

COMPOSITIO MATHEMATICA

HANS-GEORG RÜCK

Abelian surfaces and jacobian varieties over finite fields

Compositio Mathematica, tome 76, n° 3 (1990), p. 351-366

http://www.numdam.org/item?id=CM_1990__76_3_351_0

© Foundation Compositio Mathematica, 1990, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Abelian surfaces and Jacobian varieties over finite fields

HANS-GEORG RÜCK

Fachbereich 9 Mathematik, Universität des Saarlands, D-6600 Saarbrücken, Federal Republic of Germany

Received 22 November 1988; accepted in revised form 12 January 1990

1. Introduction and results

Let C be a projective non-singular curve of genus 2 over a finite field k with q ($q = p^n$) elements. The zetafunction of C is a rational function of the form

$$\frac{1 + a_1T + a_2T^2 + a_1qT^3 + q^2T^4}{(1 - T)(1 - qT)}$$

with integers a_1 and a_2 . The Riemann hypothesis for curves restricts these coefficients to $|a_1| \leq 4q^{1/2}$ and $|a_2| \leq 6q$. The problem is to find all a_1 and a_2 which occur in this way from curves over k of genus 2.

The theory of abelian varieties over finite fields is an important tool to handle this problem.

Let A be an abelian variety over k . We denote by $f_A(T)$ the characteristic polynomial of the Frobenius endomorphism π_A of A . Two abelian varieties A and B over k are k -isogenous if and only if $f_A(T)$ is equal to $f_B(T)$.

Let J be the Jacobian variety of the curve C of genus 2, then $f_J(T)$ equals $T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$, where a_1 and a_2 are the corresponding coefficients of the zetafunction of C .

Therefore the problem of finding all a_1 and a_2 can be divided into two parts. At first one has to determine the polynomials $f_A(T)$ for all the abelian varieties A over k of dimension 2. Then one has to decide whether a given abelian variety is k -isogenous to the Jacobian variety of a curve.

In this paper we present two theorems which give partial solutions of the problem.

Let $\text{End}_k(A)$ be the ring of k -endomorphisms of A . To avoid a lot of calculations for special cases we restrict ourselves to those abelian varieties A whose algebra $\text{End}_k(A) \otimes \mathbb{Q}$ is a field. The same methods can be used to solve the problem in general (see also [H-N]).

THEOREM 1.1. *The set of $f_A(T)$ for all abelian varieties A over k ($\#k = q = p^n$) of dimension 2 whose algebra $\text{End}_k(A) \otimes \mathbb{Q}$ is a field is equal to the set of*

polynomials $f(T) = T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$ where the integers a_1 and a_2 satisfy the following conditions:

- (a) $|a_1| < 4q^{1/2}$ and $2|a_1|q^{1/2} - 2q < a_2 < a_1^2/4 + 2q$,
- (b) $a_1^2 - 4a_2 + 8q$ is not a square in \mathbb{Z} ,
- (c) either (i) $v_p(a_1) = 0, v_p(a_2) \geq n/2$ and $(a_2 + 2q)^2 - 4qa_1^2$ is not a square in \mathbb{Z}_p or
 (ii) $v_p(a_2) = 0$ or (iii) $v_p(a_1) \geq n/2, v_p(a_2) \geq n$ and $f(T)$ has no root in \mathbb{Z}_p .

REMARKS. (i) The corresponding theorem for elliptic curves is given by Waterhouse [Wa].

(ii) The conditions $|a_1| < 4q^{1/2}$ and $v_p(a_1) \geq n/2$ in parts (a) and (c)

(iii) of Theorem 1.1 have the following consequences:

If n is odd and $p \geq 7$, there are only the cases $(a_1, a_2) = (0, 0)$ and $(0, \pm q)$. Then $f(T)$ has no root in \mathbb{Z}_p .

If n is even, we just get $(a_1, a_2) = (0, 0), (0, -q)$ and $(\pm q^{1/2}, q)$. $f(T)$ has no root in \mathbb{Z}_p if and only if $p \not\equiv 1 \pmod 8, p \not\equiv 1 \pmod{12}$ or $p \not\equiv 1 \pmod 5$ respectively.

We want to decide whether an abelian variety of dimension 2 is isogenous to the Jacobian variety of a curve. If the field of definition is algebraically closed, this problem is solved in the following way: Every abelian variety is isogenous to a principally polarized one. The principally polarized abelian variety has a positive divisor whose self-intersection number is 2. Then by a Theorem of Weil this divisor is either a curve of genus 2 or the sum of two positive divisors. In the first case the abelian variety is isogenous to the Jacobian variety of that curve.

If the field of definition is not algebraically closed, the problem is more complicated, because the isogeny mentioned above may not be defined over this field.

We consider the case where the field of definition of the abelian variety is the prime field $\mathbb{Z}/p\mathbb{Z}$.

THEOREM 1.2. *Let A be an abelian variety of dimension 2 over the prime field $k = \mathbb{Z}/p\mathbb{Z}$ whose algebra $\text{End}_k(A) \otimes \mathbb{Q}$ is a field, and let $f_A(T) = T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$ be the characteristic polynomial of the Frobenius endomorphism of A . We denote the integer $a_1^2 - 4a_2 + 8p$ by d .*

If (a) $(a_2 + 2p)^2 - 4pa_1^2$ is not a square in $\mathbb{Q}(\sqrt{d})$ and if (b) $\mathbb{Z}[a_1/2 + \sqrt{d}/2]$ is equal to the ring of integers in $\mathbb{Q}(\sqrt{d})$, then A is k -isogenous to the Jacobian variety of a curve over k of genus 2.

REMARKS. (i) The condition (a) of Theorem 1.2 is equivalent to the fact that the field $\text{End}_k(A) \otimes \mathbb{Q}$ is not a Galois extension of \mathbb{Q} . This is an immediate consequence of the following properties:

The field $\text{End}_k(A) \otimes \mathbb{Q}$ is equal to $\mathbb{Q}(\pi_A)$, the minimal polynomial of π_A is $f_A(T)$ which splits over $\mathbb{Q}(\sqrt{d})$ in a product $(T^2 - \lambda_1T + p)(T^2 - \lambda_2T + p)$. The product of the discriminants $\lambda_1^2 - 4p$ and $\lambda_2^2 - 4p$ equals $(a_2 + 2p)^2 - 4pa_1^2$.

(ii) The following example shows that the condition (a) of Theorem 1.2 is important: We take $p = 2, a_1 = 1, a_2 = -1$. Then Theorem 1.1 implies that the polynomial $T^4 + T^3 - T^2 + 2T + 4$ is equal to $f_A(T)$ of an abelian variety A over $\mathbb{Z}/2\mathbb{Z}$ of dimension 2. If we suppose that A is isogenous to the Jacobian variety of a curve C , then the zetafunction $\exp(\sum_{m=1}^{\infty} N_m T^m/m)$ of C is equal to

$$\frac{1 + T - T^2 + 2T^3 + 4T^4}{(1 - T)(1 - 2T)}.$$

The integers N_m are the number of points on C over extension fields of $\mathbb{Z}/2\mathbb{Z}$; in particular we get $0 \leq N_1 \leq N_2$. But in our example we evaluate $N_1 = 4$ and $N_2 = 2$. Hence A is not isogenous to a Jacobian variety. All the assumptions of Theorem 1.2 except condition (a) are fulfilled.

