Theorem 3.2. *Hence the map*

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

is well-defined.

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 5.3. 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 $\mathcal{W} : \mathcal{M}(\mathbb{F}_q, s) \to W(q)$ is *well-defined and injective.* See Sections 4, 5, especially Theorem 5.3.

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 $\pi^N = \pi_{B'}$.*
See [29], Theorem 1. This step says that for every Weil q-number there *exists $N \in \mathbb{Z}_{>0}$ such that π^N is effective.* See Section 10 , especially Theorem 10.4.

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.* See Section 10, especially 10.5 - 10.9.

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

These four steps together show that the map

$$\boxed{\mathcal{W} : \ \{\text{simple abelian variety over} \quad K\}/\sim_K \ = \ \mathcal{M}(K, s) \ \stackrel{\sim}{\longrightarrow} \ W(q)}$$

is bijective, thus proving the main theorem of Honda-Tate theory.

In 1966/1967 Serre wrote a letter to Tate in which he explained a proof of the Manin conjecture; see Section 11. That method proved the surjectivity result proved by Honda. Therefore, sometimes the theory discussed here can be called the Honda-Serre-Tate theory. As Serre's proof was never published we can also use the terminology Honda-Tate theory.

We will see several examples. Here are three special cases, which we mention now in order to convey the flavor of the aspects we will encounter.

1.4. Motivation/Some examples. See 15.5. Consider the following examples.
(1) Choose $q = p^n$, and choose $i \in \mathbb{Z}_{>0}$. Let $\pi := \zeta_i \cdot \sqrt{q}$, where ζ_i is a primitive $i-$th root of unity.
(2) Choose coprime positive integers $d > c > 0$, and choose p. Let π be a zero of

$$T^2 + p^c T + p^{d+c}.$$

(3) Let $\beta := \sqrt{2 + \sqrt{3}}$, and $q = p^n$. Let π be a zero of

$$T^2 - \beta T + q.$$

In all these cases we see that π is a Weil q-number. *How can we see that these numbers are the Weil number belonging to an isogeny class of an abelian variety simple over* $\mathbb{F}_q$? Using Theorem 1.2 this follows; however these examples might illustrate that this theorem is non-trivial. If such an isogeny class exists *what is the dimension of these abelian varieties? How can we compute this dimension? What are the p-adic properties of such an abelian variety?* See 5.4, 5.5.

2. Weil numbers and CM-fields

2.1. Definition. A field L is said to be a CM-field if

- L is a finite extension of $\mathbb{Q}$ (i.e. 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 $\rho \in \mathrm{Aut}(L/L_0)$. For every embedding $\psi : L \to \mathbb{C}$ this involution on a CM-field L corresponds with the restriction of complex conjugation on $\mathbb{C}$ to $\psi(L)$.

2.2. Proposition. *Let π be a Weil q-number.*

($\mathbb{R}$) *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 ($\mathbb{R}$) we have $\psi(\pi) \in \mathbb{R}$ for every ψ.

(ℂ) *Or for every* $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ *we have* $\psi(\pi) \notin \mathbb{R}$ (equivalently: for at least one ψ we have $\psi(\pi) \notin \mathbb{R}$). *In case* (ℂ) *the field* $\mathbb{Q}(\pi)$ *is a* CM-*field.*

See 15.9, where we explain these cases in the Honda-Tate theory.

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

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

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

Write $\beta := \pi + \frac{q}{\pi}$. Then for every ψ we have

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

Hence $L_0 := \mathbb{Q}(\beta)$ is totally real. For any Weil q-number π with $\psi(\pi) \notin \mathbb{R}$ we have

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

In this case $\psi(\pi) \notin \mathbb{R}$ for every ψ, and $L_0 := \mathbb{Q}(\beta)$ is totally real and L/L_0 is totally complex. Hence L is a CM-field. $\square$

2.3. Remark. We see a characterization of Weil q-numbers:

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

and either $\pi = \sqrt{q} \in \mathbb{R}$ or π is a zero of

$$T^2 - \beta{\cdot}T + q, \quad \text{with} \quad |\ \psi(\beta)\ | < 2\sqrt{q} \quad \text{for any} \quad \psi : \mathbb{Q}(\beta) \to \mathbb{R}.$$

Using this it is easy to construct Weil q-numbers, see Section 15 for some examples.

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 21.2. 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 define:

$$\pi_A := \left(A \quad \xrightarrow{F_{A/S}} \quad A^{(p)} \quad \xrightarrow{F_{A^{(p)}/S}} \quad A^{(p^2)} \quad \longrightarrow \quad \cdots \quad \longrightarrow \quad A^{(p^n)} = A \right).$$

This endomorphism is 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. it is an algebraic integer and for every embedding $\psi : \mathbb{Q}(\pi_A) \to \mathbb{C}$ we have*

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

See [78], page 70; [79], page 138; [47], Theorem 4 on page 206. Using the following two propositions we give a proof of this theorem.

3.3. 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* $\mathrm{Tr}(x{\cdot}x^\dagger) > 0$. $\square$
See [47], Th. 1 on page 192, see [15], Th. 17.3 on page 138. For the notation D and for the notion of the Rosati involution defined by a polarization, see Section 16, in particular 16.3 and 16.5.

3.4. 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 [47], formula (i) on page 206; also see [15], Coroll. 19.2 on page 144.

Another proof of 3.4 can be found in 5.21, 7.34 and Section 15 of [GM]. To this end we study Verschiebung, see 21.3, defined for commutative flat group schemes over a base in characteristic p. The (relative) Frobenius and the Verschiebung homomorphism for abelian varieties are related by two properties:

$$\text{for any abelian variety } \ B \ \text{ we have} \left(B \xrightarrow{F} B^{(p)} \xrightarrow{V} B\right) = p,$$

also $V{\cdot}F = p{\cdot}\mathbf{1}_{B^{(p)}}$, and

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

see 21.10. For the definition of the dual abelian scheme, and for the notation A^t see 16.2. From this we see that

$$\pi_{A^t} \cdot (\pi_A)^t = \left(F_{(A^t)^{(p^{n-1})}} \cdots F_{A^t}\right) \left(F_{A^{(p^{n-1})}} \cdots F_A\right)^t =$$

$$= F_{(A^t)^{(p^{n-1})}} \left(\cdots \left(F_{(A^t)^{(p)}} \left(F_{A^t} \cdot V_{A^t}\right) V_{(A^t)^{(p)}}\right) \cdots\right) V_{(A^t)^{(p^{n-1})}} = p^n = q.$$

In abused notation we could write: $\pi_{A^t} \cdot (\pi_A)^t = F^n{\cdot}(F^n)^t = F^n{\cdot}V^n = p^n$. $\square$3.4

3.5. We give a proof of 3.2 using 3.4 and 3.3. We use that $L = \mathbb{Q}(\pi_a)$ is the center of D, see 5.4 (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 $\mathbb{C}$. Using 3.3 we conclude that 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

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

Hence

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

$\square$3.2

3.6. Definition/Notation. Let A be a *simple* abelian variety over $K = \mathbb{F}_q$. We have seen that $\pi_A \in \mathrm{End}(A) =: D$. As A is simple, D is a division algebra, and $\mathbb{Q}(\pi_A) \subset D$ is a number field (a finite extension of $\mathbb{Q}$). We have seen that π_A is a Weil q-number. *We will say that π_A is the Weil q-number attached to the simple abelian variety A.*

3.7. Simple and absolutely simple. We give an example of an abelian variety A over a field which is K-simple, such that for some extension $K' \supset K$ the abelian variety $A \otimes K'$ is not simple, i.e. A is not absolutely simple.

Choose $q = p^n$. Let $i \in \mathbb{Z}_{>0}$, and let $\zeta = \zeta_i$ be a primitive i-th root of unity. Define $\pi = \zeta{\cdot}\sqrt{q}$. Clearly π is a Weil q-number. Using Th. 1.2, we know there exists an abelian variety A over K, which is simple such that $\pi_A \sim \pi$. Assume $i > 2$; note that for any N which is a multiple of $2i$ we have $\mathbb{Q} = \mathbb{Q}(\pi^N) \subsetneqq \mathbb{Q}(\pi)$. We will see: in this case $g := \dim(A) > 1$, and $A \otimes \mathbb{F}_{q^N} \sim (E \otimes \mathbb{F}_{q^N})^g$ where E is a supersingular curve defined over $\mathbb{F}_p$. Hence in this case A is not K-simple.

3.8. Remark/Definition. We say that an abelian variety A over a field K is *isotypic* if there exists an abelian variety B simple over K and an isogeny $A \sim B^{\mu}$ for some $\mu \in \mathbb{Z}_{>0}$; in this case we will define $\pi_A := \pi_B$; note that $f_A = (f_B)^{\mu}$ (for the definition of f_A see 16.8).

We have just seen that the property " A is simple " can get lost under a field extension. However

if A is isotypic over K and $\mathbb{F}_q = K \subset K'$ is an extension then $A \otimes K'$ is isotypic;

see 10.8.

Moreover, if K is a finite field and $[K' : K] = N$ then $(\pi_A)^N = \pi_{A \otimes K'}$, i.e. the formation $A \mapsto \pi_A$ commutes under base extension with exponentiation as explained.

4. Abelian varieties with CM

4.1. 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 $\mathbb{Q}$.

If no confusion is possible we say "A admits smCM" omitting "over K". However we should be careful; it is possible that A, defined over K, does not admit smCM, but that there exists a field extension $K \subset K'$ such that $A \otimes_K K'$ admits smCM (over K').

Equivalently. Suppose $A \sim \Pi B_i$, where each of the B_i is simple. We say that A admits smCM, if every $\mathrm{End}^0(B_i)$ contains a CM-subfield of degree $2{\cdot}\dim(B_i)$ over $\mathbb{Q}$.

For other characterizations, see [18], page 63 and [44], page 347.

4.2. Note that if a simple abelian variety A of dimension g over a field *of characteristic zero* admits smCM then its endomorphism algebra $L = \mathrm{End}^0(X)$ is a field, in fact a CM-field of degree $2g$ over $\mathbb{Q}$; see 5.9. We will use he notion "CM-type" in the case of an abelian variety A over $\mathbb{C}$ which admits smCM, and where the type is given, i.e. the action of the endomorphism algebra on the tangent space $\mathbf{t}_{A,0} \cong \mathbb{C}^g$ is part of the data, see 13.1. See 13.12: we do use CM-types in characteristic zero, but we do not define (and we do not use) such a notion over fields of positive characteristic.

Note 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.

We could use the terminology " A has complex multiplication" to denote the cases with $\mathrm{End}(A) \supsetneqq \mathbb{Z}$. However this could be misleading, and in these notes we will not use this terminology.

It can be proved that if a simple abelian variety A admits smCM in the sense defined above, then $D = \mathrm{End}^0(A)$ contains a CM-field of degree $2{\cdot}\dim(A)$ over $\mathbb{Q}$. Note that a field E with $E \subset \mathrm{End}^0(A)$ and $[E : \mathbb{Q}] = 2{\cdot}\dim(A)$ however need not be a CM-field; see 15.7.

Terminology. Let $\varphi \in \mathrm{End}^0(A)$. Then $d\varphi$ is a K-linear endomorphism of the tangent space of A at $0 \in A$. See 16.9. If the base field is $K = \mathbb{C}$, this is just multiplication by a complex matrix x. Suppose $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ where Λ is a lattice in $\mathbb{C}^g$. For $\varphi \in \mathrm{End}^0(A)$ the linear map $d\varphi$ leaves $\Lambda \subset \mathbb{C}^g$ invariant. Conversely any complex linear map complex linear map $x : \mathbb{C}^g \to \mathbb{C}^g$ leaving invariant Λ defines an endomorphism φ of A with $x = d\varphi$.

Consider $g = 1$, i.e. A is an elliptic curve and $\varphi \in \mathrm{End}(A)$. If $\varphi \notin \mathbb{Z}$ then $x \in \mathbb{C}$ and $x \notin \mathbb{R}$. Therefore an endomorphism of an elliptic curve over $\mathbb{C}$ which is not in $\mathbb{Z}$ can be 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"; we will not adopt that confusing terminology. 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 terminology "a CM-abelian variety" for an abelian variety which admits smCM.

It can happen that an abelian variety A over a field K does not admit smCM, and that $A \otimes K'$ does admit smCM.

4.3. Exercise. *Show that for any elliptic curve E defined over $\mathbb{Q}$ we have* $\mathrm{End}(E) = \mathbb{Z}$.

Show there exists an abelian surface A over $\mathbb{Q}$ with $\mathbb{Z} \neq \mathrm{End}(A) = \mathrm{End}(A \otimes \overline{\mathbb{Q}})$.

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.

See 15.6, 18.10.

4.4. Remark. An abelian variety over a field of characteristic zero which admits smCM is defined over a number field. See [69], Proposition 26 on page 109. Also see [51].

We will see that a theorem of Tate, see Theorem 5.4 implies that *an abelian variety defined over a finite field does admit* smCM. By Grothendieck we know that an abelian variety which admits smCM up to isogeny is defined over a finite field, see 4.5.

4.5. Remark. The converse of Tate's result 5.4 (2) is almost true; see 5.7.

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. E. g. see 5.8.

4.6. Lemma. *Let K be a field, and let A be an abelian variety simple over K which admits* smCM. *Choose a* CM-*field P with* $[P : \mathbb{Q}] = 2{\cdot}\dim(A)$ *inside* $\mathrm{End}^0(A)$. (This is possible by Lemma 10.1.) *Then there exists a K-isogeny $A \sim_K B$ such that $\mathcal{O}_P \hookrightarrow \mathrm{End}(B)$, where $\mathcal{O}_P$ is the ring of integers of P.* $\square$See [80], page 308.

In [80] we also find: if A in positive characteristic admits smCM by a CM-field L, and the ring of integers $\mathcal{O}_L$ is contained in $\mathrm{End}(A)$ then A can be defined over a finite field, see [80], Th. 1.3. This gives a new proof of Theorem 4.5, see [80], Th. 1.4.

4.7. Definition CM-type. Let P be a CM-field of degree $2g$. Let C be an algebraically closed field *of characteristic zero.* The set $\mathrm{Hom}(P,C)$ has $2g$ elements. For any $\varphi : P \to C$ the homomorphism $\varphi{\cdot}\rho$ is different from φ. A subset $\Phi \subset \mathrm{Hom}(P,C)$ is called a CM-type for P if $\mathrm{Hom}(P,C) = \Phi \coprod \rho(\Phi)$. Equivalently: For every $\varphi : P \to C$ either $\varphi \in \Phi$ or $\varphi{\cdot}\rho \in \Phi$.

4.8. Let A be an abelian variety simple over $\mathbb{C}$ which admits smCM. Let $P = \mathrm{End}^0(A)$. This is a CM-field of degree $2{\cdot}\dim(A)$. The action of P on the tangent space $\mathbf{t}_{A,0}$ splits as a direct sum of one-dimensional representations (as P is commutative and $\mathbb{C}$ is algebraically closed of characteristic zero). Hence this representation is given by $\Phi = \{\varphi_1, \cdots, \varphi_g\}$. One shows this is a CM-type (i.e. these homomorphisms $\varphi_i : P \to C$ are mutually different and either $\varphi \in \Phi$ or $\varphi{\cdot}\rho \in \Phi$). For the converse construction see 19.6.

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

Main references: [72], [73]. Also see the second printing of [47], especially Appendix 1 by C. P. Ramanujam.

5.1. 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 18.2, we know the structure theorem of such algebras 18.4. Moreover, as Albert, Shimura and Gerritzen showed, for any algebra D in the list by Albert, and for any characteristic, there is an abelian variety having D as endomorphism algebra. However over a finite field not all types do appear, there are restrictions; see 2.2, 15.9.

