Abelian varieties over finite fields

Frans Oort & Aise Johan de Jong

IX-XII/2008

Seminar at Columbia University,
September — December 2008

In this seminar we will prove one theorem:

Theorem [HT] (T. Honda and J. Tate). *Fix a finite field $K = \mathbb{F}_q$. The assignment $A \mapsto \pi_A$ induces a bijection*

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

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.

An amazing theorem: on the left hand side we find geometric objects, usually difficult to construct explicitly; on the right hand side we find algebraic objects, easy to construct.

Most material we need can be found in the following basic references. You can find links to all of these documents Johan de Jong's webpage http://math.columbia.edu/∼dejong at Columbia University. Also see Frans Oort's webpage http://math.columbia.edu/∼oort.

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

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

[75] 2005-05 VIGRE number theory working group. Organized by Brian Conrad and Chris Skinner.

[60] F. Oort – *Abelian varieties over finite fields.* Summer School on varieties over finite fields, Göttingen 2007. To appear. Higher-dimensional geometry over finite fields, Advanced Study Institute 2007 Proceedings (Editors: Y. Tschinkel and D. Kaledin).

Instead of following the seminar, it might be more useful (?) to read the fascinating paper [74]: just 14 pages, sufficient for understanding a proof of this theorem. In the seminar we will basically follow this paper. For more references, for an introduction to this topic and to various methods used you can consult [60].

In the seminar several concepts, definitions, results and proofs will be explained. However we will assume known certain basic concepts; these are surveyed in an appendix. In case you feel you are not enough prepared for following the seminar, in case some of the basic concepts are not familiar to you, please let us know. We can either give more references, or have talks on such a topic, or we can explain things to you in private. Do not hesitate to ask for details.

In every talk in the seminar prerequisites needed in that talk should be stated, explained and discussed. Please indicate clearly of which statement you give a proof, and which statement you use as a **black box**.

You are welcome to contact us while preparing a talk.

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".

Introduction

Here is a sketch of the main lines in the proof (for definitions of the various concepts, see below or consult references).

The basic idea starts with a theorem by A. Weil, a proof for the Weil conjecture for an abelian variety A over simple a finite field $K = \mathbb{F}_q$ with $q = p^n$, see (3.3):

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

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* Theorem (3.3). *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 (5.2). 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 Theorem (5.2).

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 (10.1).

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

This result by Honda plus the last step shows that $(A \mod \sim) \mapsto (\pi_A \mod \sim)$ is *surjective*. See (11.1) - (11.5).

These four steps together show that the map

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

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

(0.1) Quesion / Open Problem. Surjectivity of the map $\mathcal{W}$, see Step 3 and Step 4, is proved by constructing enough complex abelian varieties. Can we give a purely geometric-algebraic proof, not using methods of varieties over the complex numbers?

1 LECTURE I: Weil numbers

See [74], the first three pages; see [60] §2. To make this talk work, please do all of this in great detail.

(1.1) Topic.
Give the definition of a Weil q-number.
Treat the special cases $\pi \in \mathbb{Q}$.
Give 2 definitions of a CM-field and prove their equivalence.
Give some examples of CM-fields. Find your own!
Characterize Weil q-numbers and give examples.
Try to convince the audience that it is easy to construct Weil numbers having certain properties. Two versions: finding suitable totally real numbers, and finding suitable monic polynomials with integer coefficients.
Find examples (two kinds) of Weil q-numbers π such that $\mathbb{Q}(\pi) \neq \mathbb{Q}(\pi^n)$ for some $n > 1$.

2 LECTURE II: Endomorphisms of abelian varieties and Frobenius

(2.1) Recall Frobenius morphisms. Briefly: Discuss absolute Frobenius, denoted $Frob$ for a scheme T over $\mathbb{F}_p$. Discuss relative Frobenius F for a scheme T over a base scheme S over $\mathbb{F}_p$. Discuss geometric Frobenius π_X for a scheme X over a finite field $K = \mathbb{F}_q$. In particular, we have π_A for an abelian variety over a finite field $K = \mathbb{F}_q$. Why is it an endomorphism?