(iii) But on the other hand this important condition (a) of Theorem 1.2 is not a necessary condition: The curve $Y^2 = X^5 + X^4 + 2X^2 - X + 1$ over $\mathbb{Z}/5\mathbb{Z}$ has a zetafunction with $a_1 = 3$ and $a_2 = 4$. For this example $(a_2 + 2p)^2 - 4pa_1^2$ is equal to 16.

2. Background on Abelian Varieties

Let A be an abelian variety over the finite field k with q elements. We denote by $f_A(T)$ the characteristic polynomial of the Frobenius endomorphism π_A of A over k . This polynomial determines A up to k -isogeny, i.e. two abelian varieties A and B are k -isogenous if and only if $f_A(T)$ is equal to $f_B(T)$ ([T], Theorem 1). The group of k -homomorphisms of abelian varieties A and B and the ring of k -endomorphisms of A are denoted by $\text{Hom}_k(A, B)$ and $\text{End}_k(A)$. For a prime number l which is different from the characteristic p of k one considers the Tate module $T_l(A)$ of A .

The *Theorem of Tate* ([T], Main Theorem) states that the \mathbb{Z}_l -modules $\text{Hom}_k(A, B) \otimes \mathbb{Z}_l$ and $\text{Hom}_{\text{Gal}(\bar{k}/k)}(T_l(A), T_l(B))$ are canonically isomorphic. The elements of the second module are those homomorphisms φ_l of the \mathbb{Z}_l -modules $T_l(A)$ and $T_l(B)$ which satisfy $\varphi_l \circ (\pi_A)_l = (\pi_B)_l \circ \varphi_l$ where $(\pi_A)_l$ and $(\pi_B)_l$ are the corresponding Frobenius endomorphisms on $T_l(A)$ and $T_l(B)$.

For the prime number p one considers the Dieudonné module $M(A(p))$ of the p -divisible group $A(p)$ corresponding to A ([O], Section 3). $M(A(p))$ is a module over the ring $\mathfrak{a} = W(k)[F, V]$, where $W(k)$ is the ring of Witt vectors over k , F is the absolute Frobenius and V is the Verschiebung (translation).

Analogous to the l -adic case there is a canonical (contravariant) isomorphism from $\text{Hom}_k(A, B) \otimes \mathbb{Z}_p$ onto $\text{Hom}_{\mathfrak{a}}(M(B(p)), M(A(p)))$. If k is the prime field $\mathbb{Z}/p\mathbb{Z}$, then $W(k)$ is equal to \mathbb{Z}_p and F is just the Frobenius endomorphism $(\pi_A)_p$ on $M(A(p))$. Then $\text{Hom}_{\mathfrak{a}}(M(B(p)), M(A(p)))$ consists of those \mathbb{Z}_p -homomorphisms

which commute with $(\pi_A)_p$ and $(\pi_B)_p$. This easy characterization is the reason for the assumption on k in Theorem 1.2.

A classification of simple abelian varieties over k is given by the *Theorem of Honda-Tate* ([T-H], Théorème 1):

The assignment $A \mapsto \pi_A$ gives a one-to-one correspondence between simple abelian varieties over k (up to isogenies) and Weil numbers (these are algebraic integers whose conjugates have absolute complex value $q^{1/2}$). $\text{End}_k(A) \otimes \mathbb{Q}$ is a division algebra with center $\mathbb{Q}(\pi_A)$, it splits at each finite place prime to p , it does not split at any real place and its invariant at a place \mathfrak{p} over p is given by

$$\text{inv}_{\mathfrak{p}}(\text{End}_k(A) \otimes \mathbb{Q}) \equiv \frac{v_{\mathfrak{p}}(\pi_A)}{v_{\mathfrak{p}}(q)} \cdot [\mathbb{Q}(\pi_A)_{\mathfrak{p}} : \mathbb{Q}_{\mathfrak{p}}] \pmod{\mathbb{Z}}.$$

The dimension of A is equal to

$$\frac{1}{2}[\text{End}_k(A) \otimes \mathbb{Q} : \mathbb{Q}(\pi_A)]^{1/2} \cdot [\mathbb{Q}(\pi_A) : \mathbb{Q}].$$

From this we get immediately that the invariant at \mathfrak{p} equals $v_{\mathfrak{p}}(f_i(0))/v_{\mathfrak{p}}(q)$ where $f_i(T)$ is the irreducible monic divisor of $f_A(T)$ over \mathbb{Z}_p which corresponds to \mathfrak{p} .

The key for a proof of Theorem 1.2 is a *Theorem of Weil* ([W], Satz 2):

Let A be an abelian variety of dimension 2. Consider a positive divisor D on A whose self-intersection number (D, D) is 2. Then this divisor is either a curve of genus 2 or the sum of two positive divisors. In the first case A is isomorphic to the Jacobian variety of D , in the second case A is the product of two elliptic curves.

The self-intersection number of a divisor D on A can be evaluated by the *Riemann-Roch Theorem* ([M], III.16):

Let Φ_D be the homomorphism from A to the dual abelian variety \hat{A} , which assigns to $x \in A$ the point $\Phi_D(x)$ corresponding to the divisor class of $T_x^*D - D$. Let $\chi(D)$ be the Euler characteristic of the line bundle associated to D . These quantities satisfy: $\deg \Phi_D = \chi(D)^2$ and $2 \cdot \chi(D) = (D, D)$.

Divisors on A are closely related with “skew-symmetric” homomorphisms from A to \hat{A} :

For each prime number l ($l \neq p$) there is a non-degenerate bilinear mapping of \mathbb{Z}_l -modules $e_l^A: T_l(A) \times T_l(\hat{A}) \rightarrow \mathbb{Z}_l$ satisfying the following properties (c.f. [M], IV.20):

Let φ be a homomorphism from A to B with dual homomorphism $\hat{\varphi}: \hat{B} \rightarrow \hat{A}$, then $e_l^B(\varphi_1 x, y) = e_l^A(x, \hat{\varphi}_1 y)$.

If A is defined over the finite field k with q elements, then the Frobenius endomorphisms $(\pi_A)_l$ and $(\pi_{\hat{A}})_l$ on $T_l(\bar{H})$ and $T_l(\hat{A})$ are compatible with e_l^A by the formula $e_l^A((\pi_A)_l x, (\pi_{\hat{A}})_l y) = q \cdot e_l^A(x, y)$. To each homomorphism $\varphi: A \rightarrow \hat{A}$ one can associate a bilinear form $E_l^\varphi: T_l(A) \times T_l(A) \rightarrow \mathbb{Z}_l$ by $E_l^\varphi(x, y) = e_l^A(x, \varphi_1 y)$.