For an element $\beta \in \overline{\mathbb{Q}}$ we write $\mathrm{Irr}_{\mathbb{Q}}(\beta) = \mathrm{Irr}(\beta) \in \mathbb{Q}[T]$ for the irreducible, monic polynomial having β as zero, the *minimum polynomal* of β.

5.2. 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 $f_A = f_{A,\pi_A}$ for the characteristic polynomial of π_A. We write Write $\mathrm{Irr}_{\mathbb{Q}}(\pi_A) = \mathrm{Irr}(\pi_A) \in \mathbb{Z}[T]$ for the minimum polynomial of π_A over $\mathbb{Q}$. For the definition of a characteristic polynomial of an endomorphism, see 16.8.

The following theorems are due to Tate; these results (and much more) can be found: [72], Theorem 1 on page 139, [72], Theorem 2 on page 140 and [73], Th. 1 on page 96, [47], Appendix 1.

5.3. 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 $f_A(\pi_A) = 0$.*

If an abelian variety A is K-simple then 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

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

Remark. Note that for an abelian variety A over a finite field the characteristic polynomial f_A of $\pi_A \in \mathrm{End}(A)$ is a power of an irreducible polynomial then A is isotypic (not necessarily simple); it seems that a statement in [74] in Th. 1.1 of "The theorem of Honda and Tate" needs a small correction on this point.

For an abelian variety A over a field the endomorphism algebra $\mathrm{End}^0(A)$ is a semi-simple ring. If moreover A is K-simple, then $D = \mathrm{End}^0(A)$ is a division ring (hence a simple ring).

5.4. Theorem (Tate). *Suppose A is a simple abelian variety over the finite field $K = \mathbb{F}_q$.*
(1) *The center of $D := \mathrm{End}^0(A)$ equals $L := \mathbb{Q}(\pi_A)$.*
(2) *Moreover*

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

where g is the dimension of A. Hence: every abelian variety over a finite field admits smCM. See 4.1. *We have:*

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

(3)

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

The central simple algebra D/L

- *does not split at every real place of L,*
- *does split at every finite place not above p.*
- *For a discrete valuation w of L with $w \mid p$ the invariant of D/L is given by*

$$\mathrm{inv}_w(D/L) = \frac{w(\pi_A)}{w(q)}\cdot[L_w : \mathbb{Q}_p] \mod \mathbb{Z},$$

where L_w is the local field obtained from L by completing at w. Moreover

$$\mathrm{inv}_w(D/L) + \mathrm{inv}_{\overline{w}}(D/L) = 0 \mod \mathbb{Z},$$

where $\overline{w} = \rho(w)$ is the complex conjugate of w.

5.5. Corollary/Notation. Using Brauer theory, see Section 17, 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.*
For a given Weil q-number the division algebra with invariants as described by the theorem will be denoted by $D = \mathcal{D}(\pi)$. We write $e(\pi) = [\mathbb{Q}(\pi) : \mathbb{Q}]$, and $r(\pi)^2 = [\mathcal{D}(\pi) : \mathbb{Q}(\pi)]$ and $g(\pi) = e(\pi){\cdot}r(\pi)/2$.
Note that $g(\pi) \in \mathbb{Z}$. Indeed, in case $(\mathbb{R}e)$ we have $e = 1, r = 2$. In all other cases we have that e is even. See 15.9.

5.6. Corollary. *Let A be an abelian variety over a finite field. Then A admits* smCM.
It suffices to show this in case A is simple. A splitting field of the central simple algebra $\mathbb{Q}(\pi_A) = L \subset D = \mathrm{End}^0(A)$ is a field of degree $2g$, where $g = \dim(A)$. $\square$

Note that this splitting field in general need not be, but can can be chosen to be a CM-field, see 10.1.
The converse of this corollary is almost true.

5.7. Theorem (Grothendieck). *Let K be a field with prime field $\mathbb{P}$. Let A be an abelian variety over K which admits* smCM (over K). *Write $k = \overline{K}$. There exists an isogeny $B \sim A \otimes_K k$ such that B is defined over a finite extension of $\mathbb{P}$.*
See [51], [80], Th. 1.4. Note that if $\mathrm{char}(K) = 0$ any abelian variety with smCM is defined over a finite extension of $\mathbb{P} = \mathbb{Q}$, i.e. over a number field, see [69], Prop. 26 on page 109. However in positive characteristic there are examples where this is not the case.

5.8. An easy example. *There exists a non-finite field K, and an abelian variety A over K which admits* smCM, *such that A cannot be defined over a finite field. In this case there does not exist a* CM-*lift of A to characterisitc zero.*
Indeed, choose any abelian variety B over a finite field K' such that $(\alpha_p \times \alpha_p) = N \subset B$. One can take for B the product of two supersingular elliptic curves. More generally one can take any abelian variety C over $\mathbb{F} = \overline{\mathbb{F}_p}$ with $f(C) \leq g - 2$; there exists a finite field K' and an abelian variety B/K' having the property required above such that $B_{\mathbb{F}}$ is in the $\mathbb{F}$-isogeny class of C. Choose $K = K'(t)$. Let $(1, t) : \alpha_p \to N_K$. Define $A = B_K/(1, t)(\alpha_p)$. Show that A cannot be defined over a finite field. Observe that B admits smCM by [72], see [73], Th. 1 (2); hence A admits smCM. A CM-lifting of A is defined over a number field, by [69], Prop. 26 on page 109; this would show that A can be defined over a finite field, a contradiction.

We will see that the idea of the example above is the basis for a proof of Th. 12.4.

5.9. Remark/Exercise. Let A be an abelian variety of dimension g simple over a field K. Write $D = \mathrm{End}^0(A)$.
(1) If $\mathrm{char}(K) = 0$ and A admits smCM then D is a field.
(2) If K is finite and the p-rank $f = f(A)$ satisfies $f \geq g - 1$, "A is ordinary or A is almost ordinary", then D is commutative; e.g. see [54], Proposition 3.14.

(3) There are many examples where K is finite, $f(A) < g - 1$, and D is not commutative.
(4) There are many examples of a simple abelian variety over a field k, with either $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p$ and A ordinary such that D is not commutative; see 18.4

5.10. Lemma. *Let M be a field, and $\pi \in M^{\mathrm{sep}}$ be a separable algebraic element over M. Let $N \in \mathbb{Z}_{>0}$. Let M'/M be the Galois closure over $M(\pi)/M$. Let $\{\gamma_1, \cdots, \gamma_e\}$ be the set of conjugates of π in M'. Then:*

$$M(\pi^N) \subsetneqq M(\pi) \quad \Longleftrightarrow \quad \exists z,\ i,\ j:\ 1 \neq z \in M', \quad 1 \leq i < j \leq e,\ z^N = 1, \quad \gamma_j/\gamma_i = z.$$

I thank Yuri Zarhin for drawing my attention to this fact.
Proof. Note that $\#(\{\gamma_1, \cdots, \gamma_e\}) = [M(\pi) : M]$. As $[M(\pi^N) : M]$ equals the number of mutually different elements in $\{\gamma_1^N, \cdots, \gamma_e^N\}$ the result follows. $\square$

5.11. Proposition. *Let A be an abelian variety simple over a finite field K. Let $N \in \mathbb{Z}_{>0}$ and $[K' : K] = N$. Then*

$$\mathrm{End}(A) \subsetneqq \mathrm{End}(A \otimes K') \quad \Longleftrightarrow \quad M(\pi^N) \subsetneqq M(\pi).$$

Note that the last condition is described in the previous lemma.
Proof. Note that $\mathrm{End}(A \otimes K')/\mathrm{End}(A)$ is torsion free. Hence $\mathrm{End}(A) \subsetneqq \mathrm{End}(A \otimes K')$ iff $\mathrm{End}^0(A) \subsetneqq \mathrm{End}^0(A \otimes K')$. Hence this proposition is a corollary of 5.4. $\square$

5.12. Remark. there are two "reasons" (or a combination of both) explaining $\mathrm{End}(A) \subsetneqq \mathrm{End}(A \otimes K')$.

It can happen that (although A is k-simple) $A \otimes K'$ is not K'-simple.

It can happen that $A \otimes K'$ is K'-simple but that under $K \subset K'$ the endomorphism ring gets bigger.
Both cases do appear. For some examples see 15.15, 15.16, 15.19.

6. Injectivity

6.1. 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 integer $N > 0$ which annihilates (the finite group scheme which is) $\mathrm{Ker}(\varphi)$. Show there exists an isogeny $\psi : B \to A$ 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 $\varphi{\cdot}\psi = N{\cdot}1_B$.*
Remark. Take $A = B$, and an isogeny $\varphi \in \mathrm{End}(A)$. We have constructed the inverse φ^{-1} in $\mathrm{End}^0(A)$.

6.2. Exercise. Let $A \sim B$ be a K-isogeny of simple abelian varieties over a finite field $K = \mathbb{F}_q$; using the construction 6.1 this isogeny gives an isomorphism $\mathbb{Q}(\pi_A) \cong \mathbb{Q}(\pi_B)$. *Show that this maps π_A tot π_B.*

6.3. 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

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

is well-defined.

We have seen in 5.3 (2) that Tate showed that A and B are K-isogenous if and only if $f_A = f_B$. Hence this map $\mathcal{W}$ is *injective*.

7. Abelian varieties with good reduction

References: [48], [12], [67], [63], [6], [53], [13].
This section mostly contains references to known (non-trivial) results.

7.1. Definition. Let A be an abelian variety over a field K. Let v be a discrete valuation of K. We say that A has *good reduction* at v if there exists an abelian scheme $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_v)$ with generic fiber $\mathcal{A} \otimes K \cong A$.

We say that A has *potentially good reduction* at v if there exist a finite extension $K \subset K'$, a discrete valuation v' over v such that $A' := A \otimes K'$ has good reduction at v'.

7.2. The Néron minimal model. Let Let A be an abelian variety over a field K. Let v be a discrete valuation of K. Consider the category of smooth morphisms $Y \to \mathrm{Spec}(\mathcal{O}_v) = S$ and the contravariant functor on this category given by

$$Y/S \quad \mapsto \quad \mathrm{Hom}_K(Y \times_S \mathrm{Spec}(K), A).$$

We say that $\mathcal{A} \to S$ is the *Néron minimal model*, abbreviation: Nmm, of A at v if it represents this functor.

7.3. Theorem (Néron). *For every A/K and every v the Néron minimal model of A at v exists.* $\square$
See [48]; see [15], Section VIII.

7.4. Theorem (Chevalley). *Let G be a group variety over a perfect field m.* (That is: this is an algebraic group scheme $G \to \mathrm{Spec}(m)$ which is connected, and

geometrically reduced.) *There exists a filtration by subgroup varieties* $G_1 \subset G_2 \subset G$ *over* m *such that* G_1 *is a torus* (i.e. $G_1 \otimes \overline{m}$ is isomorphic with a product of copies of $\mathbb{G}_m$), G_2/G_1 *is affine, unipotent and* G/G_2 *is an abelian variety.*
See [12]; see [13], Th. 1.1 on page 3. $\square$

7.5. Definition. Let A be an abelian variety over a field K. Let v be a discrete valuation of K. Let $A^0_{k_v}$ be the connected component containing 0 of the special fiber of the Néron minimal model $\mathcal{A}$. We say that A has *stable reduction* at v if in the Chevalley decomposition of $A^0_{k_v}$ the unipotent part is equal to zero. We say A has *potentially stable reduction* at $v \in \Sigma_K$ if there exist a finite extension $K \subset K'$, a discrete valuation v' over v such that $A' := A \otimes K'$ has stable reduction at v'.

7.6. We refer to the literature, especially to [63], for the notions of ℓ-adic representations, algebraic monodromy, and the fact that for an abelian variety the ℓ-adic monodromy at a discrete valuation of the base field is quasi-unipotent.

As a corollaries of these ideas on can prove:

7.7. Theorem (The Néron-Ogg-Shafarevich criterion). *Suppose* A *has stable, respectively good reduction at* v *and* $B \sim_K A$. *Then* B *has stable, respectively good reduction at* v. $\square$

7.8. Theorem (Grothendieck). *Every* A/K *has potentially stable reduction at every* $v \in \Sigma_K$. $\square$

7.9. Corollary. *Let* A *be an abelian variety over a field* K *which admits* smCM. *At every* $v \in \Sigma_K$ *the abelian variety* A *has potentially good reduction.*
Sketch of a proof. After extending of the base field and choosing v again we can assume that A has stable reduction at v, where the residue class field of v is perfect. Up to isogeny we can write $A \sim \prod B_i$, with every B_i simple. By the Néron-Ogg-Shafarevich criterion we conclude every B_i has stable reduction. Hence it suffice to show: if A is K-simple + has stable reduction at v + admits smCM then A has good reduction at v.

Let $\mathcal{A}$ be its Nmm, and let $G = A^0_{k_v}$ be the connected component of the special fiber of $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_v)$. By properties of the Nmm we conclude that $\mathrm{End}^0(A) \subset \mathrm{End}(G)$. Consider the Chevalley decomposition in this case $G_1 = G_2 \subset G$. Let μ be the dimension of G_1. We obtain homomorphisms

$$\mathrm{End}^0(A) \to \mathrm{End}(G_1), \qquad \mathrm{End}^0(A) \to \mathrm{End}(G/G_1).$$

If $\mu = \dim(G_1) > 0$ it follows that $\mathrm{End}^0(A) \to \mathrm{End}(G_1) \subset \mathrm{Mat}(\mu, \mathbb{Z})$; it follows that this homomorphism is injective; given the fact that A admits smCM we derive a contradiction. Hence $\mu = 0$. Alternative argument: if $\mu > 0$, the dimension of $B = G/G_1$ is strictly smaller than $\dim(A)$ and the fact that A has smCM shows there does not exist a homomorphism $\mathrm{End}^0(A) \to \mathrm{End}^0(B)$. This contradiction shows $\mu = 0$, and hence A admits good reduction at v. $\square$

7.10. Remark. Also see 15.10. Let R be a normal integral domain, $\mathcal{A} \to S = \mathrm{Spec}(R)$ an abelian scheme, and $R \to K$ a homomorphism to a field K. Write $A_K = \mathcal{A} \otimes_R K$. We obtain a homomorphism

$$\mathrm{End}(\mathcal{A}) \quad \longrightarrow \quad \mathrm{End}(A_K).$$

This homomorphism is injective.

In general this homomorphism is *not surjective.*

If R is normal and K is the field of fractions of R the homomorphism is surjective (hence bijective).

If ℓ is a prime not equal to the characteristic of K, the additive factor group $\mathrm{End}(A_K)/\mathrm{End}(\mathcal{A})$ has no ℓ-torsion.

There are many examples where $R \to R/I = K$ gives a factor group $\mathrm{End}(A_K)/\mathrm{End}(\mathcal{A})$ which does have p-torsion, where $p = \mathrm{char}(K)$.

8. p-divisible groups

Also see Section 20.

8.1. For an abelian variety A over a base S and a prime number ℓ *which is invertible in the structure sheaf* on S one defines the ℓ-Tate module $T_\ell(A) := \lim_{\leftarrow i} \ A[\ell^i]$. This is a pro-group scheme. It can also be viewed as a local system with fiber $\mathbb{Z}_\ell$ under the fundamental group of S.

