Finite Fields and Their Applications 29 (2014) 132–150

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Finite group subschemes of abelian varieties over finite fields

Sergey Rybakov [1]

Poncelet Laboratory (UMI 2615 of CNRS and Independent University of Moscow), Institute for Information Transmission Problems of the Russian Academy of Sciences, Laboratory of Algebraic Geometry, NRU HSE, 7 Vavilova Str., Moscow, 117312, Russia

ARTICLE INFO

Article history:
Received 2 October 2012
Received in revised form 21 October 2013
Accepted 1 April 2014
Available online xxxx
Communicated by Michael Tsfasman

MSC:
14K99
14G05
14G15

Keywords:
Abelian variety
Finite field
Weil polynomial
Newton polygon
Young polygon

ABSTRACT

Let A be an abelian variety over a finite field k. The k-isogeny class of A is uniquely determined by the Weil polynomial f_A. For a given prime number $\ell \neq \operatorname{char} k$ we give a classification of group schemes $B[\ell]$, where B runs through the isogeny class, in terms of certain Newton polygons associated to f_A. As an application we classify zeta functions of Kummer surfaces over k.

E-mail addresses: rybakov@mccme.ru, rybakov.sergey@gmail.com.

[1] The author is partially supported by AG Laboratory GU-HSE, RF government grant, ag. 11 11.G34.31.0023, and by RFBR grants Nos. 11-01-12072, 11-01-00395 and 10-01-93110-CNRSLa.

http://dx.doi.org/10.1016/j.ffa.2014.04.001
1071-5797/

1. Introduction

Throughout this paper k is a finite field $\mathbb{F}_q$ of characteristic p, and k^{alg} is an algebraic closure of k. Let A be an abelian variety of dimension g over k. Let $A[m]$ be the group subscheme of A annihilated by a natural number m. Fix a prime number $\ell \neq p$. We say that $A[\ell]$ is the *ℓ-torsion of A*. In this paper we classify ℓ-torsion of abelian varieties in two cases: when the Weil polynomial is separable, and for abelian surfaces. This result is similar to the classification of groups of k-points $A(k)$ (see [9]). These two problems are closely related, but the former one seems to be easier.

Denote by $A_m = A[m](k^{alg})$ the kernel of multiplication by m in $A(k^{alg})$. Let $T_\ell(A) = \varprojlim A_{\ell^r}$ be the ℓ-th Tate module of A, and let $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the corresponding vector space over $\mathbb{Q}_\ell$. Then $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. The Frobenius endomorphism F of A acts on the Tate module by a semisimple linear transformation, which we also denote by $F : T_\ell(A) \to T_\ell(A)$. The characteristic polynomial

$$f_A(t) = \det(t - F)$$

is called *the Weil polynomial of A*. It is a monic polynomial of degree $2g$ with rational integer coefficients independent of the choice of prime ℓ. It is well known that for isogenous varieties A and B we have $f_A(t) = f_B(t)$. Tate proved that the isogeny class of an abelian variety is determined by its characteristic polynomial, that is $f_A(t) = f_B(t)$ implies that A is isogenous to B [10].

This gives a nice description of isogeny classes of abelian varieties over k in terms of Weil polynomials. It seems natural to consider classification problems concerning abelian varieties inside a given isogeny class. Our goal is to describe the Frobenius action on ℓ-torsion of abelian varieties in a given isogeny class in terms of corresponding Weil polynomial. Since $A[\ell](k^{alg})$ is an $\mathbb{F}_\ell$-vector space, we have to describe possible matrices of the Frobenius action on such vector spaces.

In the second section we reduce the problem to a particular linear algebra question. Here is a simplified version of the question. Let N be a nilpotent $d \times d$ matrix over $\mathbb{F}_\ell$, and let $Q \in \mathbb{Z}_\ell[t]$ be a polynomial of degree d such that $Q \equiv t^d \bmod \ell$. Is it possible to find a matrix M over $\mathbb{Z}_\ell$ such that the characteristic polynomial of M is Q, and $M \equiv N \bmod \ell$? We will refer to this question as *lifting of the nilpotent matrix N to $\mathbb{Z}_\ell$ with respect to Q*.

The main results of the paper are proved in Section 3. First we associate to a nilpotent matrix N a polygon of special type. Let $m_1 \geq \cdots \geq m_r$ be the dimensions of the Jordan cells of N. The numbers $m_1, \ldots, m_r$ determine the matrix up to conjugation. *The Young polygon* $\mathrm{Yp}(N)$ of N is the convex polygon with vertices $(\sum_{j=1}^{i} m_j, i)$ for $0 \leq i \leq r$. For a polynomial $Q \in \mathbb{Z}[t]$ we denote by $\mathrm{Np}_\ell(Q)$ the Newton polygon of Q with respect to ℓ (see Section 3 for a precise definition). Assume that Q is separable. The main result of Section 3 can be reformulated as follows: one can lift N to $\mathbb{Z}_\ell$ with respect to Q if and only if $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(N)$ (see Theorems 3.1 and 3.2). This result allows one

to classify ℓ-torsion of abelian varieties belonging to an isogeny class corresponding to the Weil polynomial without multiple roots (Corollaries 3.6 and 3.7).