(2.2) The Tate ℓ-group of an abelian variety. Briefly give the definition. Let A be an abelian variety over a field K. Let $\ell \in K^*$. Define $T_\ell(A)$ as a pro-finite group scheme over K. Show it is equivalent to give: either $T_\ell(A)$, or $T_\ell(A(K^{\mathrm{sep}}))$ endowed with the structure of a continuous Galois module over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Discuss some examples. Discuss the structure of this group (no proofs, black box), density of ℓ-power torsion points.

Optional: Extra on Tate ℓ-groups. Show or mention that a finite flat group scheme $N \to S$ of constant rank n, where n is invertible in $\mathcal{O}_S$ is etale over S. Discuss fundamental groups, Galois modules; e.g. see [10], 10.5. Should this be a separate topic? or material incorporated in other talks?

(2.3) Finite rank of endomorphism rings. 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. Give a proof. Conclude that the endomorphism ring has finite rank and conclude that in case A is simple, π_A is an algebraic integer, etc.

(2.4) Dual abelian varieties, and Rosati. Discuss the dual abelian variety. (Black box.) Define the notion of a polarization. Show how having a polarization gives rise to an involution on the endomorphism algebra, called the Rosati involution.

3 LECTURE III: Positivity of Rosati and the Weil conjecture for an abelian variety over a finite field

(3.1) Positivity of Rosati. Formulate and indicate the proof of this property.

(3.2) Verschiebung. Define the Veschiebung V for an abelian variety A over a field of characteristic p, by dividing $[p]$ by F. Show that the V is the transpose of the Frobenius of the dual abelian variety.

Optional: Extra on Verschiebung. Discuss V_G for a finitely presented, flat, commutative group scheme over a base in positive characteristic; see [63], Exp. VII_A.4. Show

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

for an abelian scheme over a base scheme S in positive characteristic. See [23].

(3.3) 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 [79], page 70; [80], page 138; [47], Theorem 4 on page 206. Using properties of Frobenius and Verschiebung give a proof, which is different form the classical approach by Weil, see [23].

Remark. A proof of this Weil conjecture can also be given along the "classical lines", see [47], Theorem 4 on page 206. Is this an alternative to be presented as the seminar? Or perhaps present both proofs?

4 LECTURE IV: Abelian varieties over finite fields

See [73], [74] and [84] or one of the many other possible references.

(4.1) 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. $\square$

This was conjectured by Tate. In 1966 Tate proved this in case K is a finite field, see [73]. The case of function field in characteristic p was proved by Zarhin and by Mori, see [82], [83], [43]; also see [42], pp. 9/10 and VI.5 (pp. 154-161).

(4.2) Moduli spaces of abelian varieties: Existence Formulate as a black box the existence of moduli spaces of polarized abelian varieties. Deduce finiteness properties of the numbers of isomoprhism classes of abelian vareities.

(4.3) Proof of the theorem over finite fields. Suggestion: Show (2.3) e.g. by following arguments in [47]. Then show (4.1) over a finite field, either by following [73], or by using [83].

5 LECTURE V: Full description of endomorphism algebras

(5.1) Central Simple Algebras. Recall briefly the notion of a central simple algebra and the description of them over number fields, including local to global principle.

(5.2) 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

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

(5.3) 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.
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.

(5.4) Proofs These theorems should be discussed and proved in the seminar.

(5.5) Note that refstruct1 eables us to compute from a given Weil q-number π the number $e = [\mathbb{Q}(\pi):\mathbb{Q}]$, the algebra D, and hence $d = \sqrt{[D:L]}$ and $g = ed/2$.

6 LECTURE VI: Albert classification and endomorphism algebras

(6.1) Explain the Albert classification. This is a classification of central simple algebras finite dimensional over $\mathbb{Q}$ endowed with a positive involution. See [60, Section 18.2]. Treat this result as a black box.

(6.2) Explain which types occur. Which types of the Albert classification occur as endomorphism algebras with Rosati involution for polarized abelian varieties over finite fields? See [60, Section 15.9].

(6.3) Examples. Going back to our examples of Weil q-numbers describe the associated division algebras with Rosati involution. Mention again (5.5).