For an arbitrary prime number (not necessarily invertible on the base) we choose another strategy:

8.2. Definition. Let S be a scheme. Let $h \in \mathbb{Z}_{\geq 0}$. A p-divisible group, of height h, over S is an inductive system of finite flat group schemes $G_i \to S, \quad i \in \mathbb{Z}_{\geq 0}$, such that:

- the rank of $G_i \to S$ equals $p^{h \cdot i}$;
- p^i annihilates G_i;
- there are inclusions $G_i \hookrightarrow G_{i+1}$ such that
- $G_{i+1}[p^i] = G_i$.
- Consequently $G_{i+j}/G_i = G_j$.

We will write $G = \mathrm{colim}_{i \to} G_i$; this limit considered in the category of inductive systems of finite group schemes. A p-divisible group is also called a Barsotti-Tate group.

Examples. (1) For any abelian scheme $A \to S$ (over any base), and any integer $n \in \mathbb{Z}_{>0}$ the group scheme $A[n] \to S$ is a finite flat group scheme of rank n^{2g} over S, where $g = \dim(A)$; see [47], proposition on page 64, see [15], V, Theorem 8.2 on page 115. Hence

$$\{A[p^i] \ \mid \ i \in \mathbb{Z}_{\geq 0}\}$$

is a p-divisible group of height $2g$. This will be denoted by $A[p^\infty]$. This notation should be understood symbolically: there is no morphism "$\times\infty$" and hence, strictly speaking, no "kernel" $A[p^\infty]$.

(2) Consider $\mathbb{G}_{m,S} \to S$, the multiplicative group over any base scheme S. Then

$$\mathbb{G}_{m,S}[p^i] =: G_i = \mu_{p^i,S}, \quad \text{and this defines} \quad \mathbb{G}_{m,S}[p^\infty] \to S,$$

a p-divisible group over S of height one.
(3) Consider $\mathbb{Q}_p/\mathbb{Z}_p$, which is a profinite group, which can be given by $\mathrm{colim}_{i\to}(\mathbb{Z}/p^i)$. By considering the constant group schemes $\underline{(\mathbb{Z}/p^i)}_S$ we obtain a p-divisible group $\underline{(\mathbb{Q}_p/\mathbb{Z}_p)}_S$.

8.3. The Serre dual of a p-divisible group. Let $G = \{G_i \mid i \in \mathbb{Z}_{\geq 0}\}/S$ be a p-divisible group over some base scheme S. The surjections $G_{i+1} \twoheadrightarrow G_{i+1}/G_1 = G_i$ define by Cartier duality inclusions $(G_i)^D \hookrightarrow (G_{i+1})^D$; see 16.5. This defines a p-divisible group

$$G^t := \{(G_i)^D \mid i\} \to S,$$

which is called the Serre dual of $G \to S$.

Note that $G \mapsto G^t$ is a duality for p-divisible groups, which is is defined by purely algebraic methods. We see a duality $A \mapsto A^t$ for abelian schemes, see 16.2, which is a (non-trivial) geometric theory. Notation is chosen in this way, because the duality theorem connects these two operation in a natural way: $A^t[p^\infty] = A[p^\infty]^t$, see 16.6; note that this fact is more involved than this simple notation suggests.

8.4. Exercise. Show that $(\mathbb{G}_{m,S}[p^\infty])^t = \underline{\mathbb{Q}_p/\mathbb{Z}_p}_S$.

9. Newton polygons

For a p-divisible group X or an abelian variety A over a field of characteristic p the Newton polygon $\zeta = \mathcal{N}(X)$, respectively $\xi = \mathcal{N}(A) := \mathcal{N}(A[p^\infty])$ is defined, see Section 21. In this section we give an easier definition in case we work with an abelian variety over a finite field, and we show that this coincides with the more general definition as recorded in Section 21.

9.1. Notation. Let $K = \mathbb{F}_q$ be a finite field, $q = p^n$ and let A be an abelian variety over K of dimension g. We have defined the geometric Frobenius $\pi = \pi_A \in \mathrm{End}(A)$; this endomorphism has a characteristic polynomial $f_A \in \mathbb{Z}[T]$, see 16.8; this is a monic polynomial of degree $2g$.

Suppose that A is simple. The algebraic integer π_A is a zero of its minimum polynomial $\mathrm{Irr}(\pi) \in \mathbb{Z}[T]$; this is a monic polynomial, and its degree equals $e = [\mathbb{Q}(\pi) : \mathbb{Q}]$. In this case $f_A = (\mathrm{Irr}(\pi))^r$, where r^2 is the degree of $D = \mathrm{End}^0(A)$ over its centre $L = \mathbb{Q}(\pi)$.

Suppose $f_A = \sum_j \; b_j T^{2g-j}$. We define $\xi = \xi(A)$ as a *lower convex hull*, written as lch():

$$\xi(A) = \mathrm{lch}\left(\{(j, v_p(b_j)/n) \mid o \leq j \leq 2g\}\right).$$

This is the Newton polygon of f_A compressed by the factor n. Note that if A is simple with $\mathrm{Irr}(\pi_A) = \sum_i c_i T^{e-i}$ then $\xi(A) = \mathrm{lch}(\{(r{\cdot}i, r{\cdot}v_p(c_i)/n) \mid 0 \leq i \leq e\})$.

9.2. Theorem. *Let A be an abelian variety isotypic over a finite field $K = \mathbb{F}_q$, with $q = p^n$. As above we write $\pi = \pi_A$, the geometric Frobenius of A, and $L = \mathbb{Q}(\pi)$ with $[L : \mathbb{Q}] = e$ and $D = \mathrm{End}^0(A)$ with $[D : L] = r^2$ and $\dim(A) = g = er/2$. Let $X = A[p^\infty]$. Consider the set $\Sigma_L^{(p)}$ of discrete valuations of L dividing the rational prime number p. Let $L \subset P \subset D$, where P is a* CM*-field of degree $2g$* (existence assured by 10.1. *If necessary we replace A be a K-isogenous abelian variety* (again called A) *such that $\mathcal{O}_P \subset \mathrm{End}(A)$, see* 4.6. *Then also $\mathcal{O}_L \subset \mathrm{End}(A)$.*
(1) *The decomposition*

$$D \otimes \mathbb{Q}_p = \prod_{w \in \Sigma_L^{(p)}} D_w, \qquad \mathcal{O}_L = \prod \mathcal{O}_{L_w},$$

gives a decomposition $X = \prod_w X_w$.
(2) *The height of X_w equals $[L_w : \mathbb{Q}_p]{\cdot}r$.*
(3) *The p-divisible group X_w is isoclinic of slope γ_w equal to $w(\pi_A)/w(q)$; note that $q = p^n$.*
(4) *Let $\overline{w}$ be the discrete valuation of L obtained from w by complex conjugation on the* CM*-field L; then $\gamma_w + \gamma_{\overline{w}} = 1$.*
See [77]. We will give a proof of one of the details.
Proof. (3) Fix $w \in \Sigma_L^{(p)}$, and write $Y = X_w$. Write $w(\pi_A)/n = d/h$ with $\gcd(d, h) = 1$. The kernel of

$$Y \xrightarrow{F} Y^{(p)} \xrightarrow{F} \cdots \xrightarrow{F} Y^{(p^{nh})}$$

will be denoted by $Y[F^{nh}]$
Claim. $Y[F^{nh}] = Y[p^{nd}]$.
The action of π on Y is given by F^n. We see that $w(F^{nh}/p^{nd}) = 0$. This proves that this quotient (in $\mathcal{O}_L$) acts by a unit on Y, which proves the claim. $\square$

By the Dieudonné-Manin theory we know that $Y \otimes \mathbb{F} \sim \prod G_{d_i,c_i} \otimes \mathbb{F}$. We know that $G_{d_i,c_i}[F^{c_i+d_i}] = G_{d_i,c_i}[p^{d_i}]$. By the claim this proves that in this decomposition only factors $(d_i, c_i) = (d, h-d)$ do appear, see 21.22. This proves proves that Y is isoclinic of slope equal to d/h. $\square$**(3)**

9.3. Corollary. *The polygon $\xi(A)$ constructed in* 9.1 *for an abelian variety A over a finite field equals the Newton polygon $\mathcal{N}(A)$,* as defined in Section 21.

9.4. Remark. Let A be an abelian variety over a finite field K. By the Dieudonné-Manin theory we know that $A[p^\infty] = X$ has the property that there exists a p-divisible group Y over $\mathbb{F}_p$ such that $X \otimes_K \mathbb{F} \sim Y \otimes_{\mathbb{F}_p} \mathbb{F}$. Hence $\xi(A) = \mathcal{N}(A) = \mathcal{N}(Y)$ as we have seen above. We could try to prove the corollary above by comparing the minimum polynomial of π_A and the same of Y over some common finite field. However in general one cannot compute f_A from the characteristic polynomial of $Y/\mathbb{F}_p$, as is shown by examples below.

9.5. **(1)** Let E be a supersingular elliptic curve over a finite field $K = \mathbb{F}_q$; see 21.8. We will see, 14.6, that there exists a root of unity ζ_i such that $\pi_E \sim \zeta_i\sqrt{q}$. Hence $\pi' := \pi_{E\otimes K'} = q^i$, with $K' = \mathbb{F}_{q'}$, where $q' = q^{2i} = p^{2ni}$. We can choose $Y/\mathbb{F}_q$ with $F_Y = \pm\sqrt{p}$ and $Y \otimes \mathbb{F} \cong E[p^\infty] \otimes \mathbb{F}$. Note the curious fact that in this case for a finite exension we have equality: $(F_Y)^{2ni} = \pi'$.
(2) Let E be an ordinary elliptic curve over a finite field $K = \mathbb{F}_q$, with $f_E \in \mathbb{Z}[T]$ the characteristic polynomial of π_E. For $Y = G_{(1,0)} + G_{(0,1)}$ we have $E[p^\infty] \otimes_K \mathbb{F} \cong Y \otimes_{\mathbb{F}_p} \mathbb{F}$. However, for every finite field $K' \supset K$ the p-divisible groups $E[p^\infty] \otimes_K K'$ and $Y \otimes_{\mathbb{F}_p} K'$ are *not isomorphic*. In this case the minimum polynomial of the geometric Frobenius of $E \otimes K'$ is different from the same of $Y \otimes K'$, although $\mathcal{N}(E) = \mathcal{N}(Y)$.

9.6. The Shimura-Taniyama formula. Suppose given an abelian variety A of CM-type (P, Φ) over a number field M having *good reduction at a discrete valuation* $v \in \Sigma_M$. Can we compute from these data the slopes of the geometric Frobenius π_0 of the reduction A_0/K_v over the residue class field of v ? The formula of Shimura and Taniyama precisely gives us this information.

Let $\mathcal{A}$ be the Nmm of A at v. We have

$$P = \mathrm{End}^0(A) = \mathrm{End}^0(\mathcal{A}) \hookrightarrow \mathrm{End}^0(A_0).$$

Let ℓ be a prime different form the characteristic of K_v. We see that $P \otimes \mathbb{Q}_\ell \subset \mathrm{End}^0(A) \otimes \mathbb{Q}_\ell$. As $P : \mathbb{Q}] = 2{\cdot}\dim(A)$ it follows that $P \subset \mathrm{End}^0(A)$ is its own centralizer; hence $L := \mathbb{Q}(\pi_{A_0}) \subset P$. Moreover $\pi := \pi_{A_0}$ is integral over $\mathbb{Z}$; hence $\pi \in \mathcal{O}_P$.

Let C be an algebraically closed field containing $\mathbb{Q}_p$. We have

$$H := \mathrm{Hom}(P, C), \quad H_w = \mathrm{Hom}(P_w, C), \quad H = \coprod_{w \in \Sigma_P^{(p)}} H_w.$$

We define $\Phi_w := \Phi \cap H_w$. Write $K_v = \mathbb{F}_q$. With these notations we have:

9.7. Theorem (the Shimura-Taniyama formula).

$$\forall w \in \Sigma_P, \quad w \mid p, \qquad \frac{w(\pi)}{w(q)} = \frac{\#(\Phi_w)}{\#(H_w)}.$$

See [69], §13; see [40], Corollary 2.3.
Tate gave a proof based on "CM-theory for p-divisible groups". See [73],Lemma 5; see [74], Shimura-Taniyama formula by B. Conrad, Theorem 2.1. □
See 13.12 for a further discussion.

10. Surjectivity

In this section we prove surjectivity of the map $\mathcal{W} : \mathcal{M}(K, s) \to W(q)$, hence finishing a proof for Theorem 1.2. We indicate the structure of the proof by subdividing it into the various steps.

Step (1) Proving $\mathcal{W}$ is surjective means showing every Weil number is effective, see 1.3. We start with a choice $q = p^n$, and with the choice of a Weil q-number π. In case $\pi \in \mathbb{R}$ we know effectivity. From now on we suppose that π is non-real.

Step (2) A Weil q-number π determines a number field $\mathbb{Q}(\pi) = L$ and a division algebra $D = \mathcal{D}(\pi)$; see 5.5. In the case considered π is non-real and L is a CM-field.

Step (3) We *choose* a CM-field $P \subset D$ of degree $2g$ over $\mathbb{Q}$, which is possible by the following lemma.

10.1. Lemma. *Suppose given a* CM-*field* L *and a central division algebra* $L \subset D$. *There exists* $L \subset P \subset D$ *where* P *is a* CM-*field splitting* D/L. See [73], Lemme 2 on page 100. $\square$
See Exercise 15.7

Step (4) Given π and $L \subset P \subset D = \mathcal{D}(\pi)$ as above we will *choose* a CM-type Φ for P such that

$$\forall w \in \Sigma_L^{(p)}, \quad w \mid p, \qquad \frac{w(\pi)}{w(q)} = \frac{\#(\Phi_w)}{\#(H_w)}.$$

Here $\Sigma_L^{(p)}$ is the set of finite places of L dividing p. We have a decomposition $L \otimes \mathbb{Q}_p = \prod L_w$; hence a decomposition

$$H := \mathrm{Hom}(L, \overline{\mathbb{Q}_p}) = \coprod \mathrm{Hom}(L_w, \overline{\mathbb{Q}_p}); \quad \text{write} \quad H_w = \mathrm{Hom}(L_w, \overline{\mathbb{Q}_p}); \qquad \Phi = \coprod \Phi_w.$$

The set $\Phi \subset H$ defines the sets $\Phi_w \subset H_w$; conversely $\{\Phi_w \mid w \in \Sigma_L^{(p)}\}$ determines Φ.

Claim. *The involution* $\varphi \mapsto \varphi{\cdot}\rho$ *has no fixed points on* $H := \mathrm{Hom}(L, \overline{\mathbb{Q}_p})$.
Proof. Embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{Q}_p$ give an identification $H = \mathrm{Hom}(L, \mathbb{C})$, compatible with $-{\cdot}\rho$. We know that ρ on L is complex conjugation on every embedding $L \hookrightarrow \mathbb{C}$. Hence, if we would have $\varphi = \varphi{\cdot}\rho$ we conclude that $\varphi(L) \subset \mathbb{R}$. However a CM-field is totally complex. This contradiction shows that $-{\cdot}\rho$ has no fixed point on $\mathrm{Hom}(L, \mathbb{C}) = H = \mathrm{Hom}(L, \overline{\mathbb{Q}_p})$. $\square$

Construction. Notation will be chosen in relation with 9.2. For every $w \in \Sigma_L^{(p)}$ we define:

- $\beta_w = w(\pi)/w(q)$;
- $h_w = [L_w : \mathbb{Q}_p]{\cdot}r$, where $r = r_\pi = \sqrt{[\mathcal{D}(\pi) : \mathbb{Q}(\pi)]}$;
- $d_w := h_w{\cdot}\beta_w$.