Hence a homomorphism $\varphi: A \rightarrow \hat{A}$ is defined over k if and only if $E_l^\varphi((\pi_A)_l x, (\pi_A)_l y) = q \cdot E_l^\varphi(x, y)$.

Conversely let E_l be a bilinear form on $T_l(A)$ which satisfies $E_l((\pi_A)_l x, (\pi_A)_l y) = q \cdot E_l(x, y)$, then there is a \mathbb{Z}_l -homomorphism φ_l from $T_l(A)$ to $T_l(\hat{A})$ which commutes with $(\pi_A)_l$ and $(\pi_{\hat{A}})_l$ such that $E_l(x, y) = E_l^A(x, \varphi_l y)$. By the Theorem of Tate φ_l can be approximated by k -homomorphisms from A to \hat{A} .

The corresponding statements are true for the prime number p if one takes the Dieudonné modules $M(A(p))$ and $M(\hat{A}(p))$; for details we refer to [O], Section 3.

These considerations can be used to construct a divisor on an abelian variety:

The bilinear form E_l^φ of a homomorphism $\varphi = \Phi_D$ is skew-symmetric. Conversely let $\varphi: A \rightarrow \hat{A}$ be a k -homomorphism such that the corresponding E_l^φ is skew-symmetric (skew-symmetric modulo l^N), then the divisor $D = (1 \times \varphi)^* P$ where P is a Poincaré divisor on $A \times \hat{A}$ satisfies $2 \cdot \varphi = \Phi_D$ ($2 \cdot \varphi \equiv \Phi_D \pmod{l^N}$). For a proof we refer to [M], IV. 20, Theorem 2 and [O], Proposition 1.15.

There is a Poincaré divisor which is defined over k , therefore the divisor D has also k as a field of definition.

We recall that a divisor D is defined over k , if D can be given locally by equations with coefficients in k . Another characterization is the following: D is defined over k if and only if $\sigma(D) = D$ for each automorphism σ of the Galois group of k (c.f. [R], Lemma 4, especially the last step in the proof).

3. Proof of Theorem 1.1

The theorem of Honda-Tate (c.f. §2) shows that the set of polynomials $f_A(T)$ belonging to abelian varieties A over k of dimension 2, whose algebra $\text{End}_k(A) \otimes \mathbb{Q}$ is a field, is equal to the set of irreducible monic polynomials $f(T)$ of degree 4, whose roots are Weil numbers and where in addition $v_p(f_i(0))/n$ is an integer for each irreducible monic divisor $f_i(T)$ of $f(T)$ over \mathbb{Q}_p .

LEMMA 3.1. $f(T)$ is an irreducible monic polynomial of degree 4 in $\mathbb{Z}[T]$, whose roots are Weil numbers, if and only if $f(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2$ with integers a_1 and a_2 satisfying:

- (a) $|a_1| < 4q^{1/2}$, $2|a_1|q^{1/2} - 2q < a_2 < a_1^2/4 + 2q$, and
- (b) $a_1^2 - 4a_2 + 8q$ is not a square in \mathbb{Z} .

Proof. Let $f(T)$ be an irreducible polynomial of degree 4 in $\mathbb{Z}[T]$, whose roots are Weil numbers. Since the roots are permuted by complex conjugation, they are of the form $\pi_1, q/\pi_1, \pi_2, q/\pi_2$. Hence $f(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2$ with integers a_1 and a_2 ; we get $|a_1| < 4q^{1/2}$.

The elements $\lambda_1 = \pi_1 + q/\pi_1$ and $\lambda_2 = \pi_2 + q/\pi_2$ are distinct real numbers and zeros of $T^2 + a_1 T + a_2 - 2q$, whose discriminant $a_1^2 - 4a_2 + 8q$ is positive; this yields $a_2 < a_1^2/4 + 2q$. From $f(T) = (T^2 - \lambda_1 T + q)(T^2 - \lambda_2 T + q)$ we see

that this discriminant is not a square in \mathbb{Z} , since otherwise $f(T)$ would be reducible in $\mathbb{Z}[T]$.

The formulas $|\lambda_1 - \lambda_2| + |\lambda_1 + \lambda_2| = 2 \cdot \max\{|\lambda_1|, |\lambda_2|\} < 4q^{1/2}$, $|\lambda_1 - \lambda_2|^2 = a_1^2 - 4a_2 + 8q$ and $|\lambda_1 + \lambda_2| = |a_1|$ give the inequality $a_2 > 2|a_1|q^{1/2} - 2q$.

Conversely let $f(T) = T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$ be a polynomial with properties (a) and (b). The inequalities in (a) show that the elements $\lambda_1 = -a_1/2 + (a_1^2/4 - a_2 + 2q)^{1/2}$ and $\lambda_2 = -a_1/2 - (a_1^2/4 - a_2 + 2q)^{1/2}$ are distinct real numbers with $|\lambda_1|, |\lambda_2| < 2q^{1/2}$. We also get the decomposition $f(T) = (T^2 - \lambda_1T + q)(T^2 - \lambda_2T + q)$.

Let $\pi_i, q/\pi_i$ be the zeros of $T^2 - \lambda_iT + q$, then easy calculations prove that $|\pi_i| = |q/\pi_i| = q^{1/2}$. Hence the roots of $f(T)$ are Weil numbers.

$f(T)$ is irreducible in $\mathbb{Z}[T]$, because $a_1^2 - 4a_2 + 8q$ is not a square in \mathbb{Z} . \square

LEMMA 3.2. *Let $f(T) = T^4 + a_1T^3 + a_2T^2 + a_1qT + q^2$ be a polynomial in $\mathbb{Z}[T]$. Then $v_p(f_i(0))/n$ is an integer for each irreducible monic divisor $f_i(T)$ of $f(T)$ over \mathbb{Q}_p if and only if one of the following conditions is satisfied:*

- (i) $v_p(a_1) = 0, v_p(a_2) \geq n/2$ and $(a_2 + 2q)^2 - 4qa_1^2$ is not a square in \mathbb{Z}_p ,
- (ii) $v_p(a_2) = 0$,
- (iii) $v_p(a_1) \geq n/2, v_p(a_2) \geq n$ and $f(T)$ has no root in \mathbb{Z}_p .

Proof. We consider the Newton polygon of the polynomial $f(T)$ over \mathbb{Q}_p . This polygon is the lower convex envelop of the points $(0, 2n)$, $(1, v_p(a_1) + n)$, $(2, v_p(a_2))$, $(3, v_p(a_1))$ and $(4, 0)$, and its shape leads to a decomposition of $f(T)$ over \mathbb{Q}_p (see e.g. [We], §3). We distinguish three cases (each case corresponds to a formal isogeny type of the p -divisible group of an abelian variety of dimension 2, c.f. [Ma]).