(6.4) Rephrase the notions mentioned in (5.5), and compute various examples. E.g. see (6.7).

Examples and extra topics, which can be used in the remaining talks

Here we mention some topics not yet included in despcriptions of various talks. Examples and ideas mentioned here should feature in some of the talks to be given. Please choose from these topics as material for illustation. Or/and, go through some of this material yourself in order to get some background information and feeling for the ideas of the topic of this seminar. – More information on these aspects is to be found in [60].

(6.5) Isotypic. We have defined π_A, an algebraic integer, for any simple abelian variety A over a finite field $K = \mathbb{F}_q$. We define B to be isotypic (over K), if there exists a simple A and an isogeny $B \sim A^m$ for some $m \in \mathbb{Z}_{>0}$. We define $\pi_B := \pi_A$. Note that if C is isotypic over K then $C \otimes K'$ is isotypic for every $K \subset K'$, see (11.4).

(6.6) An application of [HT]: **the Manin conjecture.** At least one lecture should include the primary motivation and this important application of Honda-Tate theory:

Let ξ be a symmetric Newton polygon and fix p.
There exists an abelian variety A over $\overline{\mathbb{F}_p}$ with Newton polygon equal to ξ.

See [74], the last example in §1; see [60], Section 11.
Remark. Another proof (nott using complex uniformization) of the Manin conjecture will be given in the course.

(6.7) Isogeny classes of elliptic curves over finite fields.
See [76]; see [60] §14.
Note the aspect that under a finite extension $\mathbb{F}_q = K \subset K' = \mathbb{F}_{q^m}$ in general several K-isogeny clasess get merged into one K'-isogeny class, and, in general there exist K'-isogeny classes which do not come from any abelian variety over K. Discuss examples.

(6.8) Behavior of $\mathrm{End}(A)$ under field extension.
If A is an abelian variety over $K$and $K \subset K'$ is a field extension, then

$$\mathrm{End}(A) \subset \mathrm{End}(A \otimes K').$$

Moreover

$$\mathrm{End} A \otimes K' \ / \ \mathrm{End}(A) \text{ has no torsion.}$$

Give a proof. Give examples.
The fact that $\mathrm{End}(A) \subsetneqq \mathrm{End} A \otimes K'$ can have two "reasons"
e.g. A is simple, and $A \otimes K'$ is not simple,

e.g. A and $A \otimes K'$ are both simple, but the endomorphism ring gets larger (or a combination of both).

Give examples.

(6.9) Exercise. Let E be an elliptic curve over a prime field $\mathbb{P}$. Show that:
(1) If $\mathbb{P} = \mathbb{Q}$ show: $\mathrm{End}(E) = \mathbb{Z}$.
(2) If $\mathbb{P} = \mathbb{F}_p$ show that $\mathrm{End}(E)$ is an imaginary quadratic field.
(3) $\mathrm{End}(E)$ is commutative.
(4) Give an example of an abelian variety A simple over $\mathbb{Q}$ with $\mathrm{End}(A) \supsetneqq \mathbb{Z}$.
(5) Give an example of an abelian variety A simple over $\mathbb{F}_p$ such that $\mathrm{End}(A)$ is not commutative.

(6.10) Behavior of $\mathrm{End}(A)$ under reduction modulo p.
Let A be an abelian scheme over an integral domain R, and let $R \to K$ be a surjective homomorphism onto a field. We obtain a homomorphism of rings $\mathrm{End}(A) \to \mathrm{End}(A \otimes_R K)$. Show:
(1) This homomorphism is injective.
(2) Suppose $n \in \mathbb{Z}_{>0}$ is not divisible by the characteristic of K. Then $\mathrm{End}(A \otimes_R K)$ / $\mathrm{End}(A)$ has no n-torsion.
(3) Give examples where $\mathrm{End}^0(A) \subsetneqq \mathrm{End}^0(A \otimes_R K)$.
(4) Give examples where $\mathrm{End}^0(A) = \mathrm{End}^0(A \otimes_R K)$ and $\mathrm{End}(A) \subsetneqq \mathrm{End}(A \otimes_R K)$

(6.11) Deligne: classification of ordinary abelian varieties. See [17].