Note that complex conjugation induces (for every embedding) an involution $\rho : P \to P$, which restricts to an involution $\rho : L \to L$ which is also complex conjugation on L. We see that $\rho(w) = w$ or $\rho(w) \neq w$.

If $\rho(w) = w$ we conclude that $\beta_w = 1/2$. In this case we choose for $\Phi_w \subset H_w$ any subset such that $\#(\Phi_w) = \#(H_w)/2$ and $\Phi_w \cap \Phi_w{\cdot}\rho = \emptyset$; this is possible as $-{\cdot}\rho$ has no fixed point on H.

If $\rho(w) \neq w$ we make a choice $\Phi_w \subset H_w$ such that $\#(\Phi_w) = d_w$, and we define $\Phi_{\rho(w)} = H_{\rho(w)} - \Phi_w{\cdot}\rho$; this ends a choice for the pair $\{w, \rho(w)\}$. This ends the construction.

Step (5) Given the CM-type (P, Φ) as above, in particular $\Phi_w \cap \Phi_w{\cdot}\rho = \emptyset$ and $\#(\Phi_w) = d_w$ for every w, we construct B over M as follows.

10.2. *We choose a number field M, an abelian variety B defined over M, and $v \in \Sigma_M^{(p)}$ with residue class field $K_v := \mathcal{O}_v/m_v \supset \mathbb{F}_q$ such that* $\mathrm{End}^0(B) = P$, *with* Φ *as* CM-type, *and such that B has good reduction at v.*
Notation. Write $[K_v : \mathbb{F}_q] = m$; write B_v for the abelian variety defined over K_v obtained by reduction of B at v.
Proof. By 19.6 we construct an abelian variety B' over $\mathbb{C}$ of CM-type (P, Φ). By [69], Proposition 26 on page 109 we know that B'' can be defined over a number field. We can choose a finite extension so that all complex multiplications are defined over that field. By 7.9 we know that an abelian variety with smCM has potentially good reduction; hence we can choose a finite extension of the base field and achieve good reduction everywhere. We choose a discrete valuation dividing p. Conclusion: after a finite extension we can achieve that B is an abelian variety defined over a number field M, with $B \otimes_M \mathbb{C} \cong B'$, and $v \in \Sigma_M^{(p)}$ such that all properties mentioned above are satisfied.

10.3. 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. $\square$
See [28], page 402 (page 520 in the second printing).

Step (6) *Suppose given π, and (P, Φ) and B/M as constructed above. There exist $s \in \mathbb{Z}_{>0}$ and an s-root of unity ζ_s such that*

$$\pi^m = \zeta_s{\cdot}\pi_{B_v}.$$

This implies that

$$\pi^{ms} = \pi_{B_v}^s = \pi_{B_v \otimes \mathbb{F}_{q^{ms}}}.$$

Hence π^N is effective with $N := ms$.
Proof. We have $\pi \in \mathcal{O}_L \subset P$. Also we have $\pi_{B_v} \in \mathcal{O}_P$. Let $\zeta := \pi^m/\pi_{B_v}$, where $[K_v : \mathbb{F}_q] = m$. As π^m and π_{B_v} are Weil $\#(K_v)$-numbers condition (i) of the previous lemma is satisfied. For every prime not above p these numbers are units, hence condition (ii) is satisfied for primes of P not dividing p. For every $w \in \Sigma_P^{(p)}$

we can apply the Shimura-Taniyama formula, see 9.7, to π_{B_v}; for the restriction of w to L we can apply 9.2 (3) to π; these shows that $w(\zeta) = 1$ for every $w \in \Sigma_P^{(p)}$. Hence the conditions mentioned in the previous lemma are satisfied. By the lemma $\zeta \in \mathcal{O}_P$ is a root of unity, say $\zeta = \zeta_s$. Hence π^N is effective for $N := ms$. This means that $\pi^N = \pi^{ms} = \pi_{B_v \otimes \mathbb{F}_{q^{ms}}}$ is effective. $\square$

The arguments in this section up to here in fact prove the following fundamental theorem.

10.4. Theorem (Honda). *Let $K = \mathbb{F}_q$. Let A_0 be an abelian variety, defined and simple over K. Let $L \subset \mathrm{End}^0(A_0)$ be a* CM*-field of degree $2g$ over $\mathbb{Q}$. There exists a finite extension $K \subset K'$, an abelian variety B_0 over K' and a K'-isogeny $A_0 \otimes_K K' \sim B_0$ such that B_0/K' satisfies* (CML) *by L.* $\square$
See [29], Th. 1 on page 86, see [73], Th. 2 on page 102. For the notion (CML) see 12.2.

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

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

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

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

In this situation, with K'/K separable, 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. 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 [25], Exp. 195, page 195-13. Also see [74], Nick Ramsey - CM seminar talk, Section 2.

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

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

$\square$

See [73], page 100.

We make a little detour. From [14], 3.19 we cite:

10.7. Theorem (Chow). *Let K'/K be an extension such that K is separably closed in K'.* (For example K' is finite and purely inseparable over K.) *Let A and B be abelian varieties over K. Then*

$$\mathrm{Hom}(A, B) \quad \xrightarrow{\sim} \quad \mathrm{Hom}(A \otimes K', B \otimes K')$$

is an isomorphism. In particular, if A is K-simple, then $A \otimes K'$ is K'-simple. $\square$

10.8. Claim.

For an isotypic abelian variety A over a field K, and an extension $K \subset K'$, we have that $A \otimes K'$ is isotypic.

Proof. It suffices to this this in case A is K-simple. It suffices to show this in case K'/K is finite. Moreover, by the previous result it suffices to show this in case K'/K is separable.

Let $K \subset K'$ be a separable extension, $[K' : K] = N$. Write $\Pi = \Pi_{\mathrm{Spec}(K')/\mathrm{Spec}(K)}$. For any abelian variety A over K we have $\Pi(A \otimes_K K') \cong A^N$, and for any C over K' we have $\Pi(C) \otimes_K K' \cong C^N$, as can be seen by the construction; e.g. see the original proof by Weil, or see [74], Nick Ramsey - CM seminar talk, Section 2; see 10.5. If there is an isogeny $A \otimes_K K' \sim C_1 \times C_2$, with non-zero C_1 and C_2 we have $\Pi(C_1 \times C_2) \sim A^N$. Hence we can choose positive integers e and f with $\Pi(C_1) \sim A^e$ and $\Pi(C_2) \sim A^f$. Hence

$$\Pi(C_1) \otimes K' \cong (C_1)^N \sim (A \otimes_K K')^{eN}, \quad (C_2)^N \sim (A \otimes_K K')^{fN};$$

hence $\mathrm{Hom}(C_1, C_2) \neq 0$. We conclude: if A is simple, any two isogeny factors of $A \otimes_K K'$ are isogenous. $\square$

By Step 6 and by Lemma 10.6 we conclude:

10.9. Corollary (Tate). *Let π be a Weil q-number and $N \in \mathbb{Z}_{>0}$ such that π^N is effective. Then π is effective.*
See [73], Lemme 1 on page 100. $\square$

Remark. The abelian variety B_v as constructed above is isotypic and hence π_{B_v} is well-defined. It might be that the B_v thus obtained is not simple. Moreover $A := \Pi_{K'/K}(B_v)$ is isotypic with $\pi_A \sim \pi$.

Step (7) **End of the proof.** By the theorem by Honda we know that there exists $N \in \mathbb{Z}_{>0}$ such that π^N is effective. We conclude that π is effective. Hence we have proved that $\mathcal{W} : \mathcal{M}(K, s) \to W(q)$ is surjective. $\square$Theorem 1.2

Warning (again). 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.

10.10. 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 $\mathbb{Q}(\pi_A) = \mathbb{Q}(\pi')$ for every $N \in \mathbb{Z}_{>0}$ implies that A is absolutely simple (i.e. $A \otimes \mathbb{F}$ is simple).

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

11. A conjecture by Manin

We recall an important corollary from the Honda-Tate theory. This result was observed and proved independently by Honda and by Serre.

11.1. Definition. Let ξ be a Newton polygon. Suppose it consists of slopes $1 \geq \beta_1 \geq \cdots \geq \beta_h \geq 0$. We say that ξ is *symmetric* if $h = 2g$ is even, and for every $1 \leq i \leq h$ we have $\beta_i = 1 - \beta_{h+1-i}$.

11.2. Proposition. *Let A be an abelian variety in positive characteristic, and let $\xi = \mathcal{N}(A)$ be its Newton polygon. Then ξ is symmetric.*
Over a finite field this was proved by Manin, see [39], page 74; in that proof the functional equation of the zeta-function for an abelian variety over a finite field is used. The general case (an abelian variety over an arbitrary field of positive characteristic) follows from [49], Theorem 19.1; see 21.23.

11.3. Exercise. Give a **proof** of this proposition in case we work over a finite field. Suggestion: use 9.2.

Does the converse hold? I.e.:

11.4. Conjecture (Manin, see [39], 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 in $\mathcal{A}_g \otimes \mathbb{F}_p$; see [32], Th. 2.3.1 on page 143.

11.5. Proof of the Manin Conjecture (Serre, Honda), see [73], 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

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

with $f \geq 0$, $s \geq 0$ and moreover $d_i > c_i > 0$ being coprime integers.

Note that $\mathcal{N}(A) \cup \mathcal{N}(B) = \mathcal{N}(A \times B)$; here we write $\mathcal{N}(A) \cup \mathcal{N}(B)$ for the Newton polygon obtained by taking all slopes in $\mathcal{N}(A)$ and in $\mathcal{N}(B)$, and arranging them in non-decreasing order.

We know that for an ordinary elliptic curve E we have $\mathcal{N}(E) = (1,0)+(0,1)$, and for a supersingular 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

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

For such integers we consider a zero π of the poynomial

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

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 5.4 (3), the Newton polygon of U tells us the p-adic values of zeros of U; this shows that the invariants of D/L are c/n and d/n. This proves that $[D : L] = n^2$. Using Theorem 1.2 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 $n = d + c$. Using 9.2 (3) we compute the Frobenius slopes: we conclude that $\mathcal{N}(A) = (d, c) + (c, d)$. Hence, using the theorem by Honda and Tate, see 1.2, the Manin conjecture is proved. $\square$

11.6. Exercise. *Let $g > 2$ be a prime number and let A be an abelian variety simple over a finite field K of dimension g. Show that either* $\mathrm{End}^0(A)$ *is a field, or* $\mathrm{End}^0(A)$ *is of* Type(1,g), i.e. a division algebra of rank g^2 central over an imaginary quadratic field. *Show that for any odd prime number in every characteristic both types of endomorphism algebras do appear.* See [54], 3.13.

11.7. Exercise. 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.*

11.8. We have seen a proof of the Manin conjecture using the Honda-Tate theory. For a reference to a different proof see 21.25.

12. CM-liftings of abelian varieties

References: [56], [11].

12.1. Definition. Let A_0 be an abelian variety over a field $K \supset \mathbb{F}_p$. We say A/R is a *lifting of A_0 to characteristic zero* if R is an integral domain of characteristic zero, with a ring homomorphism $R \to K$, and $A \to \mathrm{Spec}(R)$ is an abelian scheme such that $A \otimes_R K = A_0$.

12.2. Definition. Suppose A_0 be an abelian variety over a field $K \supset \mathbb{F}_p$ such that A_0 admits smCM. We say A is a CM-*lifting of A_0 to characteristic zero* if A/R is a lifting of A_0, and if moreover A/R admits smCM. If this is the case we say that A_0/K satisfies (CML). Moreover, if $L \subset \mathrm{End}^0(A_0)$ is a CM- field of degree $2g$ over $\mathbb{Q}$ and $\mathrm{End}^0(A) = L$ we say that A_0/K satisfies (CML) by L.

We say that A_0/K satisfies (CMLN), if A_0 admits a CM-*lifting to a normal characteristic zero domain.*

Note that in these cases $\mathrm{End}^0(A_M) = \mathrm{End}^0(A) \hookrightarrow \mathrm{End}^0(A_0)$ need not be bijective.

12.3. As Honda proved, [29], Th. 1 on page 86, see [73], Th. 2, see 10.4, for an abelian variety A over a finite field, after a finite field extension, and after an isogeny we obtain an abelian vareity $B_0 \sim A \otimes K'$ which admits a CM-lifting to characteristic zero.

Question 1. *Is an isogeny necessary* ?

Question 2. *Is a field extension necessary* ?

12.4. Theorem I. *For any $g \geq 3$ and for any $0 \leq f \leq g-2$ there exists an abelian variety A_0 over $\mathbb{F} = \overline{\mathbb{F}_p}$, with $\dim(A) = g$ and of p-rank $f(A) = f$, such that A_0 does not admit a* CM-*lifting to characteristic zero.*
See [56], Th. B on page 131. Compare 5.8.

We indicate the essence of the proof; for details, see [56].
(1) Suppose given a prime number p, and a symmetric Newton polygon ξ which is non-supersingular with $f(\xi) \leq g-2$. Using [36] choose an abelian variety C over $\mathbb{F} = \overline{\mathbb{F}_p}$ with $\mathcal{N}(C) = \xi$ such that $\mathrm{End}^0(C)$ is a *field*.
(2) Choose an abelian variety B over a finite field K such that $B \otimes \mathbb{F} \sim C$, such that $a(B) = 2$ and such that for every $\alpha_p \subset B$ we have $a(B/\alpha_p) \leq 2$. For a definition of the a-number, see 21.7. Fix an isomorphism $(\alpha_p \times \alpha_p)_K \xrightarrow{\sim} B[F,V] \subset B$. Important observation. Suppose $t \in \mathbb{F}$; suppose $B_{\mathbb{F}}/((1,t)(\alpha_p) =: A_t$ can be defined over K', with $K \subset K' \subset \mathbb{F}$. Then $t \in K'$.
(3) We study all quotients of the form $B_{\mathbb{F}}/((1,t)(\alpha_p) = A_t$ and see which one can be CM-lifted to characteristic zero. Because $\mathrm{End}^0(B)$ is a field, we can classify all such CM-liftings over $\mathbb{C}$, and arrive at:
(4) There exist $K \subset K' \subset \Gamma \subset \mathbb{F}$ such that $[K' : K] < \infty$, moreover Γ/K' is a pro-p-extension, and if $t \notin \Gamma$ then A_t does not a CM-lift to characteristic zero. Note that $\Gamma \subsetneqq \mathbb{F}$, and hence the theorem is proved. $\square$

Conclusion. An isogeny is necessary. *In general, an abelian variety defined over a finite field does not admit a* CM-*lifting to characteristic zero.*

12.5. Definition. Let $K = \mathbb{F}_q$. Let A_0 be an abelian variety, defined over K. We say that A_0/K satisfies (CMLI), *can be* CM-*lifted after an isogeny*, if there exist $A_0 \sim B_0$ such that B_0 satisfies (CML). We say A_0/K satisfies (CMLNI), if moreover if B_0 can be chosen satisfying (CMLN).

12.6. At present it is an open problem whether any abelian variety defined over a finite field satisfies (CMLI), see 22.2

12.7. Theorem IIs / Example. (Failure of CMLNI.) (B. Conrad) *Let $\pi = p\zeta_5$. This is a Weil p^2-number. Suppose $p \equiv 2, 3 \pmod 5$.* Note that this implies that p is inert in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$. *Let A be any abelian variety over $\mathbb{F}_{p^2}$ in the isogeny class corresponding to this Weil number by the Honda-Tate theory, see* 1.2. Note that $\dim(A) = 2$ and $\mathrm{End}^0(A) \cong L = \mathbb{Q}(\zeta_5)$ and A is supersingular. *The abelian variety $A/\mathbb{F}_{p^2}$ does not satisfy* CMLN *up to isogeny.*
A proof, taken from [11], will be given in Section 13.