Case 1. The point $(3, v_p(a_1))$ is a vertex of the polygon:

This is equivalent to $v_p(a_1) < n/2$ and $v_p(a_2) > 2v_p(a_1)$. We get the decomposition $f(T) = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3)(T - \alpha_4)$ with $v_p(\alpha_1) = v_p(a_1)$ and $v_p(\alpha_4) = n - v_p(a_1)$. In addition the polynomials $T - \alpha_1$, $(T - \alpha_2)(T - \alpha_3)$ and $T - \alpha_4$ are in $\mathbb{Q}_p[T]$. Hence all the numbers $v_p(f_i(0))/n$ are integers if and only if $v_p(a_1) = 0, v_p(a_2) \geq n/2, (T - \alpha_2)(T - \alpha_3)$ is irreducible over \mathbb{Q}_p . The latter is equivalent to condition (i), because $f(T)$ is equal to a product $(T^2 - \lambda_1T + q)(T^2 - \lambda_2T + q)$ with $(\lambda_1^2 - 4q)(\lambda_2^2 - 4q) = (a_2 + 2q)^2 - 4qa_1^2$ (c.f. the proof of Lemma 3.1).

Case 2. The point $(3, v_p(a_1))$ is not a vertex, but $(2, v_p(a_2))$ is a vertex of the polygon:

This is equivalent to $v_p(a_2) < n$ and $2v_p(a_1) \geq v_p(a_2)$.

Then $f(T)$ can be decomposed in $(T - \alpha_1)(T - \alpha_2)(T - \alpha_3)(T - \alpha_4)$ with $v_p(\alpha_1) = v_p(\alpha_2) = v_p(a_2)/2$ and $v_p(\alpha_3) = v_p(\alpha_4) = n - v_p(a_2)/2$. The two quadratic

polynomials $(T - \alpha_1)(T - \alpha_2)$ and $(T - \alpha_3)(T - \alpha_4)$ are in $\mathbb{Q}_p[T]$.

Here we get that all the numbers $v_p(f_i(0))/n$ are integers if and only if $v_p(a_2) = 0$.

Case 3. The Newton polygon of $f(T)$ is a straight line:

This is equivalent to $v_p(a_1) \geq n/2$ and $v_p(a_2) \geq n$. We get $f(T) = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3)(T - \alpha_4)$ with $v_p(\alpha_i) = n/2$. In this case the additional condition is that $f(T)$ has no root in \mathbb{Z}_p . \square

Lemma 3.1 and Lemma 3.2 give a proof of Theorem 1.1.

4. Some Lemmas

The basic idea of the proof of Theorem 1.2 is to construct a positive divisor on an abelian variety with self-intersection number 2 which is defined over the field of definition of the abelian variety. We present some lemmas which will lead to the construction of such a divisor.

From now on let k denote the prime field $\mathbb{Z}/p\mathbb{Z}$.

The lemmas are true for an arbitrary finite field, whenever the prime number p is not involved, but for sake of simplicity we do not distinguish these cases.

LEMMA 4.1. *Let A be an abelian variety over k of dimension g . For a given basis on the Tate module $T_l(A)$ (the Dieudonné module $M(A(p))$ if $l = p$) let F_l be the matrix of the Frobenius endomorphism $(\pi_A)_l$.*

Suppose M is a non-singular $(2g \times 2g)$ -matrix with coefficients in \mathbb{Z}_l such that the coefficients of $M^{-1}F_lM$ are also in \mathbb{Z}_l . Then there are a k -isogeny $\varphi: B \rightarrow A$ ($\varphi: A \rightarrow B$ if $l = p$) of degree $l^{v_l(\det M)}$ and a basis of $T_l(B)$ ($M(B(p))$ if $l = p$) such that φ_l has the matrix M . And the matrix $M^{-1}F_lM$ corresponds to the Frobenius endomorphism $(\pi_B)_l$.

Proof. We consider the finite subgroup $U = M \cdot T_l(A)/l^{v_l(\det M)} \cdot T_l(A)$, if $l \neq p$.

Otherwise let U be the finite commutative group scheme corresponding to the \mathfrak{a} -module $M(A(p))/M \cdot M(A(p))$ (c.f. [O], Theorem 3.14). Since the coefficients of $M^{-1}F_lM$ are in \mathbb{Z}_l , the canonical isogenies $A \rightarrow A/U$ and $A/U \rightarrow A$ are defined over k . The isogeny $A/U \rightarrow A$ ($A \rightarrow A/U$ if $l = p$) fulfills the properties of the lemma. \square

With the next lemma we can construct a divisor on an abelian variety with a given local behaviour.

LEMMA 4.2. *Let A be an abelian variety over k of dimension 2. We assume that the characteristic polynomial $f_A(T)$ is irreducible over \mathbb{Z} . Suppose that S is a finite set of prime numbers. Then we get a k -isogeny $B \rightarrow A$ where B satisfies the following properties: There are a divisor D on B which is defined over k and a k -homomorphism $\varphi: B \rightarrow \hat{B}$ whose degree is prime to S , such that $\Phi_D = 2 \cdot \varphi$.*

Proof. We may assume that 2 is contained in S .

(i) Suppose that B is an abelian variety over k with the following properties:

For each $l \in S$ there is a \mathbb{Z}_l -homomorphism $f_l: T_l(B) \rightarrow T_l(\hat{B})$ ($M(\hat{B}(p)) \rightarrow M(B(p))$ if $l = p$) with

- (a) $f_l \circ (\pi_B)_l = (\pi_{\hat{B}})_l \circ f_l$ ($f_p \circ (\pi_B)_p = (\pi_B)_p \circ f_p$ if $l = p$),
- (b) the bilinear form $(x, y) \mapsto e_l^B(x, f_l y)$ is skew-symmetric,
- (c) $\det(f_l)$ is a unit in \mathbb{Z}_l .

Then by the Theorem of Tate (c.f. §2) we get for each $l \in S$ a k -homomorphism $\varphi^{(l)}: B \rightarrow \hat{B}$ such that $\varphi^{(l)} \equiv f_l \pmod{l^2}$. The bilinear form $E_l^{\varphi^{(l)}}$ is skew-symmetric modulo l^2 . Thus there is a divisor $D^{(l)}$ which is defined over k such that $2 \cdot \varphi^{(l)} \equiv \Phi_{D^{(l)}} \pmod{l^2}$ (c.f. §2).

Now we take

$$D = \sum_{l \in S} \left(\prod_{\substack{s \in S \\ s \neq l}} s^2 \right) \cdot D^{(l)},$$

D is defined over k and satisfies

$$\Phi_D \equiv 2 \cdot \left(\prod_{\substack{s \in S \\ s \neq l}} s^2 \right) \cdot \varphi^{(l)} \pmod{l^2} \quad \text{for each } l \in S.$$

Since $2 \in S$, we see that there is a k -homomorphism $\varphi: B \rightarrow \hat{B}$ with $\Phi_D = 2 \cdot \varphi$. In addition the degree of φ is prime to S .

