

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*

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

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 at Columbia University. Also see Frans Oort's webpage.

[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'après T. Honda)*. Sémin. 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 $\text{colim}_{i \rightarrow}$ 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 $\psi : \mathbb{Q}(\pi_A) \rightarrow \mathbb{C}$ has absolute value $|\psi(\pi_A)| = \sqrt{q}$.*

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*

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

is well-defined.

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

$$A \sim B \iff \pi_A \sim \pi_B.$$

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 $\mathcal{W} : \mathcal{M}(\mathbb{F}_q, s) \rightarrow W(q)$ 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 (11.1).

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 $(A \bmod \sim) \mapsto (\pi_A \bmod \sim)$ is *surjective*. See (13.1) - (13.5).

These four steps together show that the map

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

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

(0.1) Question / 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 $T_\ell(A(K^{\text{sep}}))$ endowed with the structure of a continuous Galois module over $\text{Gal}(K^{\text{sep}}/K)$. 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 $N \rightarrow S$ 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 $\ell \neq \text{char}(K)$ the natural map

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

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 Verschiebung 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

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

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 $\pi_A \in \text{End}(A)$, 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 $\psi : \mathbb{Q}(\pi_A) \rightarrow \mathbb{C}$ we have*

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

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 from 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*

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

is an isomorphism. □

This was conjectured by Tate. In 1966 Tate proved this in case K is a finite field, see [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 isomorphism classes of abelian varieties.

(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 $\pi_A \in \text{End}(A)$ 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 $\text{Irr}(\pi_A) \in \mathbb{Z}[T]$.

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

$$A \sim_K B \iff f_A = f_B.$$

(5.3) Theorem (Tate). Suppose A is a simple abelian variety over the finite field $K = \mathbb{F}_q$.

(1) The center of $D := \text{End}^0(A)$ equals $L := \mathbb{Q}(\pi_A)$.

(2) Moreover

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

where g is the dimension of A . Hence: every abelian variety over a finite field admits smCM.

We have:

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

(3)

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

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

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

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

$$\text{inv}_w(D/L) + \text{inv}_{\bar{w}}(D/L) = 0 \pmod{\mathbb{Z}},$$

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

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

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 described the associated division algebras with Rosati involution.

7 FURTHER LECTURES

The following material below still has to be subdivided into lectures.

8 Statement of [HT], and many examples.

This should be mentioned in the introduction of the seminar, and can be recalled if necessary. In several talks examples should be given.

(8.1) Topic. Application (14.1), the Manin conjecture: a proof should be given using Honda-Tate theory. (A proof using methods in characteristic p will be given in the course).

(8.2) Topic. The classification of all isogeny classes of elliptic curves over finite fields should be given as an illustration, see (14.3). In this case show that under an extension of finite fields new isogeny classes are created, and old isogeny classes can be joined

9 p -divisible groups

(9.1) Topic. Give the definition of a p -divisible group. Give a discussion with examples. Give a proof of the theorem below.

Suggestion: 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.

(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 $D = \text{End}^0(A)$ 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 $2g$. If necessary we replace A by a K -isogenous abelian variety (again called A) such that $\mathcal{O}_P \subset \text{End}(A)$. Then also $\mathcal{O}_L \subset \text{End}(A)$.*

(1) The decomposition

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

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 \bar{w} be the discrete valuation of L obtained from w by complex conjugation on the CM-field L ; then $\gamma_w + \gamma_{\bar{w}} = 1$.

See [78]. See [60], 9.2 and 21.22.

10 The Shimura-Taniyama formula

(10.1) Topic. Formulate this formula, e.g. see [60], Section 9. Should/can we give a proof or treat this as a “black box” in the seminar? See [70], §13; see [40], Corollary 2.3.

Tate gave a proof based on “CM-theory for p -divisible groups”. See [74], Lemma 5; see [75], Shimura-Taniyama formula by B. Conrad, Theorem 2.1.

11 Start surjectivity: 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 is conjugated to π .

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

See [74]. See [60], Section 10, Steps 1 – 6.

(11.2) Topic(s). This theorem should be proved. It seems useful to split up the talk(s) in steps in order to make the proof transparent, to make clear what exactly is used and what is proved in the seminar.

(11.3) An open problem. We will see that the proof we know of the Honda theorem (11.1) is via complex uniformization.

Is there a proof of this theorem using only algebraic, and no analytic methods?

12 A corollary of the Honda lifting theorem.

Material in this section is not necessary for the general line of thought.

(12.1) 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 $L \subset \text{End}^0(A_0)$ is a CM-field of degree $2g$ over \mathbb{Q} and $\text{End}^0(A) = L$ we say that A_0/K satisfies (CML) by L .

(12.2) Theorem (Honda). *Let $K = \mathbb{F}_q$. Let A_0 be an abelian variety, defined and simple over K . Let $L \subset \text{End}^0(A_0)$ 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 [74], Th. 2 on page 102. For the notion (CML) see (12.1).