12.8. Remark. The previous example can be generalized. Let ℓ be a prime number such that $L = \mathbb{Q}(\zeta_\ell)$ contains no proper CM field (e.g. ℓ is a Fermat prime). Let p be a rational prime, such that the residue class field of L above p has degree more than 2. Let $\pi = p\zeta_\ell$ and proceed as above. Note that also in this example we obtain a supersingular abelian variety.

12.9. Theorem IIns / Example. (Failure of CMLNI.) (Chai) *Let p be a rational prime number such that $p \equiv 2,\ 3 \pmod 5$,* i.e. p is inert in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$. *Suppose $K/\mathbb{Q}$ is imaginary quadratic, such that p is split in $K/\mathbb{Q}$ with an element $\beta \in O_K$ such that $O_K{\cdot}\beta$ is one of the primes above p in O_K* (to ensure existence of β, assume for example K to be chosen in such a way that the class number of K is equal to 1). *Let L/K be an extension of degree 5 generated by $\pi := \sqrt[5]{p^2\beta}$. We see that π is a Weil p-number. Let A be any abelian variety over $\mathbb{F}_p$ in the isogeny class corresponding to this Weil number by the Honda-Tate theory, see* 1.2. *Note that* $\dim(A) = 5$*, the Newton polygon of A has slopes equal to* $2/5$ *respectively* $3/5$*, and* $\mathrm{End}^0(A)$ *is a field of degree* 10 *over $\mathbb{Q}$. The abelian variety $A/\mathbb{F}_p$ does not satisfy* (CMLN) *up to isogeny.*
A proof, taken from [11], will be suggested in Section 13.

Conclusion. A field extension is necessary. *In general, an abelian variety defined over a finite field does not satisfy* (CMLNI).

13. The residual reflex condition ensures (CMLNI)

13.1. The reflex field. See [69] Section 8 (the dual of a CM-type), [34], I.5. Let P be a CM-field, and let $\rho \in \mathrm{Aut}(P)$ be the involution on P which is complex conjugation under every complex embedding $P \hookrightarrow \mathbb{C}$.

Let (P, Φ) be a CM-type. The *reflex field* L' defined by (L, Φ) is the finite extension of $\mathbb{Q}$ generated by all traces:

$$L' := \mathbb{Q}(\sum_{\varphi\in\Phi} \varphi(x) \mid x \in L).$$

If $L/\mathbb{Q}$ is Galois we have $L' \subset L$. It is known that L' is a CM-field.

Suppose B is an abelian variety, simple over $\mathbb{C}$, with smCM by $P = \mathrm{End}^0(B)$. The representation of P on the tangent space of B defines a CM-type. It follows that any field of definition for B contains L'; see [69], 8.5, Prop. 30; see [34], 3.2 Th. 1.1. Conversely for every such CM-type and every field M containing L' there exists an abelian variety B over M having smCM by L with CM-type Φ.

13.2. Remark. Suppose P is a CM-field, and let Φ be a CM-type for P. Let w' be a discrete valuation of the reflex field P'; write $K_{w'}$ for its residue class field. Suppose B is an abelian variety defined over a number field M such that B/M admits smCM of type (P, Φ). In particular $[P : \mathbb{Q}] = 2\dim(B)$. Then $M \supset L'$; see 13.1 for references. Let v be a discrete valuation of M extending w'. Suppose B has good reduction at v. Let B_v/K_v be the reduction of B at v.

The residual reflex condition. Then K_v contains $K_{w'}$.

(A remark on notation. We use to write w for a discrete valuation of a CM-field, and v for a discrete valuation of a base field.)

13.3. Proof of 12.7. We see that $\mathrm{End}^0(A) = \mathbb{Q}(\zeta_5) = L$. Note that $L/\mathbb{Q}$ is Galois; hence $L' \subset L$; moreover $L'/\mathbb{Q}$ is a CM-field; hence $L' = L$; this equality can also be checked directly using the possible CM-types for $L = \mathbb{Q}(\zeta_5)$. Suppose there would exist up to isogeny over $K = \mathbb{F}_{p^2}$ a CM-lifting B/M to a field of characteristic zero. We see that the residue class field $K' = K_v$ of M contains the residue class field $K_{w'}$ of L'. As p is inert in $L = L'$ it follows that $K \supset K_{w'} = \mathbb{F}_{p^4}$. This contradicts the fact that A is defined over $\mathbb{F}_{p^2}$. $\square$12.7

A proof of 12.9 can be given along the same lines, by showing that $K_{w'} \supset \mathbb{F}_{p^2}$.

13.4. Given a CM-type (P, Φ) and a discrete valuation w' of the reflex field P' we obtain $K_{w'} \supset \mathbb{F}_p$. We see that in order that A_0/K with $K = \mathbb{F}_q$ does allow a lifting with CM-type (P, Φ) it is necessary that it satisfies the *residual reflex condition*: $K_{w'} \subset K$. Moreover note that the triple (P, Φ, w') determines the Newton polygon of B_v (notation as above): see [73], page 107, Th. 3, see 9.7. The triple (P, Φ, w') will be called a p-adic CM-type, where p is the residue characteristic of w'. The following theorem says that the *residual reflex condition is sufficient for ensuring* (NLCM) *up to isogeny.*

13.5. Theorem III. *Let A_0/K be an abelian variety of dimension g simple over a finite field $K \supset \mathbb{F}_p$. Let $L \subset \mathrm{End}^0(A_0)$ be a* CM *-field of degree $2{\cdot}g$ over $\mathbb{Q}$. Suppose there exists a p-adic* CM*-type (L, Φ, w') such that it gives the Newton polygon of A_0 and such that $K_{w'} \subset K$. Then A_0 satisfies* (CMNL) *up to isogeny.* We expect more details will appear in [11].

13.6. 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:

13.7. 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.
This was proved in [20]. See [55], Section 14, in particular 14.7.

13.8. Remark/Exercise * (Lubin and Tate). *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* $\mathrm{End}(E[p^\infty]) \supsetneqq \mathbb{Z}_p$. (We could say: E does not have CM, but $E[p^\infty]$ does have CM.) See [38], 3.5.

13.9. Remark. We have seen that the Tate conjecture holds for abelian varieties over a base field of finite type over the prime field; see 20.5. By the previous exercise we see that an analogue of the Tate conjecture for abelian varieties does not hold over a local field.

Grothendieck formulated his "anabelian conjecture" for hyperbolic curves; see [27], Section 3. Maybe his motivation was partly the Tate conjecture, partly the description of algebraic curves defined over $\overline{\mathbb{Q}}$ by Bielyi. Grothendieck stressed the fact that the base field should be a number field. This "anabelian" conjecture by Grothendieck generalizes the Neukirch-Uchida theorem for number fields to curves over number fields. Various forms of this conjecture for curves have been proved (Nakamura, Tamagawa, Moichizuki).

It came as a big surprise that this anabelian conjecture for curves actually is true over local fields, as Mochizuchi showed, see [41]. The ℓ-adic representation for abelian varieties is in an *abelian* group: H^1-ℓ-adic or $\pi_1(A)$. It turned out that for curves the representation in the *non-abelian group* $\pi_1(C)$ gives much more information. This is an essential tool in Mochizuki's result.

13.10. We keep notation as in 12.7: $\pi = p\zeta_5$ with $p \equiv 2, 3 \pmod 5$. Write $L = \mathbb{Q}(\zeta_5)$ where $\zeta = \zeta_5$ and write $\mathcal{O} = \mathcal{O}_L$ for the ring of integers of L. We choose A over $\mathbb{F}_p$ such that $\pi_A \sim \pi$ and $\mathcal{O}_L = \mathrm{End}(A)$, see 4.6. We consider

$$\rho_{0,F} : \mathcal{O} \longrightarrow \mathrm{End}(A[F]) = \mathrm{End}(\mathbb{D}(A[F])) = \mathrm{Mat}(2, \mathbb{F}_{p^2}),$$

and

$$\rho_{0,p} : \mathcal{O} \longrightarrow \mathrm{End}(A[p]) = \mathrm{End}(\mathbb{D}(A[p])) = \mathrm{Mat}(4, \mathbb{F}_{p^2}).$$

Let $u \in \mathbb{F}_{p^4}$ be a primitive 5-th root of unity.

Claim. (1) *The set of eigenvalues of $\rho_{0,F}(\zeta)$ is either $\{u, u^4\}$ or $\{u^2, u^3\}$.*
(2) *The set of eigenvalues of $\rho_{0,p}(\zeta)$ is $\{u, u^2, u^3, u^4\}$.*
(3) *The abelian variety A over $\mathbb{F}_{p^2}$ defined above does not admit* (CML). ADDED: this statement (3) is incorrect.
Proof. Clearly the eigenvalues considered are a power of u. As the trace of $\rho_{0,p}(\zeta)$ is in $\mathbb{F}_{p^2}$ this shows **(1)**.

Consider $\mathcal{O} \otimes_{\mathbb{Z}} W_\infty(\mathbb{F}_{p^2})$. This ring is isomorphic with a product $\Lambda_1 \times \Lambda_2$ according to the two irreducible factors $[(T-\zeta)(T-\zeta^4)]$ respectively $[(T-\zeta^2)(T-\zeta^3)]$ of $\mathrm{Irr}_{\mathbb{Q}}(\pi) = (T^5-1)/(T-1) \in W_\infty(\mathbb{F}_{p^2})[T]$. The action of $\Lambda_1 \times \Lambda_2$ on the additive group $\mathbb{D}(A[p]$ gives a splitting into $\mathbb{D}(A[F])$ and $\mathrm{Ker}(\mathbb{D}(A[p] \to \mathbb{D}(A[F])$. This proves **(2)**.

Suppose there would exist a CM-lifting of A. Then there would be a normal CM-lifting of $B_0 := A \otimes \mathbb{F}$. I.e. the would exist: a normal integral local domain R with residue class field $\mathbb{F}$ and field of fractions M, an abelian scheme $\mathcal{B} \to \mathrm{Spec}(R)$ such that $\mathcal{B} \otimes \mathbb{F} \cong B_0$, and such that $\Gamma := \mathrm{End}(\mathcal{B})$ is an order in $\mathcal{O}$; hence the field of fractions of Γ is L. Write $B = \mathcal{B} \otimes M$ for the generic fiber. Let $z \in W_\infty(\mathbb{F})$ be a primitive root 5-th of unity such that $z \bmod p = u$. Consider $T = \mathbf{t}_{\mathcal{B},0}$ the tangent bundle of $\mathcal{B} \to S := \mathrm{Spec}(R)$ along the zero section. We obtain an action $\Gamma \to \mathrm{End}(T/S)$. Note that $\mathcal{B} \to S$ admits smCM, hence

$\mathcal{B} \otimes \mathbb{C}$ has a CM-type. Hence on the generic fiber $T \otimes_R M$ the action of $\zeta \in L$ is either with eigenvalues $\{z, z^2\}$, or $\{z, z^3\}$ or $\{z^4, z^2\}$ or $\{z^4, z^3\}$. This action also can be computed as follows. Consider the p-divisible group $\mathcal{B}[p^\infty]$, with action $\rho : \Gamma \to \mathrm{End}(\mathcal{B}[p^\infty])$. The action on the generic fiber $\rho_\eta : \Gamma \to \mathrm{End}(B[p^\infty])$ extends to $\rho_\eta : L \to \mathrm{End}(B[p^\infty])$. Hence we see that the action of ζ on $T_\eta := T \otimes M$ has eigenvalues as given by the CM-type.

As Γ acts via $\rho : \Gamma \to \mathcal{B}$ we obtain an action

$$\rho_{p^\infty} : \Gamma \to \mathrm{End}(\mathcal{B}[p^\infty]).$$

The closed fiber

$$\rho_{0,p^\infty} : \Gamma \to \mathrm{End}(B_0[p^\infty])$$

of this action extends to the original $\mathcal{O} \to \mathrm{End}(B_0[p^\infty])$.

We conclude that on the one hand ζ acts on $B_0[F]$ by eigenvalues either $\{u, u^4\}$ or $\{u^2, u^3\}$, on the other hand by one of the four possibilities given by a CM-type. This is a contradiction (Incorrect). This (does NOT) prove **(3)**.

13.11. Does there exist for every prime number p an example with $f = 0$ and $g = 2$ of an abelian variety over a finite field which does not admit a CM-lifting?

13.12. (0) For an abelian variety A over a field M of characteristic *zero* with smCM an embedding $M \subset \mathbb{C}$ we obtain a CM-type. Of course, an isogeny does not change the CM-type. Is there an analogue in positive characteristic?

(p) In the example just discussed we see that in the isogeny class of $A \otimes \mathbb{F}$ the action of ζ on the tangent space of different members of the isogeny class can have different "types". An isogeny may change the "CM-type" in positive characteristic. In a more general situation than the one just considered it also not so clear what to expect for a reasonable definition of a "CM-type".

However in 9.2 we see a description of a notion which is intrinsic in the isogeny class of an abelian variety with smCM: not the action on the tangent space, but the action on the p-divisible group does split the p-divisible group into isogeny factors; this splitting is stable under isogenies.

We see the general strategy: in characteristic zero it often suffices to study the tangent space of an abelian variety, whereas in positive characteristic the whole p-divisible group is the right concept to study "infinitesimal properties".

The Shimura-Taniyama formula and the contents of this section are the study of these two aspects, and the way they fit together under reduction modulo p and under lifting to characteristic zero.

14. Elliptic curves

14.1. Reminder. Let E be an eliptic curve over a field $K \supset \mathbb{F}_p$. We say that E is *supersingular* if $E[p](k) = 0$, for an algebraically closed field $k \supset K$. In 21.20 and 21.21 we discuss the definition of an abelian variety being supersingular. We mention that any supersingular abelian variety has p-rank equal to zero; however the converse is not true: for any $g \geq 3$ there exist abelian varieties of p-rank equal to zero of that dimension which are not supersingular.

We say that an abelian variety A of dimension g over a field $K \supset \mathbb{F}_p$ is *ordinary* if its p-rank equals g, i.e. $A[p](k) \cong (\mathbb{Z}/p)^g$. Note that

an elliptic curve E is ordinary iff $E[p](k) \neq 0$, i.e. iff E is not supersingular.

14.2. Exercise. Let E be an elliptic curve over $K \supset \mathbb{F}_p$.
(1) *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* $\mathbb{F}_{p^2}$.
For the notion of "can be defined over K", see 15.1.
(4) (Warning)
Give an example of an elliptic curve E *over a field* $K \supset \mathbb{F}_p$ *with* $F_{E^{(p)}} \cdot F_{E^{(p)}} = p$ *and give an example with* $F_{E^{(p)}} \cdot F_{E^{(p)}} \neq p$.

14.3. 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 [71] page 52, we see that for $j \in K$ an elliptic curve over K with that j invariant exists:

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

$$Y^2 + XY = X^3 - \frac{36}{j - 1728}X - \frac{1}{j - 1728}.$$

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 $\{p, \infty\}$ and ramified at p and at ∞. This was an inspiration 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.

14.4. Endomorphism algebras of elliptic 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) $\boxed{E \textit{ is ordinary; } e = 2, \quad d = 1 \textit{ and } \mathrm{End}^0(E) = L = \mathbb{Q}(\pi_E)}$ *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 $K \subset K'$ we have $\mathrm{End}(E) = \mathrm{End}(E \otimes K')$.*

(2) (1.2) $\boxed{E \textit{ is supersingular, } e = 1, \quad d = 2 \textit{ and } \mathrm{End}^0(E) \cong \mathbb{Q}_{p,\infty}.}$
This is the case if and only if $\pi_E \in \mathbb{Q}$. For every field extension $K \subset K'$ we have $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes K')$.