(ii) We have to find an abelian variety B and \mathbb{Z}_l -homomorphisms f_l with properties (a), (b) and (c):

In terms of matrices we have to find matrices M_l with coefficients in \mathbb{Z}_l with (c.f. the properties of e_l^B)

- (ã) $F_l^T M_l F_l = p \cdot M_l$, where F_l is the matrix to $(\pi_B)_l$,
- (b̃) M_l is skew-symmetric,
- (c̃) $\det M_l$ is a unit in \mathbb{Z}_l .

If F_l on $T_l(A)$ ($M(A(p))$ if $l = p$) has a “simple” form, we can take $B = A$ and give M_l directly. Otherwise we change A to an abelian variety B over k by applying Lemma 4.1, this moves F_l to a matrix of the form $M^{-1} F_l M$. Since the degree of the isogeny $A \rightarrow B$ in Lemma 4.1 is a power of l , the Tate modules (Dieudonné module) at other prime numbers are not changed. We apply this procedure for each $l \in S$, hence we get an abelian variety B over k of dimension 2, where for each $l \in S$ the matrix F_l has a “simple” form.

We distinguish several cases which depend on the factorization of $f_A(T)$ over \mathbb{Z}_l . In each case we give a “simple” form for F_l and a matrix M_l with properties (ã), (b̃) and (c̃). The details are easy to verify.

Case 1. $f_A(T) = (T - \alpha)(T - p/\alpha)(T - \beta)(T - p/\beta)$ with $\alpha, \beta \in \mathbb{Z}_l$:

$$F_l = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & p/\alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & p/\beta \end{bmatrix}, \quad M_l = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Case 2. $f_A(T) = (T - \alpha)(T - p/\alpha)(T^2 - \lambda T + p)$ with $\alpha, \lambda \in \mathbb{Z}_l$:

$$F_l = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & p/\alpha & 0 & 0 \\ 0 & 0 & 0 & -p \\ 0 & 0 & 1 & \lambda \end{bmatrix}, \quad M_l = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Case 3. $f_A(T) = (T^2 - \lambda_1 T + p)(T^2 - \lambda_2 T + p)$ with $\lambda_1, \lambda_2 \in \mathbb{Z}_l$:

$$F_l = \begin{bmatrix} 0 & -p & 0 & 0 \\ 1 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & -p \\ 0 & 0 & 1 & \lambda_2 \end{bmatrix}, \quad M_l = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Case 4. $f_A(T) = (T^2 + \mu_1 T + v_1)(T^2 + \mu_2 T + v_2)$ with $\mu_1, \mu_2, v_1, v_2 \in \mathbb{Z}_l$, $v_1 \neq p, v_2 \neq p, v_1 \cdot v_2 = p^2, \mu_1 \cdot p = \mu_2 \cdot v_1$.

We assume that $(v_1/p) \in \mathbb{Z}_l$.

$$F_l = \begin{bmatrix} 0 & -v_1/p & 0 & 0 \\ p & -\mu_1 & 0 & 0 \\ 0 & 0 & 0 & -v_2 \\ 0 & 0 & 1 & -\mu_2 \end{bmatrix}, \quad M_l = \begin{bmatrix} 0 & 0 & 1 & -\mu_2 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ \mu_2 & -1 & 0 & 0 \end{bmatrix}.$$

Case 5. $f_A(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 p T + p^2$ is irreducible over \mathbb{Z}_l :

$$F_l = \begin{bmatrix} 0 & 0 & 0 & -p \\ p & 0 & 0 & -a_1 p \\ 0 & 1 & 0 & -a_2 \\ 0 & 0 & 1 & -a_1 \end{bmatrix}, \quad M_l = \begin{bmatrix} 0 & 0 & 1 & -a_1 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ a_1 & -1 & 0 & 0 \end{bmatrix}.$$

This proves the lemma. □

The next lemma describes the decomposition into irreducible components of the Tate module and of a bilinear form on it.

Let A be an abelian variety over k . For a prime number l we consider the factorization $f_A(T) = \prod_i f_i(T)$ over \mathbb{Z}_l with irreducible polynomials $f_i(T)$.

For each $f_i(T)$ we define $(\tau f_i)(T) = (1/f_i(0))f_i(p/T)T^{\deg f_i(T)}$. Since all the roots of $f_A(T)$ are Weil numbers, $(\tau f_i)(T)$ is also an irreducible divisor of $f_A(T)$.

It is not difficult to prove:

LEMMA 4.3. *Let l ($l \neq p$) be a prime number which does not divide the discriminant of $f_A(T)$.*

There is a decomposition of the Tate module $T_l(A) = \bigoplus_i T_l(A)(f_i)$ as a $\mathbb{Z}_l[(\pi_A)_l]$ -module where each $T_l(A)(f_i)$ is isomorphic to $\mathbb{Z}_l[T]/f_i(T)$. Let $E_l: T_l(A) \times T_l(A) \rightarrow \mathbb{Z}_l$ be a skew-symmetric bilinear form which satisfies $E_l((\pi_A)_l x, (\pi_A)_l y) = p \cdot E_l(x, y)$ and $\det E_l \neq 0$. Then we get:

- (i) $E_l | T_l(A)(f_i) \times T_l(A)(f_j) = 0$ if $f_j(T) \neq (\tau f_i)(T)$,
- (ii) $E_l | T_l(A)(f_i) \times T_l(A)(\tau f_i) = l^{m_i} \cdot E_l(f_i)$ where $m_i \geq 0$ and $E_l(f_i)$ is a bilinear form over \mathbb{Z}_l on $T_l(A)(f_i) \times T_l(A)(\tau f_i)$ with $v_l(\det E_l(f_i)) = 0$.
- (iii) $v_l(\det E_l) = \sum_i m_i \cdot \deg f_i(T)$. □

We want to use Lemma 4.3 to change a given divisor. Let D be a divisor on an abelian variety A and let $\psi: B \rightarrow A$ be an isogeny, then the definition of the dual isogeny $\hat{\psi}: \hat{A} \rightarrow \hat{B}$ yields that $\hat{\psi} \circ \Phi_D \circ \psi = \Phi_{\psi^*D}$. With the next lemma we find suitable isogenies for that procedure.