7 LECTURE VII: On p-divisible groups

(7.1) Topic. Give the definition of a p-divisible group. Define homomorphisms and endomorphism rings of p-divisible groups. Define isogenies of p-divisible groups. Give a discussion with examples.

Additional: Give an easy example to show that the "naive Tate-p-group" of an abelian scheme over a base on which p is not invertible is not a good notion.

(7.2) Lemma. *Let A be an abelian variety over a field K. Let $\mathcal{O} \subset \mathrm{End}^0(A)$ be a subring of the endomorphism algebra of A. Show that if $\mathcal{O}$ is a finite $\mathbb{Z}$-module, then there exists an isogeny $A \to B$ of abelian varieties over K such that $\mathcal{O} \subset \mathrm{End}(B)$.*

Additional: Give an example to show an isogeny is needed. Give the analogue of this lemma for p-divisible groups.

(7.3) Lemma. *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 $\dim(A) = g = er/2$. Show there exists a number field field P, with $L \subset P \subset D$, where P is a CM-field of degree $2g$ over $\mathbb{Q}$.*

A reference for a proof of this is Tate's Bourbaki lecture [74], Section 3, Lemma 2. Give a proof of this lemma.

Remark/Notation. We will write L for the center of $D = \mathrm{End}^0(A)$. We will write $P \supset L$ for a splitting field of D/L. Also we write P for a CM-algebra for an abelian variety.

Additional: What would be an analogue of this lemma for p-divisible groups over finite fields? Is it true?

(7.4) 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 $X = A[p^\infty]$. Assume that $\mathcal{O}_L \subset \mathrm{End}(A)$, which we may after replacing A by an isogenous abelian variety because of Lemma (7.2) above. Consider the set $\Sigma_L^{(p)}$ of discrete valuations of L dividing the rational prime number p.*
(1) *The decomposition*

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

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 $\gamma_w + \gamma_{\overline{w}} = 1$.*

This theorem should have been proved almost completely in the talk giving the precise description of the endomoprhism algebra of an abelian variety over a finite field. Recall the necessary setup if needed. See also: [78], and [60], 9.2 and 21.22.

(7.5) CM-types. Define the notion of a CM-type of a CM field. Suppose that A is an abelian variety over the complex numbers $\mathbb{C}$. Suppose that P is a CM-field contained in $\mathrm{End}^0(A)$. Assume that $[P : \mathbb{Q}] = 2\dim(A)$. Show that the set of complex embeddings $\Phi = \{\varphi_1, \cdots, \varphi_g\}$ of P which occur in the P-action on the tangent space of A form a CM-type; i.e. $\Phi \sqcup \Phi{\cdot}\rho = \mathrm{Hom}(P, \mathbb{C})$, where ρ is the involution of P having the totally real subfield as fixed field.

Additional: Define similarly the notion of a CM-type for a finite separable algebra P over $\mathbb{Q}_p$. Is there an analogue of the result above for actions of P on p-divisible groups over a field of characteristic p? What about p-divisible groups over complete discrete valuation rings of mixed characteristic $(0, p)$?

8 LECTURE VIII: The Shimura-Taniyama formula

(8.1) Topic. This formula relates the characteristic p reduction of the p-divisible group of an CM-abelian variety with good reduction to the CM-field + CM-type of the abelian variety in characteristic 0. In this talk we formulate this formula and prove it along the lines of Tate's argument using CM-theory for p-divisible groups in his Bourbaki lecture.

Please follow Brian Conrad's notes; here is a link
http://math.stanford.edu/∼conrad/vigregroup/vigre04/stformula.pdf.

Other references: [74], Lemma 5, or [60], Section 9, or [70], §13, or [40], Corollary 2.3.

9 LECTURE IX: CM-abelian varieties

In this lecture we treat the following topics.

(9.1) Definition. Give the definition of smCM for an abelian variety.