(3) (2.1.ns) $\boxed{E \textit{ is supersingular, } e = 2, \quad d = 1 \textit{ and } \mathrm{End}^0(E) = L \supsetneqq \mathbb{Q}.}$
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 $\mathrm{End}^0(E \otimes K') \cong \mathbb{Q}_{p,\infty}$ for any field K' 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 14.6. Here we indicate a proof independent of that classification of all elliptic curves over a finite field, but using 5.4 and 1.2.

Proof. By 5.4 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), note that $\dim(E) = 1$, or $\pi_E \notin \mathbb{R}$ and $D = L := \mathbb{Q}(\pi_E) = \mathbb{Q}$ and $L/\mathbb{Q}$ is an imaginary quadratic field.

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

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

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, see 18.1. 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 20.7, see [77], 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

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

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 contradiction 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. $\square$

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). $\square$

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

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

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 [28], second printing, §20, absolute values suitably normalized) shows that ζ is also a unit at v. By 10.3 we conclude that ζ is a root of unity. This proves Claim (Three). $\square$

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

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

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 $K \subset \mathbb{F}_{q^N} \subset K'$ we have

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

$\square$14.4

14.5. 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 $L = \mathrm{End}^0(A)$. Note that $E/\mathbb{Q}$ is an imaginary quadratic extension. Suppose A has good reduction A_0 modulo the prime above 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.)

14.6. Classification of isogeny classes of all elliptic curves over finite fields. See [75], 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

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

The Newton polygon of E equals the Newton polygon of U with the vertical axis compressed by n, see 9.3. Hence:

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

and

$$(v_p(\beta) > 0) \;\Leftrightarrow\; (E \text{ is supersingular}) \Leftrightarrow\; (v_p(\beta) \geq n/2) \;\Leftrightarrow (q \text{ divides } \beta^2);$$

$$(E \text{ is supersingular}) \iff \beta^2 \in \{0, q, 2q, 3q, 4q\}.$$

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 1.2 *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 $q = p^{2j+1}$.
For supersingular E we have that q divides β^2. As moreover $0 \leq \beta^2 \leq 4q$ we conclude

$$\beta^2 \in \{0, q, 2q, 3q, 4q\}.$$

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

In all cases below (E is *supersingular* and) $\pi_E \notin \mathbb{Q}$; hence

$$\mathbb{Q} \subsetneqq L = D \not\cong \mathbb{Q}_{p,\infty} \quad \text{and} \quad L \subsetneqq \mathrm{End}(E \otimes \overline{\mathbb{F}}) \cong \mathbb{Q}_{p,\infty}.$$

(3) $\beta^2 = 3q$ $\boxed{p = 3, \quad \beta = \pm 3^{j+1}}$, $\quad q = 3^{2j+1}$.
Here $p = 3$, $\quad n = 2j + 1$ is odd, and
$\pi \sim \zeta_3\sqrt{-q}$ or $\pi \sim \zeta_6\sqrt{-q}$: $\quad \pi \sim \zeta_{12}\sqrt{q}$, $\quad L = \mathbb{Q}(\sqrt{-3})$.

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

(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, then $\pi_E \sim \zeta_r\sqrt{q}$ 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) then p divides β and E is supersingular and $\beta^2 \in \{0, q, 2q, 3q, 4q\}$.

If $\beta^2 = 4q$, we are in Case (2); this is clear; also see 15.9.

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).

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 isogeny classes of elliptic curves over a finite field as given in [75], pp. 536/7. $\square$14.6

15. Some examples and exercises

15.1. 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 $B_0 \otimes_{K_0} K' \cong A \otimes_K K'$. – The following exercise shows that this *does not imply in general that we can choose B_0 over K_0 such that $B_0 \otimes_{K_0} K \cong A$.*

15.2. Exercise. Let p be a prime number, $p \equiv 3 \pmod 4$. Let $\pi := p{\cdot}\sqrt{-1}$.
(1) *Show that* π *is a* p^2*-Weil number.* Let A be an abelian variety simple over $K := \mathbb{F}_{p^2}$ 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* $K_0 := \mathbb{F}_p$ *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.

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

15.4. 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 $T^2 - \sqrt{2}{\cdot}T + 8$,

15.5. Exercise. Consider the following examples.
(1) Let $\beta := \sqrt{2+\sqrt{3}}$, and $q = p^n$. Let π be a zero of

$$T^2 - \beta T + q.$$

(2) Choose coprime positive integers $d > c > 0$, and choose p. Let π be a zero of

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

See Section 11, in particular 11.5.
(3) Choose $q = p^n$ and $i \in \mathbb{Z}_{>0}$. Let $\pi := \zeta_i{\cdot}\sqrt{q}$, where ζ_i is a primitive $i-$th root of unity.

(a) *Show that every of these numbers* π *indeed is a Weil* q*-number.*
For each of these let A_π be an abelian variety simple over $\mathbb{F}_q$ having this number as geometric Frobenius endomorphism.
(b) *Determine* $\dim(A_\pi)$ *and its Newton poygon* $\mathcal{N}(A_\pi)$.
(c) *For every possible choice of* π *determine the smallest* $N \in \mathbb{Z}_{>0}$ *such that for every* $t > 0$ *we have*

$$\mathrm{End}^0(A_\pi \otimes \mathbb{F}_{q^N}) = \mathrm{End}^0(A_\pi \otimes \mathbb{F}_{q^{Nt}}).$$

You might want to use 5.10.

15.6. Exercise. **(1)** *Let* E *be an elliptic curve over* $\mathbb{F}_p$. *Show that* $\mathrm{End}^0(E)$ *is a field.*
(2) *Give an example of an abelian variety simple over* $\mathbb{F}_p$ *such that* $\mathrm{End}(A)$ *is non-commutative.*
(3) *Let* E *be an elliptic curve over* $\mathbb{Q}$. *Show that* $\mathrm{End}(E) = \mathbb{Z}$.
(4) *Show there exists an abelian variety* A *simple over* $\mathbb{Q}$ *such that* $\mathbb{Z} \neq \mathrm{End}(A)$. Compare 18.10.

15.7. Remark/Exercise. Suppose A is an abelian variety over a field K which admits smCM. Let $D = \mathrm{End}^0(A)$ and let $L' \subset D$ be a subfield of degree $[L' : \mathbb{Q}] = 2g = 2{\cdot}\dim(A)$. In this case L' not be a CM field.
Construct A, K, L', where A is an abelian variety over K, a finite field, such that $D = \mathrm{End}^0(A)$ is of Type IV(1,g), i.e. A admits smCM, and D is a division algebra central over degree g^2 over an imaginary quadratic field $L = \mathbb{Q}(\pi_A)$, and $L \subset L' \subset D$ is a field which splits D/L such that L' is not a CM-field.

15.8. Exercise. Consider the number π constructed in 12.7, respectively 12.9. Prove it is a Weil number and determine $\mathcal{D}(\pi)$, and $g(\pi)$ and the Newton polygon of the isogeny class thus constructed. For notation see 5.5.

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

$$[L : \mathbb{Q}] =: e, \quad [D : L] =: d^2, \quad 2g := e{\cdot}d. \qquad \text{See Section 18, see 5.5.}$$

For the different types of Albert algebras see 18.2. As we have seen in Proposition 2.2 there are three possibilities in case we work over a finite field:

($\mathbb{R}$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 hence $\sqrt{q} \notin \mathbb{Q}$.*

$$\boxed{\text{Type III(2)}, \quad g = 2}$$

In this case $L_0 = L = \mathbb{Q}(\sqrt{p})$, a real quadratic field. We see that D ramifies exactly at the two infinite places with 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 $\psi(\pi) \notin \mathbb{R}$.*

$$\boxed{\mathrm{IV}(e_0, d), \quad g := e_0{\cdot}d}$$

In this case all conjugates of $\psi(\pi)$ are non-real. We can determine $[D : L]$ knowing all $v(\pi)$ by 5.4 (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 $\mathrm{IV}(e_0, d)$. For $K = \mathbb{F}_q \subset K' = \mathbb{F}_{q^m}$ we have

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

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

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

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* $\mathrm{End}(A_K)/\mathrm{End}(\mathcal{A})$ *does have torsion.*

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

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

15.11. 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 [75], page 538:

15.11.1 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 $\overline{k}$..." See [75], page 538.

15.11.2 Exercise/Example. *Classify all isogeny classes of elliptic curves, and their endomorphism algebras for every p, for every $q = p^n$.* See 14.6.

15.11.3 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.

15.11.4 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.*

15.12. 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 *simple over* $\mathbb{F}_3$ *such that* $\pi_A = \pi$.

15.13. 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

$$g := T^2 - \beta T + p^4 \in L_0[T].$$

(a) *Show that the discriminant of* g *is totally 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:

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

15.15. Exercise. Let $b \in \mathbb{Z}$ and p and $q = p^n$ satisfy $b^2 < 4q^3$ such that 3 divides b but 3^2 does not divide b. Let β be a zero of $f := X^3 - 3qX - b$. Let ρ be a zero of $Y^2 - bY + q^3$. Let π be a zero of $T^2 - \beta T + q$. Let N be the Galois closure of $\mathbb{Q}(\pi)/Q$. Show:
(a) $f \in \mathbb{Z}[X]$ is irreducible; β is totally real; write $L_0 = \mathbb{Q}(\beta)$;
(b) π is a Weil q-number; ρ is a Weil q^3-number;
(c) $\pi^3 \sim \rho$; there exists an inclusion $\mathbb{Q}(\rho) \subset \mathbb{Q}(\pi) =: L$;
(e) there exists an element $1 \neq z \in N$ with $z^3 = 1$; such an element is not contained in $\mathbb{Q}(\pi)$;
(f) for $w' \in \Sigma_{L_0}^{(p)}$ compute $w'(\beta)$.
(g) Let A be a K-simple abelian variety with $\pi_A = \pi$. Show how to compute $\dim(A)$ once b and q are given. Is A absolutely simple?

15.16. Exercise. Formulate and solve an exercise analogous to the previous one with $f = X^5 - 5qT^3 + 5q^2T - b$.

15.17. Exercise. Let $N \in \mathbb{Z}_{\geq 2}$ be a prime number. Let π be a Weil q-number, and $L = \mathbb{Q}(\pi)$. Suppose $L' := \mathbb{Q}(\pi^N) \subsetneqq L = \mathbb{Q}(\pi)$. Show:
(a) If ζ_N is not conjugated to an element in L then $[L : L'] = N$.
(b) If ζ_N is conjugated to an element in L then $[L : L']$ divides $N - 1$.

15.18. 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.* See 22.1(4).

15.19. 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 Weil p-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.

15.20. Exercise. (See Section 9.) 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*

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

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

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

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

15.21. 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: [33], Th. 3.1 in 8.3 on page 194.

16. Appendix 1: Abelian varieties

Basic references: [47], [15], [GM].

For the notion of abelian variety over a field, abelian scheme over a base scheme, isogenies, and much more we refer to the literature. But let us at least give one definition.

16.1. Definition. Let S be a scheme. We say that $G \to S$ is a *group scheme* over S if $\mathrm{Mor}_S(-, G)$ represents a group functor on the category of schemes over S.
A group scheme $A \to S$ is an *abelian scheme* if A/S is smooth and proper with geometrically irreducible fibers. If $S = \mathrm{Spec}(K)$, an abelian scheme over S is called an *abelian variety* defined over K.

From these properties it follows that A/S is a commutative group scheme. However the name does not come from this, but from the fact that certain integrals of differential forms on a Riemann surface where studied by Niels Henrik Abel, and that the values of such integral are in an algebraizable complex torus; hence these objects were called abelian varieties.

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 $K' \supsetneq K$ 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.

An abelian variety A over a field K, as defined above, is a "complete group variety defined over K" (in pre-Grothendieck terminology). In particular $A \otimes \overline{K}$ is an integral algebraic scheme.

Exercise. *Show that $G \to S$ is a group scheme over S iff there exist morphisms $S \to G$, and $m : G \times G \to A$ and $i : G \to G$ satisfying certain properties encoded in commutative diagrams as given by the group axioms.*

16.2. For an abelian variety over a field K the *dual abelian variety* $A^t = \underline{\mathrm{Pic}}^0_A$ exists. This is an abelian variety of the same dimension as A.

For the definition of a polarization see [47]; [45], 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. For an abelian variety A over a field K an isogeny $\varphi : A \to A^t$ is called a *polarization* if over some over-field of K this homomorphism can be defined by an ample divisor. We say we have a *principal polarization* if $\varphi : A \to A^t$ is an isomorphism.

As every abelian variety admits a polarization we see that A and A^t are isogenous.

16.3. The Rosati involution. Let A be an abelian variety over a field K We write $D = \mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, called the *endomorphism algebra* of A. Let $\varphi : A \to A^t$ be a polarization. We define $\dagger : D \to D$ by $\dagger(x) := \varphi^{-1} \cdot x^t \cdot \varphi$; for the existence of φ^{-1} in D, see 6.1.This map is an *anti-involution* on the algebra D, called the Rosati-involution. If φ is a principal polarization, we have $\dagger : \mathrm{End}(A) \to \mathrm{End}(A)$. See [47], pp.189 - 193. See [15], Chap. V, §17; note however that the subset of $\mathrm{End}^0(A)$ fixed by the Rosati involution need not be a subalgebra.

16.4. 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.*

16.5. 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 this is a finite group scheme over S. See [49], I.2.

Equivalent definition. Let $N \to S$ be as above. Consider the functor $T \mapsto \mathrm{Hom}_T(N_T, \mathbb{G}_{m,T})$. By the Cartier-Shatz formula this functor is representable by $\mathrm{Hom}(-, N^D)$, see [49], Theorem 16.1. Conversely this can be used as defintion of Cartier duality $N \mapsto N^D$.

16.6. 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*

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

gives rise to an exact sequence

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

$\square$

See [49]. Theorem 19.1. For the definition of N^D, see 16.5.

16.7. Corollary. *Let S be a locally noetherian base scheme and let $A \to S$ be an abelian scheme. There is a natural isomorphism $A^t[p^\infty] = A[p^\infty]^t$.* $\square$

16.8. 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 defining property that for any $t \in \mathbb{Z}$ we have $f_{A,\varphi}(\varphi - t) = \deg(\varphi - t)$; see [15] page 125.

See 20.1 for the definition of $T_\ell(A)$; for every $\ell \neq \mathrm{char}(K)$ the polynomial $f_{A,\varphi}$ equals the characteristic polynomial of $T_\ell(\varphi) \in \mathrm{End}(T_\ell(A)(\overline{K})) \cong M_{2g}(\mathbb{Z}_\ell)$. This can be used to give a definition of $f_{A,\varphi}$.

If $\varphi \in \mathrm{End}(A)$ and $\psi \in \mathrm{End}(B)$ then $f_{A\times B,(\varphi,\psi)} = f_{A,\varphi} \times f_{B,\psi}$.
If $A = B^\mu$ and B is simple over a finite field, then $f_{A,\pi_A} = (f_{B,\pi_B})^\mu$.

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

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

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 $\mathbb{Z} \subsetneqq \mathrm{End}(A)$. See 15.6.

16.10. 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* $\mathrm{End}(A){\cdot}p$.

We say an abelian variety $A \neq 0$ over a field K is *simple*, or K-simple if confusion might occur, if for any abelian subvariety $B \subset A$ we have either $0 = B$ or $B = A$.