LEMMA 4.4. *Let A be an abelian variety over k . We consider a divisor D on A which is defined over k and a k -homomorphism $\varphi: A \rightarrow \hat{A}$ with $2 \cdot \varphi = \Phi_D$.*

For a prime number l ($l \neq p$) which does not divide the discriminant of $f_A(T)$ we fix an irreducible divisor $f_i(T)$ of $f_A(T)$ over \mathbb{Z}_l . Then there is a k -isogeny $\psi: B \rightarrow A$ whose degree is a power of l such that the bilinear forms E_l^φ and $E_l^{\hat{\psi} \circ \varphi \circ \psi}$ satisfy:

- (i) $E_l^{\hat{\psi} \circ \varphi \circ \psi} | T_l(B)(f_j) \times T_l(B)(\tau f_j) \cong E_l^\varphi | T_l(A)(f_j) \times T_l(A)(\tau f_j)$, if $f_j(T) \neq f_i(T)$ and $f_j(T) \neq (\tau f_i)(T)$.
- (ii) $E_l^{\hat{\psi} \circ \varphi \circ \psi} | T_l(B)(f_i) \times T_l(B)(\tau f_i) \cong l^\delta \cdot E_l^\varphi | T_l(A)(f_i) \times T_l(A)(\tau f_i)$, where $\delta = 1$ if $(\tau f_i)(T) \neq f_i(T)$ and $\delta = 2$ if $(\tau f_i)(T) = f_i(T)$.

Proof. In view of the decomposition $T_l(A) = \bigoplus_j T_l(A)(f_j)$ of Lemma 4.3 we consider the diagonal matrix M which describes the identity on $T_l(A)(f_j)$ (if $f_j(T) \neq f_i(T)$) and the multiplication by l on $T_l(A)(f_i)$.

If F_l is a matrix of $(\pi_A)_l$ respecting the decomposition of $T_l(A)$, we get $M^{-1}F_lM = F_l$. Therefore Lemma 4.1 yields a k -isogeny $\psi: B \rightarrow A$ such that ψ_l is given by M .

Let M^φ be the matrix of the bilinear form E_l^φ , then $M^T M^\varphi M$ corresponds to $E_l^{\hat{\psi} \circ \varphi \circ \psi}$. The evaluation of the matrix multiplication proves the lemma. □

With Lemma 4.4 we try to change a k -homomorphism $\varphi: A \rightarrow \hat{A}$ by a k -isogeny $\psi: B \rightarrow A$ such that the new bilinear form $E_l^{\hat{\psi} \circ \varphi \circ \psi}$ has the same value l^m

on each part $T_l(B)(f_i) \times T_l(B)(\tau f_i)$ (c.f. Lemma 4.3). If we succeed, then $\hat{\psi} \circ \varphi \circ \psi$ is of the form $l^m \cdot \tilde{\varphi}$, where $\tilde{\varphi}: B \rightarrow \hat{B}$ is a k -homomorphism whose degree is prime to l .

Only those divisors $f_i(T)$ of $f_A(T)$ with $(\tau f_i)(T) = f_i(T)$ might cause some trouble, in all other cases we can take $\delta = 1$ in Lemma 4.4. For two-dimensional abelian varieties a case-by-case examination of the possible decomposition of $f_A(T)$ (like in the proof of Lemma 4.2) yields the following:

LEMMA 4.5. *Let A be an abelian variety over k of dimension 2, and let $\varphi: A \rightarrow \hat{A}$ be a k -homomorphism with $2 \cdot \varphi = \Phi_D$ for a divisor D on A . For a prime number l ($l \neq p$) which does not divide the discriminant of $f_A(T)$ we consider the decomposition in irreducible factors $f_A(T) = \prod_i f_i(T)$ over \mathbb{Z}_l .*

If (i) the decomposition is different from $(T^2 - \lambda_1 T + p)(T^2 - \lambda_2 T + p)$ or if (ii) the decomposition is $(T^2 - \lambda_1 T + p)(T^2 - \lambda_2 T + p)$ and in addition the matrix of E_l^φ is of the form

$$\begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & f \\ 0 & 0 & -f & 0 \end{bmatrix}$$

such that $v_l(a) - v_l(f)$ is an even integer, then we get a k -isogeny $\psi: B \rightarrow A$, whose degree is a power of l , and a k -homomorphism $\tilde{\varphi}: B \rightarrow \hat{B}$, whose degree is prime to l , with $\hat{\psi} \circ \varphi \circ \psi = l^m \cdot \tilde{\varphi}$. □

We want to give an example:

Suppose $f_A(T) = (T^2 - \lambda T + p)(T - \alpha)(T - (p/\alpha))$ is the decomposition in irreducible factors. Then there is a basis of $T_l(A)$ such that the Frobenius endomorphism $(\pi_A)_l$ is given by

$$F_l = \begin{bmatrix} 0 & -p & 0 & 0 \\ 1 & \lambda & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & p/\alpha \end{bmatrix}.$$

Let

$$M_l^\varphi = \begin{bmatrix} 0 & l & 0 & 0 \\ -l & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

be the matrix of $\varphi: A \rightarrow \hat{A}$. Following Lemma 4.4 we take

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & l & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and find a k -isogeny $\psi: B \rightarrow A$ with

$$M \hat{\psi} \circ \varphi \circ \psi = M^T M_l^\varphi M = l \cdot \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Hence $\hat{\psi} \circ \varphi \circ \psi = l \cdot \tilde{\varphi}$ where the degree of $\tilde{\varphi}: B \rightarrow \hat{B}$ is not divisible by l .

On the other hand if the difference $v_l(a) - v_l(f)$ in Lemma 4.5(ii) is odd, there is no way to find a k -homomorphism $\tilde{\varphi}$ with this procedure. Before we can apply Lemma 4.5, we have to change this difference to an even number by a different method.

LEMMA 4.6. *Let A be an abelian variety over k with an irreducible polynomial $f_A(T)$ over \mathbb{Z} . We consider a divisor D on A over k and a k -homomorphism $\varphi: A \rightarrow \hat{A}$ with $2 \cdot \varphi = \Phi_D$. Let $\varepsilon \in \text{End}_k(A)$, then we get:*

- (i) *Then there is a divisor D_ε on A over k with $2 \cdot \varphi \circ \varepsilon = \Phi_{D_\varepsilon}$ if and only if $\varepsilon \in \mathbb{Q}(\pi_A + (p/\pi_A))$.*
- (ii) *If $\varepsilon \in \mathbb{Q}(\pi_A + (p/\pi_A))$, then the Euler characteristic $\chi(D_\varepsilon)$ of D_ε is equal to $N_{\mathbb{Q}(\pi_A + p/\pi_A)/\mathbb{Q}}(\varepsilon) \cdot \chi(D)$.*

Proof. (i) Let $l (l \neq p)$ be a prime number. There exists a divisor D_ε on A over k with $\Phi_{D_\varepsilon} = 2 \cdot \varphi \circ \varepsilon$ if and only if the bilinear form $E_l^{\varphi \circ \varepsilon}$ is skew-symmetric (c.f. §2). The endomorphism ε is a polynomial $g(\pi_A)$ in π_A , because $f_A(T)$ is irreducible over \mathbb{Z} . Since E_l^φ is skew-symmetric and defined over k by assumption, the form $E_l^{\varphi \circ \varepsilon}$ is also skew-symmetric if and only if $g(\pi_A) = g(p/\pi_A)$. The latter condition is equivalent to $\varepsilon \in \mathbb{Q}(\pi_A + (p/\pi_A))$.