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

(12.3) Analyzing the road to a proof of this theorem we see that complex uniformization is used. However in [11], Section 5 and Appendix A we see that a purely algebraic proof can be given. Is this something to discuss in the seminar?

(12.4) Topic. Using previous results in the seminar, show the Honda lifting theorem. It might be instructive to discuss [56], and to discuss some examples as in [11].

13 The Weil restriction functor

(13.1) 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); write $S = \text{Spec}(K)$ and $S' = \text{Spec}(K')$. We have the base change functor

$$\text{Sch}/_S \rightarrow \text{Sch}_{S'}, \quad T \mapsto T_{S'} := T \times_S S'.$$

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

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

In this situation, with K'/K separable, Weil showed that $\Pi_{S'/S}(Z)$ exists. In fact, consider $\times_{S'}^{[K':K]} Z = Z \times_{S'} \cdots \times_{S'} Z$, 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 [75], Nick Ramsey - CM seminar talk, Section 2.

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

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

□

See [74], page 100.

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

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*

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

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

□

(13.4) 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 $\Pi = \Pi_{\text{Spec}(K')/\text{Spec}(K)}$. 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 (13.1). 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

$$\Pi(C_1) \otimes K' \cong (C_1)^N \sim (A \otimes_K K')^{eN}, \quad (C_2)^N \sim (A \otimes_K K')^{fN}; \quad \text{hence} \quad \text{Hom}(C_1, C_2) \neq 0.$$

Hence: if A is simple, any two isogeny factors of $A \otimes_K K'$ are isogenous.

□

By Step 6 and by Lemma (13.2) of [60], Section 10 we conclude:

(13.5) 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.

(13.6) Topic. Discuss the Weil restriction functor. Apply to abelian varieties over finite fields. Using the Honda theorem (11.1), finish the proof of [HT], e.g. see [60], Section 10, Step 7.

14 Some applications and examples.

(14.1) An application of [HT]: the Manin conjecture. *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 [39], Conjecture 2 on page 76; see [74] page 98; see [60] §11.

(14.2) Deligne: classification of ordinary abelian varieties.

See [17].

(14.3) All isogeny classes of elliptic curves over a finite field.

See [76]; see [60] §14.

15 Checklist topics/talks

Here we can fill in the various topics with speakers.

(1) Topic.
Speaker.

(2) Topic.
Speaker.

(3) Topic.
Speaker.

(4) Topic.
Speaker.

(5) Topic.
Speaker.

(6) Topic.
Speaker.

(7) Topic.
Speaker.

(8) Topic.
Speaker.

(9) Topic.
Speaker.

(10) Topic.
Speaker.

(11) Topic.
Speaker.

(12) Topic.
Speaker.

(13) Topic.
Speaker.

16 Appendix: prerequisites

In this appendix 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 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].

(16.1) Algebra.

We need: standard facts about fields, number fields, valuations, ramification in finite extensions.

(16.2) Central simple algebras: the Brauer group.

Basic references: [7], [62], [8] Chapter 7, [66] Chapter 10.

(16.3) Abelian varieties.

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

(16.4) 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.

(16.5) Complex tori with smCM and abelian varieties with CM.

See [70], [47], [35], [61]; see [60] §19.

(16.6) Abelian varieties with good reduction.

References: [48], [12], [68], [64], [6], [53], [13].

(16.7) Dieudonné theory, some properties in positive characteristic. See [39], [19].

For information on group schemes see [49], [63], [77], [10].

17 The Tate- p -conjecture.

Probably we will not use the following results:

(17.1) Exercise. Let A and B be abelian varieties over a field K . We know that $\text{Hom}(A, B)$ is of finite rank as \mathbb{Z} -module. Let p be a prime number. Show that the natural map

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

is *injective*. Also see [78], Theorem 5 on page 56. Also see [84].

(17.2) Remark. One 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.

(17.3) 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*

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

is an isomorphism. □

This was proved by Tate in case K is a finite field; a proof was written up in [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 (17.4).

(17.4) 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 $\text{Spec}(R)$. Let $\beta_K : X_K \rightarrow Y_K$ be a homomorphism. There exists (uniquely) $\beta : X \rightarrow Y$ over $\text{Spec}(R)$ extending β_K .* □

This was proved by Tate, under the extra assumption that the characteristic of K is zero. For the case $\text{char}(K) = p$, 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 varieties 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 Göttingen 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 démonstration d'un thorme sur les groupes algébriques*. 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*. Grundle. math. Wissensch. 255, Springer – Verlag 1983.
- [35] H. Lange & C. Birkenhake - *Complex abelian varieties*. Grundle. 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 – *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*. Intl. 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'après T. Honda)*. Sémin. 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.lsa.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

Columbia University, Dept. Math. Rm 415

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