16.11. Theorem (Poincaré-Weil). *For any abelian variety $A \neq 0$ over a field K there exist simple abelian varieties B_i over K and an isogeny $A \sim_K \Pi_i \; B_i$.*
See [47], Th. 1 on page 173 for abelian varieties over an algebraically closed field. See [GM] for the general case. $\square$

17. Appendix 2: Central simple algebras

Basic references: [7], [61], [8] Chapter 7, [65] Chapter 10. We will not give a full treatment of this theory here.

17.1. 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 $\mathrm{Mat}(r, D)$ 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 $R \cong \mathrm{Mat}(r, D)$ 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.

17.2. Exercise. Let $A \neq 0$ be an abelian variety over a field K. (Suggestion, see 16.11, and see 15.9.)
(1) *Show that* $\mathrm{End}^0(A)$ *is a semisimple ring.*
(2) *Prove: if A is simple, then* $\mathrm{End}^0(A)$ *is a division algebra.*
(3) *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.*

17.3. 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.

Suppose a field L is given. Let D and D' be central simple algebras over L. We say that D and D' are similar, notation $D \sim D'$ if there exist $m, m' \in \mathbb{Z}_{\geq 0}$ and an isomorphism $D \otimes_L \mathrm{Mat}(m, L) \cong D' \otimes_L \mathrm{Mat}(m', L)$. The set of 'similarity classes" of central simple algebras over L will be denoted by $\mathrm{Br}(L)$. On this set we define a "multiplication" by $[D_1]{\cdot}[D_2] := [D_1 \otimes_L D_2]$; this is well defined, and there is an "inverse" $[D] \mapsto [D^{\mathrm{opp}}]$, where D^{opp} is the opposite algebra. As every central simple algebra is a matrix algebra over a central division algebra over L (Wedderburn's Theorem) one can show that under the operations given $\mathrm{Br}(L)$ is a group, called the *Brauer group* of L. See the literature cited for definitions, and properties.

17.4. 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*

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

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.

(4) *Let $L \subset D$ be simple central division algebra; by* (3) *we know it is given by a set of invariants* $\{\mathrm{inv}_w(D) \mid w \in \Sigma_L\}$, *with* $\mathrm{inv}_w(D) \in \mathbb{Q}/\mathbb{Z}$. *Let r be the least common multiple of the denominators of these rational numbers written as a a quotient with coprime nominator and denominator. Then $[D : L] = r^2$.*

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 really need Brauer theory.

17.1.

Example. For a (rational) prime number p we consider the invariant $1/2$ at the prime p in $\mathbb{Z}$, i.e. $p \in \Sigma_{\mathbb{Q}}$ and the invariant $1/2$ at the infinite prime of $\mathbb{Q}$. As these invariants add up to zero in $\mathbb{Q}/\mathbb{Z}$ there is a division algebra central over $\mathbb{Q}$ given by these invariants. This is a quaternion algebra, split at all finite places unequal to p. In [20] this algebra is denoted by $\mathbb{Q}_{p,\infty}$. By 5.4 we see that a supersingular elliptic curve E over $\mathbb{F}$ has endomorphism algebra $\mathrm{End}^0(E) \cong \mathbb{Q}_{p,\infty}$

18. Appendix 3: Endomorphism algebras.

Basic references: [68], [47], [35] Chapt. 5, [54].
We will see: *endomorphism algebras* of abelian varieties 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.

18.1. Proposition (Weil). *Let A, B be abelian varieties over a field K. The group* $\mathrm{Hom}(A, B)$ *is free abelian of finite rank. In fact,*

(1) $\mathrm{rank}\,(\mathrm{Hom}(A, B)) \leq 4{\cdot}g_A{\cdot}g_B$;

(2) *if the characteristic of K equals zero,* $\mathrm{rank}\,(\mathrm{Hom}(A, B)) \leq 2{\cdot}g_A{\cdot}g_B$.

Let ℓ be a prime different from the characteristic of K. Let $T_\ell(A)$, respectively $T_\ell(B)$ be the Tate-ℓ-groups as defined in 20.1.
(3) *The natural homomorphisms*

$$\mathrm{Hom}(A,B) \hookrightarrow \mathrm{Hom}(A,B)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}(T_\ell(A),T_\ell(B))$$

are injective.
See [47], Th. 3 on page 176. □

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].

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

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

Type III(e_0) Here $d = 2$, $e = e_0$, $\mathrm{inv}_w(D) \neq 0$ for all infinite w, 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 $[D : L] = d^2$.

18.3. Theorem. *Let A be an abelian variety over a field K. Then* $\mathrm{End}^0(A)$ *is an Albert algebra.* □
See[47], Theorem 2 on page 201.

18.4. As Albert, Shimura and Gerritzen proved: for any prime field $\mathbb{P}$, and every Albert algebra D there exists an algebraically closed field $k \supset \mathbb{P}$ and an abelian variety A over k such that $\mathrm{End}^0(A) \cong D$; see [54], Section 3 for a discussion and references. In case $\mathbb{P} = \mathbb{F}_p$ in all these cases one can choose for A an ordinary abelian variety.

In particular Gerritzen proves the following more precise result. For an Albert algebra D define $t_0(D) \in \{1, 2\}$ by:

$t_0(D) = 1$ if D is of type I, or II, or IV$(e_0, d > 1)$ (D is generated by the $\dagger$-invariants),

$t_0(D) = 2$ if D is of type III, or IV$(e_0, d = 1)$ (D is not generated by the $\dagger$-invariants).

18.5. Theorem (Gerritzen). *For a given prime field $\mathbb{P}$, and a given Albert algebra D, choose any integer $t \geq t_0(D) = 1$, and define $g := t{\cdot}[D : \mathbb{Q}]$; there exists an algebraically closed field k containing $\mathbb{P}$ and an abelian variety A over k such that* $\mathrm{End}^0(A) \cong D$.
See [24], Th. 12. See [54], Th. 3.3.

18.6. 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:

18.7. 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 $\mathbb{C}$.

18.8. Exercise. Show that 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 $[\mathcal{O}_E : \mathrm{End}(A)] > m$.

18.9. Remark. For a simple *ordinary* abelian variety A over a finite field the orders in $\mathrm{End}^0(A)$ containing π_A and ν_A are precisely all possible orders appearing as endomorphism ring in the isogeny class of A, see [75], Th. 7.4.

However this may fail for a non-ordinary abelian variety, see [75], page 555/556, where an example is given of an order containing π_A and ν_A, but which does not appear as the endomorphism ring of any abelian variety.

We see difficulties in determining which orders in $\mathrm{End}^0(A)$ can appear 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 [75].

18.10. 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, simple 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.)

18.11. 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 [75], Theorem 7.2 we read that for simple and ordinary abelian varieties "$\mathrm{End}(A)$ is commutative and unchanged by base change". Some care has to be take in understanding this. The conclusion of the preceding exercise is not correct without te condition "$A \otimes K'$ is simple".

18.12. 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.

18.13. 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* (hence a field); see [36]. For constructions of other endomorphism algebras of an abelian variety over $\mathbb{F}$ see [9], Th. 5.4.

18.14. 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 [75], 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.*

18.15. For abelian varieties over a *finite field* separable isogenies give an equivalence relation, see [75], 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.*

18.16. 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 an embedding which may be an equality, but also inequality does appear; examples are easy to give, see 16.9, 15.19.

18.17. 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 [54], (3.13).

18.18. 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 15.

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.

18.19. Theorem (H. W. 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 $m = \overline{\mathbb{F}_p}$ 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 [36].

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

For more general constructions of endomorphism algebra with given invariants of an abelian variety over a finite field, see [9], Section 5.

19. Appendix 4: Complex tori with smCM

See [69], [47], [35], [60].

19.1. Let A be an abelian variety over $\mathbb{C}$. Write $T := A(\mathbb{C})$. This is a *complex torus*, i.e. a complex Lie group obtained as quotient $\mathbb{C}^g/\Lambda$, where $\mathbb{Z}^{2g} \cong \Lambda \subset \mathbb{C}^g \cong \mathbb{R}^{2g}$ is a discrete subgroup. Indeed, we have an exact sequence

$$0 \quad \to \mathbb{Z}^{2g} \cong \quad \Lambda \quad \longrightarrow \quad V \cong \mathbb{C}^g \quad \xrightarrow{e} \quad T = A(\mathbb{C}) \quad \to \quad 0.$$

There there are at least two different interpretations of the homomorphism e.

One can take the tangent space $V := \mathbf{t}_{A,0}$. This is also the tangent space of the complex Lie groep T. The *exponential map* of commutatieve complex Lie groups gives $e : V \to T$.

One can also consider the topological space T, and construct its *universal covering space* $V := \tilde{T}$. This is a complex Lie group (in a unique way) such that the covering map e is a homomorphism. The kernel is the fundamental group $\pi_1(T, 0) = \Lambda \cong \mathbb{Z}^{2g}$.

19.2. The complex torus $T := A(\mathbb{C})$ is algebraizable, i.e. comes from an algebraic variety. If this is the case, the structure of algebraic variety, and the structure of algebraic group giving the complex torus is unique up to isomorphism (note that a complex torus is compact); see [66], corollaire on page 30.

In general a complex torus of dimension at least two need not be algebraizable as is show by the following two examples.

19.3. Example. Choose any abelian variety A over $\mathbb{C}$ of dimension $g > 1$. There exists an analytic family $\mathcal{T} \to \mathcal{M}$, where $\mathcal{M}$ is a unit cube of dimension g^2, such that over that infinitesimal thickening of the origin the restriction of $\mathcal{T} \to \mathcal{M}$ is the formal deformation space $\mathrm{Def}(A)$. Every polarization μ on A gives a regular formal subscheme $S_\mu \subset \mathrm{Def}(A)$ of dimension $g(g+1)/2$. Let $C \to \mathcal{M}$ be a one dimensional regular analytic curve inside $\mathcal{M}$ whose tangent space is not contained in the tangent spaces to S_μ for any μ; such a curve exists because the set of polarizations on A is countable and because $g(g+1)/2 < g^2$ for $g > 1$. One shows that there exists a point $s \in C$ such that $\mathcal{T}_s$ is not algebraizable.

19.4. Example (Zarhin - FO). Choose a division algebra of finite degree over $\mathbb{Q}$ *which is not an Albert algebra.* For example take a field which is not totally real, and which is not a CM-field; e.g. $D = \mathbb{Q}(\sqrt[3]{2})$. By [60], Corollary 2.3 we know there exists a complex torus T with $\mathrm{End}^0(T) \cong D$. If this torus would be algebraizable, $A(\mathbb{C}) \cong T$, then this would imply $\mathrm{End}^0(A) \cong D$ by GAGA, see [66], Proposition 15 on page 29. By Albert's classification this is not possible, see 18.3.

19.5. Let A be an abelian variety over $\mathbb{C}$. Suppose it is simple. Suppose it admits smCM. In that case $\mathrm{End}^0(A) = P$ is a field of degree $2g$ over $\mathbb{Q}$. Moreover P is a CM-field. We obtain a representation $\rho_0 : P \to \mathrm{End}(\mathbf{t}_{A,0}) \cong \mathrm{GL}(g, \mathbb{C})$. As P is commutative and $\mathbb{C}$ is algebraically closed this representation splits a a direct sum of 1-dimensional representations. Each of these is canonically equivalent to giving a homomorphism $P \to \mathbb{C}$. One shows that these g homomorphisms are mutually different, and that no two are complex conjugated. Conclusion: ρ_0 is a CM-type, call it Φ; conversely a CM-type gives such a representation P operating via a diagonal matrix given by the elements of Φ. This process $(A/\mathbb{C}, P) \mapsto (P, \Phi)$ can be reversed, and the construction gives complex tori which are algebraizable.

19.6. Theorem. *Let* (P, Φ) *be a* CM-type. *There exists an abelian variety* A *over* $\mathbb{C}$ *with* $P \cong \mathrm{End}^0(A)$ *such that the representation* ρ_0 *of* P *on the tangent space* $\mathbf{t}_{A,0}$ *is given by the* CM-type Φ. □

See [69], §6. There are many more references possible.

20. Appendix 5: Tate-ℓ and Tate-p conjectures for abelian varieties

Most important reference: [72]. Also see [22], [83].

20.1. 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

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

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

20.2. Let G be a finite flat 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 étale; [50].

20.3. 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 étale 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 étale finite group schemes over K and the category of finite continuous G-modules.*

See [76], 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 étale 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 étale 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.

20.4. 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; see 18.1.

20.5. 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 [72]. The case of function field in characteristic p was proved by Zarhin and by Mori, see [81], [82], [43]; also see [42], 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 [21]. For the case of a function field in characteristic zero, see [22], Th. 1 on page 204.

20.6. We like to have a p-adic analogue of 20.5. 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

$$A[p^\infty] = \mathrm{colim}_{i\to}\ A[p^i],$$

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.

20.7. Exercise. Let A and B be abelian varieties over a field K. In 18.1 we have seen that $\mathrm{Hom}(A, B)$ is of finite rank as $\mathbb{Z}$-module. Let p be a prime number. Using 18.1, show that the natural map

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

is *injective*. Also see [77], theorem 5 on page 56. Also see [83].

20.8. Remark. On could feel the objects $T_\ell(A)$ and $A[p^\infty]$ as *arithmetic objects* in the following sense. If A and B are abelian varieties over a field K which are isomorphic over $\overline{K}$, then they are isomorphic over a finite extension of K; these are geometric objects. Suppose X and Y are p-divisible groups over a field K which are isomorphic over $\overline{K}$ then they need not be isomorphic over any finite extension of K, these are arithmetic objects. The same statement for pro-ℓ-group schemes.

20.9. 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 [77]. The case of a function field over a finite field was proved by Johan de Jong, see [30], Th. 2.6. This case follows from the result by Tate and from the following result on extending homomorphisms 20.10.

20.10. 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 [30], 1.2 and [31], Th. 2 on page 261. $\square$

21. Appendix 6: Some properties in characteristic p

See [39]. For information on group schemes see [49], [62], [76], [10].

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.

21.1. A finite group scheme in characteristic zero, of more generally a finite group scheme of rank prime to all residue characteristics, is étale over the base; e.g. see [50]. However if the rank of a finite group scheme is not invertible on the base, it need not be étale.

21.2. 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 [62], 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 $F_{T/S} = \mathrm{fr} : T \to T$.

21.3. Verschiebung. Let A be a *commutative* group scheme flat over a characteristic p base scheme. In [62], Exp. VII_A.4 we find the definition of the "relative Verschiebung"

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

In case A is an abelian variety we see that F_A is surjective, and $\mathrm{Ker}(F_A) \subset A[p]$. In this case we do not need the somewhat tricky construction of [62], Exp. VII_A.4, but we can define V_A by $V_A{\cdot}F_A = [p]_A$ and check that $F_A{\cdot}V_A = [p]_{A^{(p)}}$.

21.4. 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 following 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 Frobenius morphism 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 structure 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 $t \in \mathbb{Z}_{\geq 1}$. Here $F_G = 0$ and V_G is an isomorphism. Note that the algebras defining $\alpha_{p,\mathbb{F}_p}$ and $\mu_{p,\mathbb{F}_p}$ are isomorphic, but the comultiplications are different.

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 [49].

Commutative group scheme of p-power rank over a perfect base field can be classified with the help of Dieudonné modules, not dicussed here, but see [39], see [19].

21.5. The p-rank. For an 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 $f(A) = \dim(A) =: g$.

21.6. For a classification of isomorphism classes of ordinary abelian varieties over finite fields (using Serre-Tate canonical lifts, and classical theory) see the wonderful paper [17]. This is a much finer classification than the Honda-Tate theory which studies isogeny classes.