(ii) Since the degree of ε is equal to the norm $N_{\mathbb{Q}(\pi_A)/\mathbb{Q}}(\varepsilon)$, the Riemann-Roch Theorem implies $\chi(D_\varepsilon)^2 = (N_{\mathbb{Q}(\pi_A + p/\pi_A)/\mathbb{Q}}(\varepsilon) \cdot \chi(D))^2$. The two functions $\chi(D_\varepsilon)$ and $N_{\mathbb{Q}(\pi_A + p/\pi_A)/\mathbb{Q}}(\varepsilon)$ are homogenous polynomials in ε . This yields the formula for $\chi(D_\varepsilon)$. □

Let $l (l \neq p)$ be a prime number where the polynomial $f_A(T)$ has the decomposition $(T^2 - \lambda_1 T + p)(T^2 - \lambda_2 T + p)$ over \mathbb{Z}_l . The difference $v_l(a) - v_l(f)$ (c.f. Lemma 4.5(ii)) of a k -homomorphism $\varphi: A \rightarrow \hat{A}$ may be odd.

If we find an endomorphism $\varepsilon \in \mathbb{Q}(\pi_A + (p/\pi_A))$ whose norm is exactly divisible by an odd power of l , then $\varphi \circ \varepsilon$ satisfies condition (ii) of Lemma 4.5, i.e. the corresponding difference is even. Of course the degree of $\varphi \circ \varepsilon$ should not contain new prime numbers where Lemma 4.5 is not applicable. The existence of ε is guaranteed by the next lemma.

LEMMA 4.7. *Consider an abelian variety A which satisfies the assumptions of Theorem 1.2. Let S be a finite set of prime numbers and in addition let l be a prime number ($l \neq 2$, $l \neq p$, $l \notin S$) such that the decomposition of $f_A(T)$ in irreducible factors over \mathbb{Z}_l is equal to $(T^2 - \lambda_1 T + p)(T^2 - \lambda_2 T + p)$.*

Then there is an endomorphism $\varepsilon \in \text{End}_k(A) \cap \mathbb{Q}(\pi_A + (p/\pi_A))$ whose norm $N_{\mathbb{Q}(\pi_A + p/\pi_A)/\mathbb{Q}}(\varepsilon)$ is prime to S and equal to $l \cdot (\prod_i p_i) \cdot a^2$, where a is an integer and where p_i are prime numbers such that $f_A(T)$ has a root in \mathbb{Z}_{p_i} .

Proof. Like in Theorem 1.2 we denote the integer $a_1^2 - 4a_2 + 8p$ by d , let in addition $e = (a_2 + 2p)^2 - 4pa_1^2$. Then $\mathbb{Q}(\pi_A + (p/\pi_A))$ is equal to $\mathbb{Q}(\sqrt{d})$. By assumption (a) of Theorem 1.2 the integer e is not a square in $\mathbb{Q}(\sqrt{d})$. A consequence of assumption (b) is that the ring of integers in $\mathbb{Q}(\sqrt{d})$ is equal to $\text{End}_k(A) \cap \mathbb{Q}(\pi_A + (p/\pi_A))$.

In view of these remarks the problem can be reduced to find an element in $\mathbb{Q}(\sqrt{d})$ whose norm is $l \cdot (\prod_i p_i)$.

Let d_0 and e_0 be the squarefree parts of the positive integers d and e .

If a prime number p_i satisfies $\left(\frac{d_0}{p_i}\right) = 1$, then $f_A(T)$ is equal to $(T^2 - \lambda_1 T + p)(T^2 - \lambda_2 T + p)$ over \mathbb{Z}_{p_i} .

Since $e = (\lambda_1^2 - 4p)(\lambda_2^2 - 4p)$, the additional condition $\left(\frac{e_0}{p_i}\right) = -1$ yields that one of the two quadratic polynomials splits over \mathbb{Z}_{p_i} . The prime number l satisfies $\left(\frac{d_0}{l}\right) = \left(\frac{e_0}{l}\right) = 1$.

Let $d_0 = q_1 \cdots q_r$ be the decomposition in prime factors. Since e is not a square in $\mathbb{Q}(\sqrt{d})$, e_0 is different from 1 and d_0 .

If e_0 is not a divisor of d_0 , we choose a prime number p_1 with the following conditions:

$$p_1 \equiv l \pmod{4}, \quad \left(\frac{q_j}{p_1}\right) = \left(\frac{q_j}{l}\right) \quad \text{for } j = 1, \dots, r, \quad \left(\frac{e_0}{p_1}\right) = -1.$$

Since these conditions are independent, there are infinitely many p_1 satisfying them. We get $\left(\frac{d_0}{p_1}\right) = 1$ and $\left(\frac{e_0}{p_1}\right) = -1$. Using the Hilbert symbols it is not difficult to show that $l \cdot p_1$ is norm of an element in $\mathbb{Q}(\sqrt{d})$.

If e_0 is a divisor of d_0 , we may assume that $e_0 = q_1 \cdots q_s$ with $s < r$. Now we choose prime numbers p_1 and p_2 with the conditions:

$$p_1 \equiv l \pmod{4}, \quad \left(\frac{q_j}{p_1}\right) = \left(\frac{q_j}{l}\right) \quad \text{for } j = 2, \dots, r-1,$$

$$\left(\frac{q_j}{p_1}\right) = -\left(\frac{q_j}{l}\right) \quad \text{for } j = 1 \text{ and } r,$$

$$p_2 \equiv 1 \pmod{4}, \quad \left(\frac{q_j}{p_2}\right) = 1 \quad \text{for } j = 2, \dots, r-1,$$

$$\left(\frac{q_j}{p_2}\right) = -1 \quad \text{for } j = 1 \text{ and } r.$$

There are infinitely many p_1 and p_2 , and they satisfy

$$\left(\frac{d_0}{p_1}\right) = \left(\frac{d_0}{p_2}\right) = 1 \quad \text{and} \quad \left(\frac{e_0}{p_1}\right) = \left(\frac{e_0}{p_2}\right) = -1.$$

The calculation of the Hilbert symbols shows that $l \cdot p_1 \cdot p_2$ is norm of an element in $\mathbb{Q}(\sqrt{d})$. □

5. Proof of Theorem 1.2

Let again k be the prime field with p elements.

Step 1. We choose a finite set S of prime numbers containing $2, p$ and all the divisors of the discriminant of $f_A(T)$.

Applying Lemma 4.2 there is a k -isogeny $A_1 \rightarrow A$, a divisor D_1 on A_1 over k and a k -homomorphism $\varphi_1: A_1 \rightarrow \hat{A}_1$, such that $2 \cdot \varphi_1 = \Phi_{D_1}$ and $\deg \varphi_1$ is prime to S .