(9.2) Construction. Recall the definition of a CM-type Φ on a CM-field P. Let $\Phi = \{\sigma_1, \ldots, \sigma_g\}$. Thus Φ induces a map

$$\sigma_\Phi = (\sigma_1, \ldots, \sigma_g) : P \longrightarrow \mathbb{C}^g.$$

Show that $T = \mathbb{C}^g/\sigma_\Phi(\mathcal{O}_P)$ is a complex torus with $P \subset \mathrm{End}^0(A)$.

Remark/Notation. We will write L for the center of $D = \mathrm{End}^0(A)$. We will write $P \supset L$ for a splitting field of D/L. Also we write P for a CM-algebra for an abelian variety.

(9.3) Lemma. For any (P, Φ) as above the complex torus T constructed in (9.2) is an abelian variety, i.e., it is the complex manifold associated to an abelian variety A. Also, show that $P \subset \mathrm{End}^0(A)$ and that we can recover Φ from this as in Lemma (7.5).

(9.4) Lemma. Suppose that A is an abelian variety with smCM over an algebraically closed field k. If the characteristic of k is zero, show that there exists a number field $M \subset k$ and an abelian variety A_M over M such that A and $A_M \otimes k$ are isomorphic over k.

Additonal: What is an analogous statement to this if the characteristic of k is $p > 0$. Is this analogous statement true? You might want to consult [51]. Or first do:

Exercise. Show there exists an abelian variety A over a field $K \supset \mathbb{F}_p$ such that A admits smCM, and such that A cannot be defined over a finite field (and here K is not a finite field).

(9.5) Black Box: Néron models. Let R be a complete discrete valuation ring with field of fractions K. Let A_K be an abelian variety over K. Define the notion of a *Néron model* of A_K over R. Formulate existence and functoriality of the Néron model. In particular, discuss how the endomorphisms of A_K act on the special fibre.

(9.6) Black box: Potential semi-stable reduction Formulate potentially semi-stable reduction.

(9.7) Lemma. *Show, using ℓ-torsion points that in the semi-stable reduction case the endomorphism ring of the generic fibre injects into the endomorphism ring of the special fibre.*

(9.8) Lemma. *Use the above to show that given an abelian variety A with smCM over a number field K, there exists a finite extension $K \subset K'$ such that $A_{K'}$ has everywhere good reduction, i.e., extends to an abelian scheme over the ring of integers $\mathcal{O}_{K'}$.*

(9.9) Remark. An abelian variety of CM-type is an abelian variety in *characteristic zero* with smCM where moreover the inclusion $P \subset \mathrm{End}^0(A)$ is given. However an abelian variety in positive charactersitic will not be called an abelian variety of CM-type. See a discussion in [60], 13.12 why.

10 LECTURE X: The Honda lifting theorem.

A Weil q-number π is said to be *effective* if there exists an abelian variety A over $\mathbb{F}_q$ such that the geometric Frobenius π_A corresponds to π. The goal of this lecture is to prove the following theorem, using the material from the preceding lectures.

(10.1) Theorem (Honda). *For every Weil q-number π there is an integer $N > 0$ such that π^N is effective.*

(10.2) An open problem. The proof we know of the Honda theorem (10.1) is via complex uniformization. *Is there a proof of this theorem using only algebraic, and no analytic methods?*

Using previous results in the seminar, show the Honda lifting theorem. The rest of the material in this section is not necessary for the general line of thought, but please include some of it in the lecture as time permits! Namely, we think it is instructive to discuss [56], and as well as some examples as in [11]. Here is a definition and theorem that might be discussed.

(10.3) Definition. Suppose A_0 be an abelian variety over a field $K \supset \mathbb{F}_p$ such that A_0 admits smCM.

1. A *lifting of A_0 to characteristic zero* is given by an integral domain $(R, \mathfrak{m})$, with a homomorphism $R \to K$, an abelian scheme A over R, such that (a) $A_0 \cong A \otimes_R K$, and (b) the characteristic of the fraction field of R is zero.
2. 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).
3. Moreover, if $P \subset \mathrm{End}^0(A_0)$ is a CM-field of degree $2g$ over $\mathbb{Q}$ and $\mathrm{End}^0(A) = P$ we say that A_0/K satisfies (CML) by P.