21.7. The a-number. Let G be a group scheme over a field K of characteristic p. We write

$$a(G) = \dim_k(\mathrm{Hom}(\alpha_p, G \otimes k)),$$

where k is an algebraically closed field containing K. For a further discussion, see [10], 5.4 - 5.8

21.8. Examples. If E is an elliptic curve in characteristic p then:

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

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.

21.9. 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 étale,*
(4) *the rank of the group* $\mathrm{Hom}(\mu_p, A \otimes \overline{K})$ *equals p^g.*
(5) $\mathrm{Hom}(\mu_p, A \otimes \overline{K}) \cong (\mathbb{Z}/p)^g$.

21.10. 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, see 16.5.

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 [49], Theorem 19.1, we arrive at:

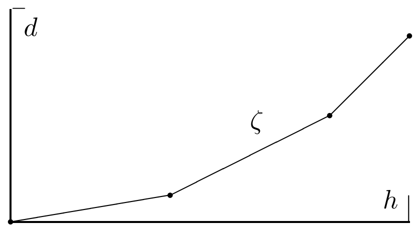
For an abelian scheme $A \to S$ over a base $S \to \mathrm{Spec}(\mathbb{F}_p)$ we have

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

21.11. 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)

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

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

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

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

$$\sigma_j = \gamma_j, \quad v_p(\sigma_j) \geq \beta_h + \cdots + \beta_{h-j+1}, \quad \beta_1 = v_p(\gamma_h).$$

21.12. *A p-divisible group X over a field of characteristic p determines uniquely a Newton polygon.* The general definition can be found in [39]. The isogeny class of a p-divisible group over and algebraically closed field k uniquely determines (and is uniquely determined by) its Newton polygon. We use "the Newton polygon of Frobenius", a notion to be explained below.

21.13. Theorem (Dieudonné and Manin), see [39], "Classification theorem " on page 35 .

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

21.14. 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 $\mathcal{N}(A[p^\infty])$.

21.15. Exercise. Show that for an abelian variety A over the prime field $\mathbb{F}_p$ this construction is valid, and does give the Newton polygon of A as defined in Section 9.

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

21.16. 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 $G_{d,c}$. This is a p-divisible group of dimension d and of height $d+c$. 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 [39]; the definition of $G_{d,c}$ is on page 35 of [39]. 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 $G_{d,c} \otimes_{\mathbb{F}_p} K$. Moreover the p-divisible groups $G_{d,c}$ and $G_{c,d}$ over $\mathbb{F}_p$ satisfy $(G_{d,c})^t \cong (G_{c,d})$; here X^t denotes te Serre dual of X, see 8.3.
Remark. With this defintion we have $G_{d,c}[F^{d+c}] = G_{d,c}[p^d]$ and $G_{d,c}[V^{d+c}] = G_{d,c}[p^c]$

21.17. Exercise. Assume the existence of $X = G_{d,c}$ over $\mathbb{F}_p$ as explained above. Let ζ be the Newton polygon of the Frobenius endomorphism of X. Show that ζ consists of $d+c$ slopes equal to $d/(d+c)$: this polygon is isoclinic (it is a straight line) and it ends at $(d+c, d)$.

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

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

21.18. In [39], 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 [39], Classification Theorem on page 35.

21.19. Definition of the Newton polygon of a p-divisible group. The isogeny class of $\prod_i G_{d_i,c_i}$ 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 $\mathbb{Q} \times \mathbb{Q}$.

For an abelian variety over a field of characteristic p we define $\mathcal{N}(A) := \mathcal{N}(A[p^\infty])$.

Note that for a p-divisible group X over K its Newton polygon only depends on $\mathcal{N}(X \otimes k)$, this only depends on the isogeny factors of $X \otimes k$, and we can choose these isogeny factors in such a way that they are defined over $\mathbb{F}_p$.

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 $c/(d+c)$.

21.20. Definition. An abelian variety A over a field $K \supset \mathbb{F}_p$ is called *supersingular* if $\mathcal{N}(A)$ is isoclinic with all slopes equal to $1/2$.
Equivalently. An abelian variety A over a field $K \supset \mathbb{F}_p$ is *supersingular* if there exists an isogeny $(A \otimes k)[p^\infty] \sim (G_{1,1})^g$.
Exercise. Show that for an elliptic curve this definition and the one given in 21.8 coincide.

Theorem (Tate, Shioda, Deligne, FO). *An abelian variety A is supersingular iff there exists a supersingular elliptic curve E and an isogeny $A \otimes k \sim E^g \otimes k$.*
See [72], Th. 2 on page 140, see [70], [52], Section 4.

21.21. Definition/Remark/Exercise. (1) Note that the definition of A being supersingular can be given knowing only the p-divisible group $A[p^\infty]$;

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

where $\sigma = g(1,1)$ is the Newton polygon having only slopes equal to $1/2$.
Equivalently this definition can be given by the property in the theorem just mentioned.
(2) We see that $g > 1$ and $\mathcal{N}(A) = \sigma$ imply 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 [36], see 18.13.
(3) 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.

21.22. Exercise. Let Y be a p-divisible group over a field K. Suppose $Y \sim \prod_i G_{d_i,c_i}$. Suppose there exist integers $d, h \in \mathbb{Z}_{>0}$ such that $Y[F^h] = Y[p^d]$. Show: *only factors G_{d_i,c_i} do appear with $d_i/(d_i + c_i) = d/h$.*

21.23. Proposition. *For every pair (d, c) of coprime non-negative integers we have $G_{d,c} \cong (G_{c,d})^t$. Let A be an abelian variety over a field $K \supset \mathbb{F}_p$, and $X = A[p^\infty]$. The Newton polygon $\mathcal{N}(A) := \mathcal{N}(X)$ is symmetric,* in the sense of 11.1.
Proof. The first equality follows from the definitions.

By 16.6 we have $A[m]^D = A^t[m]$ for every $m \in \mathbb{Z}_{>0}$. Hence $A[p^\infty]^t = A^t[p^\infty]$; use the definition of the Serre dual X^t; this formula is less trivial than notation suggests. Hence $G_{d,c}$and $G_{c,d}$ appear with the same multiplicity in the isogeny type of $X = A[p^\infty]$. This proves symmetry of $\mathcal{N}(X)$. $\square$

21.24. Remark. The theory as developed by Dieudonné and Manin gives the Newton polygon of a p-divisible group, and of an abelian variety over an arbitrary field in characteristic p. Note that for an abelian variety an easier construction is possible, which gives the same result, see Section 9, especially 9.3.

21.25. A proof for the Manin Conjecture. We have seen that the Manin Conjecture can be proved using the Honda-Tate theory, see Section 11. In [58], Section 5 we find a proof of that conjecture, using only methods of characteristic p. We sketch that proof (and please see the reference cited for notations and details).

We know that the conjecture holds for $G_{1,1}$: in every characteristic p there exists a supersingular elliptic curve, and $E[p^\infty] \cong G_{1,1}$. Hence every supersingular p-divisible group is algebraizable. We show that for a given $g \geq 1$ there exists an abelian variety A_0 with a principal polarization λ_0 such that A_0 is supersingular, and $a(A_0) = 1$. Methods of [58] show that for a given symmetric Newton polygon ξ, which automatically lies below $\sigma = \mathcal{N}(A_0)$, there exists a formal deformation of $(X_0, \lambda_0) = (A_0, \lambda_0)[p^\infty]$ to (X, λ) with $\mathcal{N}(X) = \xi$. By the Serre-Tate Theorem we know that a formal deformation of an algebraizable p-divisible group is algebraizable; hence there exists (A, λ) with $(X, \lambda) = (A, \lambda)[p^\infty]$; this proves the Manin Conjecture.

22. Some questions

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

22.1. Definition; see 12.2. 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. See Section 12. **(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, [72].
(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 [20], pp. 259 – 263; for a proof also see [55], 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 [55], 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 [56], 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.*

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

22.3. 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 [58], Section 5.

22.4. Open Problem. *Does there exist a proof of the Honda-Tate theorem* 1.2 *only using methods in characteristic p* ?

22.5. 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 [68], pp. 175/176; also see [47], pp. 202/203; see [35], 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 matrix algebras 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 [68], pp. 175/176 and [47] pp. 202/203 for characteristic zero; for arbitrary characteristic see [24]; for a discussion see [54], Theorem 3.3 and Theorem 3.4.

22.6. 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.*

22.7. 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.*

22.8. 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

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

22.9. 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 [57], Section 2.

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] S. Bosch, W. Lütkebohmert & M. Raynaud – *Néron models.* Ergebn. Math. (3) Vol. 21, Springer – Verlag 1990.

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

[8] 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.

[9] C.-L. Chai & F. Oort – *Hypersymmetric abelian varieties.* Quarterly Journal of Pure and Applied Mathematics, **2** (Special Issue: In honor of John H. Coates), (2006), 1–27.

[10] C.-L. Chai & F. Oort – *Moduli of abelian varieites and p-divisible groups.* Conference on arithmetic geometry, Göttingen July/August 2006. To appear: Clay Mathematics Proceedings.

[11] C.-L. Chai, B. Conrad & F. Oort - *CM-lifting of abelian varieties.* [In preparation]

[12] C. Chevalley – *Une démonstration d'un théorème sur les groupes algébriques.* Journ. de Math. 39 (1960), 307 – 317.

[13] B. Conrad – *A modern proof of Chevalley's theorem on algebraic groups.* J. Ramanujan Math. Soc. **18** (2002), 1 – 18.

[14] B. Conrad – *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem.* Enseign. Math. (2) **52** (2006), 37–108.

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

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

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

[18] 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.

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

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

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

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

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

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

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

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

[27] A. Grothendieck – *Esquisse d'un programme.* Manuscript 56 pp., January 1984. Reproduced in: Geometric Galois actions (Ed. L. Schneps & P. Lochak). Vol. 1: Around Grothendieck's *Esquisse d'un programme.* London Math. Soc. Lect. Note Series 242, Cambridge Univ. Press 1997; pp. 5 – 48 (English translation pp. 243 – 283).
http://www.institut.math.jussieu.fr/ leila/grothendieckcircle/EsquisseEng.pdf

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

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

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

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

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

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

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

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

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

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

[38] J. Lubin & J. Tate – . *Formal moduli for one-parameter formal Lie groups.* Bull. Soc. Math. France **94** (1966), 49 – 66.

[39] 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.

[40] J. Milne – it The fundamental theorem of complex multiplication.
arXiv:0705.3446v1, 23 May 2007

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

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

[43] 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.

[44] D. Mumford – *A note of Shimura's paper "Discontinuous groups and abelian varieties".*

Math. Ann. **181** (1969), 345 - 351.
[45] D. Mumford – *Geometric invariant theory.* Ergebn. Math. Vol. 34, Springer – Verlag 1965 (second version 1982, 1994).
[46] D. Mumford - A note of Shimura's paper "Discontinuous groups and abelian varieties". Math. Ann. **181** (1969), 345-351.
[47] D. Mumford – *Abelian varieties.* Tata Inst. Fund. Research and Oxford Univ. Press 1970 (2nd printing 1974).
[48] A. Néron – *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux.* Publ. Math. IHES **21**, 1964.
[49] F. Oort – *Commutative group schemes.* Lect. Notes Math. 15, Springer - Verlag 1966.
[50] F. Oort – *Algebraic group schemes in characteristic zero are reduced.* Invent. Math. **2** (1966), 79 - 80.
[51] 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.
[52] F. Oort – *Subvarieties of moduli spaces.* Invent. Math. **24** (1974), 95 - 119.
[53] F. Oort – *Good and stable reduction of abelian varieties.* Manuscr. Math. **11** (1974), 171 - 197.
[54] 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.
[55] 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.
[56] F. Oort – *CM-liftings of abelian varieties.* Journ. Algebraic Geometry **1** (1992), 131 - 146.
[57] F. Oort – *Some questions in algebraic geometry,* preliminary version. Manuscript, June 1995. http://www.math.uu.nl/people/oort/
[58] F. Oort — *Newton polygons and formal groups: conjectures by Manin and Grothendieck.* Ann. Math. **152** (2000), 183 - 206.
[59] 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.
[60] F. Oort & Yu. G. Zarhin - *Endomorphism algebras of complex tori.* Math. Ann. **303** (1995), 11 - 29.
[61] I. Reiner – *Maximal orders.* London Math. Soc. Monographs Vol. 28. Oxford 2003.
[62] M. Demazure & A. Grothendieck – *Schémas en groupes, Séminaire de géométrie algébrique, SGA3.* Vol I: Lect. Notes Math. **151**, Springer – Verlag 1970.
[63] A. Grothendieck – *Séminaire de Géométrie Algébrique, Groupes de monodromie en géométrie algébrique, SGA 7.* Lect. Notes Math. **288**, Springer – Verlag 1972.
[64] R. Schoof – *Nonsingular plane cubic curves over finite fields.* Journal Computat. Theory, Series A, **46** (1987) 183 – 211.
[65] J-P. Serre – *Corps locaux.* Hermann Paris 1962.
[66] J-P. Serre – *Géométrie algébrique et géométrie analytique.* Ann. Inst. Fourier **6)** (1956), 1 – 42.
[67] J-P. Serre & J. Tate – *Good reduction of abelian varieties.* Ann. Math. **88** (1968), 492 – 517.
[68] G. Shimura – *On analytic families of polarized abelian varieties and automorphic functions.* Ann. Math. **78** (1963), 149 – 193.
[69] G. Shimura & Y. Taniyama – *Complex multiplication of abelian varieties and its applications to number theory.* Publ. Math. Soc. Japan **6**, Tokyo 1961.
[70] T. Shioda – *Supersingular K3 surfaces.* In: *Algebraic Geometry,* Copenhagen 1978 (Ed. K. Lønsted). Lect. Notes Math. 732, Springer - Verlag (1979), 564 - 591.
[71] J. Silverman – *The arithmetic of elliptic curves.* Grad. Texts Math. 106, Springer – Verlag, 1986.
[72] J. Tate – *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134-144.
[73] J. Tate – *Classes d'isogénies de variétés abéliennes sur un corps fini (d'àpres T. Honda).*

Sém. Bourbaki **21** (1968/69), Exp. 352.
[74] 2005-05 VIGRE number theory working group. Organized by Brian Conrad and Chris Skinner. On: http://www.math.Isa.umich.edu/ bdconrad/vigre04.html
[75] W. C. Waterhouse – *Abelian varieties over finite fields.* Ann. Sc. Ec. Norm. Sup. 4.Ser, **2** (1969), 521 – 560).
[76] W. C. Waterhouse – *Introduction to affine group schemes.* Grad. Texts Math. 66, Springer – Verlag, 1979.
[77] 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.
[78] A. Weil – *Sur les courbes algébriques et les variétés qui s'en déduisent.* Hermann, 1948.
[79] A. Weil – *Variétés abéliennes et courbes algébriques.* Hermann, 1948.
[80] C.-F. Yu – *The isomorphism classes of abelian varieties of CM-type.* Journ. Pure Appl. Algebra **187** (2004), 305 – 319.
[81] J. G. Zarhin – *Isogenies of abelian varieties over fields of finite characteristic.* Math. USSR Sbornik **24** (1974), 451 – 461.
[82] J. G. Zarhin – *A remark on endomorphisms of abelian varieties over function fields of finite characteristic.* Math. USSR Izv. **8** (1974), 477 – 480.
[83] J. G. Zarhin – *Homomorphisms of abelian varieties over finite fields.* Summer school in Göttingen, June 2007. See this volume.

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