We may assume that $\chi(D_1) > 0$, because otherwise we change φ_1 by an endomorphism ε whose norm is negative (c.f. Lemma 4.6).

Step 2. Each prime divisor of $\deg \varphi_1$ does not divide the discriminant of $f_A(T)$. The only prime numbers l which do not satisfy the assumptions of Lemma 4.5 are those where $f_A(T)$ has the decomposition $(T^2 - \lambda_1 T + p)(t^2 - \lambda_2 T + p)$ over \mathbb{Z}_l and where $v_l(\deg \varphi_1) \equiv 2 \pmod{4}$ (i.e. the difference $v_l(a) - v_l(f)$ in Lemma 4.5(ii) is odd). For each l_i ($i = 1, \dots, r$) with these conditions we find by Lemma 4.7 an endomorphism $\varepsilon_i \in \text{End}_k(A_1) \cap \mathbb{Q}(\pi_A + (p/\pi_A))$ with norm $N_{\mathbb{Q}(\pi_A + p/\pi_A)/\mathbb{Q}}(\varepsilon_i) = l_i \cdot (\prod_j p_{ij}) \cdot a_i^2$, where $f_A(T)$ has a zero in $\mathbb{Z}_{p_{ij}}$. We apply Lemma 4.6 and get a k -homomorphism $\tilde{\varphi}_1 = \varphi_1 \circ \varepsilon_1 \circ \cdots \circ \varepsilon_r$ and a divisor \tilde{D}_1 on

A_1 over k with $2 \cdot \tilde{\varphi}_1 = \Phi_{\tilde{D}_1}$, such that $\deg \tilde{\varphi}_1$ contains only prime numbers for which Lemma 4.5 is applicable.

Step 3. Let l_1 be a prime divisor of $\deg \tilde{\varphi}_1$. By Lemma 4.5 there is a k -isogeny $\psi_1: A_2 \rightarrow A_1$, whose degree is a power of l_1 , such that $\hat{\psi}_1 \circ \tilde{\varphi}_1 \circ \psi_1 = l_1^{m_1} \cdot \varphi_2$, where the degree of the k -homomorphism $\varphi_2: A_2 \rightarrow \hat{A}_2$ is not divisible by l_1 .

In addition $2 \cdot \varphi_2 = \Phi_{D_2}$, where D_2 is a divisor on A_2 over k with $\chi(D_2) > 0$ (c.f. §2 and [M], III. 12, Theorem 2).

Since $\deg \psi_1$ and $\deg \hat{\psi}_1$ are powers of l_1 , nothing is changed at other prime numbers. Then we take the next prime divisor l_2 of $\deg \varphi_2$ and repeat the same procedure.

Finally we get a k -isogeny $\psi: B \rightarrow A_1$ ($\psi = \psi_s \circ \dots \circ \psi_1$), a divisor E on B over k and a k -homomorphism $\varphi: B \rightarrow \hat{B}$, such that $2 \cdot \varphi = \Phi_E$ and $\deg \varphi = 1$.

Step 4. Since $2 \cdot \varphi = \Phi_E$, there is a divisor \tilde{E} on B with $2 \cdot \tilde{E} \cong E$ and $\varphi = \Phi_{\tilde{E}}$ ([M], IV. 23, Theorem 3). With the Riemann-Roch Theorem we evaluate: $(\tilde{E}, \tilde{E}) = 2 \cdot \chi(\tilde{E}) = 2$.

Unfortunately the divisor \tilde{E} may not be defined over k .

Without loss of generality we assume that \tilde{E} is positive (either \tilde{E} or $-\tilde{E}$ is ample, because $\chi(\tilde{E}) = 1$).

Let σ be the generator of the Galois group $\text{Gal}(\bar{k}/k)$. The mapping $\text{Gal}(\bar{k}/k) \rightarrow \text{Pic}^0(B) = \hat{B}$ with $\sigma^m \mapsto \overline{\sigma^m \tilde{E} - \tilde{E}}$ is a 1-cocycle, because $2 \cdot (\sigma \tilde{E} - \tilde{E}) \cong \sigma E - E \cong 0$.

Since $H^1(\text{Gal}(\bar{k}/k), \hat{B}) = 1$ (c.f. [L]), there is a $\hat{b} \in \hat{B}$ with $\overline{\sigma \tilde{E} - \tilde{E}} = \hat{b} - \sigma \hat{b}$. We choose $b \in B$ with $\hat{b} = \overline{T_b^* \tilde{E} - \tilde{E}}$.

Let D be the divisor $T_b^* \tilde{E}$, then we get $\sigma D \cong D$.

This implies $\sigma D = D$, because D is positive with $\chi(D) = 1$. Hence D is defined over k and $(D, D) = 2$ (c.f. §2).

In view of Weil's Theorem (c.f. §2) D is either a curve of genus 2 or the sum of two elliptic curves.

In the second case the abelian variety A is isogenous over the quadratic extension of k to the product of two elliptic curves. But then the reducibility of the characteristic polynomial of π_A^2 yields that the integer $(a_2 + 2p)^2 - 4pa_1^2$ is a square in \mathbb{Z} .

Hence the assumptions of Theorem 1.2 imply that A is k -isogenous to the Jacobian variety of the curve D .

References

- [H-N] Hayashida, T.-Nishi, M.: Existence of curves of genus two on a product of two elliptic curves, *J. Math. Soc. Japan*, Vol. 17 (1965), 1–16.
- [L] Lang, S.: Algebraic groups over finite fields, *Amer. J. of Math.* 78 (1956), 555–563.

- [Ma] Manin, Y. I.: The Theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surv.*, Vol. 18 (1963), 1–83.
- [M] Mumford, D.: *Abelian Varieties*, Second Edition, Oxford Univ. Press, Oxford (1974).
- [O] Oda T.: The first de Rham cohomology group and Dieudonné modules, *Ann. scient. Éc. Norm. Sup.*, (4), t. 2 (1969), 63–135.
- [R] Ramanujam, C. P.: *The Theorem of Tate*, Appendix I in [M].
- [T] Tate, J.: Endomorphisms of abelian varieties over finite fields, *Invent. Math.*, Vol. 2 (1966), 134–144.
- [T-H] Tate, J.: Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), *Sem. Bourbaki* 358, 1968–1969.
- [Wa] Waterhouse, W.C.: Abelian varieties over finite fields, *Ann. scient. Éc. Norm. Sup.*, (4), t. 2 (1969), 521–560.
- [W] Weil, A.: Zum Beweis des Torellischen Satzes, *Nachr. Akad. Wiss Göttingen, Math.-Phys. Kl.* (1957), 33–53.
- [We] Weiss, E.: *Algebraic Number Theory*, McGraw-Hill, New-York (1963).