(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.*

See [29], Th. 1 on page 86, see [74], Th. 2 on page 102. For the notion (CML) see (10.3).

The isogeny mentioned in the theorem is necessary in general, as follows from [56]. It is an open problem whether the exension $K \subset K'$ of finite fields is necessary ?!

Additional: Analyzing the road to a proof of this theorem we see that complex uniformization is used. However in [11], Section 5 and Appendix A, a purely algebraic proof for (10.4) is given. Comments?

Note that we do not have an algebraic proof for (10.1), nor do we have an algebraic proof for [HT] on page 1.

11 LECTURE XI: The Weil restriction functor

(11.1) 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 in this seminar. Write $S = \mathrm{Spec}(K)$ and $S' = \mathrm{Spec}(K')$. We have the base change functor

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

General nonsense defines a *right adjoint functor* to the base change functor to be a functor

$$\Pi = \Pi_{S'/S} = \Pi_{K'/K} \ : \ \mathrm{Sch}_{S'} \quad \to \quad \mathrm{Sch}_S,$$

characterized by the following universal property:

$$\mathrm{Mor}_S(T, \Pi_{S'/S}(Z)) = \mathrm{Mor}_{S'}(T_{S'}, Z).$$

functorially in $T \in \mathrm{Sch}_S$, and $Z \in \mathrm{Sch}_{S'}$. In other words, the scheme $\Pi(Z)$ is supposed to represent the functor $T \mapsto \mathrm{Mor}_{S'}(T_{S'}, Z)$.

Note that, in our case where K'/K is Galois we have $\Pi_{S'/S}(Z) \times_S S' = Z \times_{S'} \cdots \times_{S'} Z$ the self-product of $[K' : K]$-copies of Z over S'. Please explain why!

In our situation, with K'/K Galois, Weil showed that $\Pi_{S'/S}(Z)$ exists. In fact, consider $Z \times_{S'} \cdots \times_{S'} Z$, the self-product of $[K' : K]$ copies of Z over S'. It can be shown that, if Z is quasi-projective over K', then $Z \times_{S'} \cdots \times_{S'} Z$ can be descended to K in such a way that it solves this problem. Namely, there is a natural action of $G = \mathrm{Gal}(K'/K)$ on the self product such that

$$\Pi_{S'/S}(Z) = (Z \times_{S'} \cdots \times_{S'} Z)/G.$$

Please explain! For a more general situation, see [25], Exp. 195, page 195-13. Also see [75], Nick Ramsey - CM seminar talk, Section 2.

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

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

where $f_B(T)$, resp. $f_{B'}(T)$ are the characteristic polynomials of Frobenius on B, resp. B'.

See [74], page 100. We make a little detour. From [14], 3.19 we cite:

(11.3) 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.

(11.4) 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 [75], Nick Ramsey - CM seminar talk, Section 2; see (11.1). 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 $\mathrm{Hom}(C_1, C_2) \neq 0$. Hence: if A is simple, any two isogeny factors of $A \otimes_K K'$ are isogenous. $\square$

By Step 6 and by Lemma (11.2) of [60], Section 10 we conclude:

(11.5) 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 [74], Lemme 1 on page 100.

12 Checklist topics/talks

Here we can fill in the various topics with speakers.

(1) 12-IX-2008
Speaker: Bhargav Bhatt

(2) 19-IX-2008
Speaker: Matt Deland

(3) 26-IX-2008
Speaker: Sho Tanimoto

(4) 3-X-2008
Speaker: Alon Levy

(5) 10-X-2008
Speaker: Mingmin Shen

(6) 17-X-2008
Speaker: Bin Du

(7) 24 - X - 2008
Speaker:

(8) 31 - X - 2008
Speaker:

(9) 7 - XI - 2008
Speaker:

(10) 14 - XI - 2008
Speaker:

(11) Last talk: 21 - XI - 2008
Speaker:

13 Appendix: prerequisites

In this apendix we indicate some of the definitions, concepts and results we assume you know. please study these, ask for advice or ask for further explanation.

Also in the seminar some "black boxes" will be used: results, technical details, with a a reference, which will be used, but not proved in the seminar.

However, some of the subjects below could be chosen as a **"Topic"** in the seminar.

Recommended reading:
Abelian varieties: [47], [35], [15] Chapter V.
Honda-Tate theory: [74], [29], [75].
Abelian varieties over finite fields: [73], [76], [78], [65].
Group schemes: [63], [49].
Endomorphism rings and endomorphism algebras: [69], [24], [73], [76], [54].
CM-liftings: [56], [11].

(13.1) Algebra.
We need: standard facts about fields, number fields, valuations, ramification in finite extensions.

(13.2) Central simple algebras: the Brauer group.
Basic references: [7], [62], [8] Chapter 7, [66] Chapter 10.

(13.3) Abelian varieties.
Basic references: [47], [15], [GM].

(13.4) Endomorphism algebras of abelian varieties.
Basic references: [69], [47], [35] Chapt. 5, [54].
Endomorphism algebras of abelian varieties can be classified. In many cases we know which algebras do appear. However it is difficult in general to describe all orders in these algebras which can appear as the *endomorphism ring* of an abelian variety.

(13.5) Complex tori with smCM **and abelian varieties with** CM.
See [70], [47], [35], [61]; see [60] §19.

(13.6) Abelian varieties with good reduction.
References: [48], [12], [68], [64], [6], [53], [13].

(13.7) Dieudonné theory, some properties in positive characteristic. See [39], [19]. For information on group schemes see [49], [63], [77], [10].

14 The Tate-p-conjecture.

Probably we will not use the following results:

(14.1) Exercise. Let A and B be abelian varieties over a field K. We know that $\mathrm{Hom}(A, B)$ is of finite rank as $\mathbb{Z}$-module. Let p be a prime number. 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 [78], Theorem 5 on page 56. Also see [84].

(14.2) 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.

(14.3) 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. $\square$

This was proved by Tate in case K is a finite field; a proof was written up in [78]. 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 (14.4).

(14.4) 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.* $\square$

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.

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.* Summer School on arithmetic geometry, Göttingen July/August 2006. To appear: Clay Mathematics Proceedings. Arithmetic geometry, Proceedings of the Clay Summer School Gttingen 2006, (Editors: Y. Tschinkel, H. Darmon and B. Hassett)

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

[12] C. Chevalley – *Une dmonstration d'un thorme sur les groupes algbriques.* Journ. de Math.39 (1960), 307317.

[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 – *Abelian varieties over finite fields.* Summer School on varieties over finite fields, Göttingen 2007. Higher-dimensional geometry over finite fields, Advanced Study Institute 2007 Proceedings (Editors: Y. Tschinkel and D. Kaledin). To appear.

[61] F. Oort & Yu. G. Zarhin - *Endomorphism algebras of complex tori.* Math. Ann. **303** (1995), 11 - 29.

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

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

[64] A. Grothendieck – *Séminaire de Géométrie Algébrique, Groupes de monodromie en géométrie algébrique, SGA 7.* Lect. Notes Math. **288**, Springer – Verlag 1972.

[65] R. Schoof – *Nonsingular plane cubic curves over finite fields.* Journal Computat. Theory, Series A, **46** (1987) 183 – 211.

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

[67] J-P. Serre – *Géométrie algébrique et géométrie analytique.* Ann. Inst. Fourier **6** (1956), 1 – 42.

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

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

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

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

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

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

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

[75] 2005-05 VIGRE number theory working group. Organized by Brian Conrad and Chris Skinner. On: http://www.math.Isa.umich.edu/ bdconrad/vigre04.html

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

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

[78] 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.

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

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

[81] C.-F. Yu – *The isomorphism classes of abelian varieties of CM-type.* Journ. Pure Appl. Algebra **187** (2004), 305 – 319.

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

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

[84] J. G. Zarhin – *Homomorphisms of abelian varieties over finite fields.* Summer School on varieties over finite fields, Göttingen 2007. Higher-dimensional geometry over finite fields, Advanced Study Institute 2007 Proceedings (Editors: Y. Tschinkel and D. Kaledin). To appear.

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

Aise Johan de Jong
Columbia University, dejong@math.columbia.edu