In Section 4 we establish a relationship between Young polygons for the Frobenius actions on an abelian variety and its dual. We also treat the following question due to B. Poonen: Is it true that for an abelian surface A the group of k-rational points $A(k)$ is isomorphic to the group of k-rational points $\widehat{A}(k)$ on its dual? The answer is no, and we give a counterexample.

In Section 5 we prove that (generalized) matrix factorizations correspond to Tate modules. This technique turns out to be useful when Weil polynomial is not separable. In Section 6 we explicitly classify ℓ-torsion of abelian surfaces. In the final section we apply this result to the classification of zeta functions of Kummer surfaces.

2. Preliminaries

2.1. Finite group subschemes of abelian varieties

A finite étale group scheme G over k is uniquely determined by the Frobenius action on $G(k^{alg})$ (see [2]). If $\ell \cdot G = 0$, then $G(k^{alg})$ is an $\mathbb{F}_\ell$-vector space and Frobenius action is $\mathbb{F}_\ell$-linear. By definition of the Tate module, we have $A[\ell](k^{alg}) \cong T_\ell(A)/\ell T_\ell(A)$. Thus the structure of a group scheme on $A[\ell]$ depends only on the module structure on $T_\ell(A)$ over $R = \mathbb{Z}_\ell[F] \subset \mathrm{End}_k(A)$. Moreover, since the action of F on $V_\ell(A)$ is semisimple, f_A determines the R-module $V_\ell(A)$ uniquely up to isomorphism.

The following lemma shows what R-modules can arise as Tate modules of varieties from a fixed isogeny class.

Lemma 2.1. *(See [6, IV.2.3].) If $f : B \to A$ is an isogeny then, $T_\ell(f) : T_\ell(B) \to T_\ell(A)$ is an embedding of R-modules, and if T denotes its image then*

$$F(T) \subset T \quad \text{and} \quad T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell. \tag{1}$$

Conversely, if $T \subset T_\ell(A)$ is a $\mathbb{Z}_\ell$-submodule such that (1) holds, then there exists an abelian variety B defined over k and an isogeny $f : B \to A$ such that $T_\ell(f)$ induces an isomorphism $T_\ell(B) \cong T$. □

2.2. Generalized Jordan form

Let K be a field, and let λ be an algebraic number over K. Put $L = K(\lambda)$. Take a vector space L^r with a natural basis $v_1, \dots, v_r$. Let $M : L^r \to L^r$ be a linear transformation such that its matrix is a sum of Jordan cells with eigenvalue λ, i.e. $M = \lambda I_r + N$, where I_r is the identity matrix and N is a nilpotent matrix of dimension r. The set $\{\lambda^j v_i \mid 1 \le i \le r, 0 \le j \le n-1\}$ is a basis of L^r as a K-vector space. Denote by $J(\lambda, N)$ the matrix of M in this basis. It is called *generalized Jordan cell*. We have the following generalization of the Jordan decomposition theorem.

Theorem 2.2. *Let M be a linear transformation of a K-vector space V with the characteristic polynomial P. Suppose that any irreducible divisor of P is separable. Let Δ be the set of roots of P, and $\Lambda \subset \Delta$ be the image of a section of the natural map $\Delta \to \Delta/\operatorname{Gal}(K^{sep}/K)$, i.e. for any root $\delta \in \Delta$ there exists a unique $\lambda \in \Lambda$ which is conjugate to δ. Then there exists a basis of V such that the matrix of M is a direct sum of generalized Jordan cells $J(\lambda, N_\lambda)$ for $\lambda \in \Lambda$. This data determines M uniquely up to isomorphism over K.*

Proof. Let $P = \prod_{\lambda_\in \Lambda} P_\lambda^{d_\lambda}$ be the decomposition of P into a product of monic irreducible separable polynomials $P_\lambda \in K[t]$ such that $P_\lambda(\lambda) = 0$ for any $\lambda \in \Lambda$. Then by the Chinese remainder theorem

$$\overline{R} = K[t]/P(t)K[t] \cong \prod_{\lambda\in\Lambda} K[t]/P_\lambda(t)^{d_\lambda}K[t].$$

The vector space V is an $\overline{R}$-module such that the image of t in $\overline{R}$ acts on V as M. Put $\overline{L}_\lambda = K[t]/P_\lambda(t)K[t]$, and $\overline{R}_\lambda = K[t]/P_\lambda(t)^{d_\lambda}K[t]$. It follows that $V \cong \bigoplus V_\lambda$, where $V_\lambda = \overline{R}_\lambda V$ is an $\overline{R}_\lambda$-module. For any $\lambda \in \Lambda$ the polynomial P_λ is separable, thus $\operatorname{Spec} \overline{L}_\lambda$ is smooth over $\operatorname{Spec} K$. By [3, 17.5.1] (see also [4, II. exercise 8.6]) we can find a section ψ_λ of the natural morphism $\varphi_\lambda : \overline{R}_\lambda \to \overline{L}_\lambda$, i.e., $\overline{R}_\lambda$ is an $\overline{L}_\lambda$-algebra, and V_λ has a structure of an $\overline{L}_\lambda$-vector space. Denote by $t_\lambda \in \overline{R}_\lambda$ the image of t under the natural projection $K[t] \to \overline{R}_\lambda$. Then $\lambda = \varphi_\lambda(t_\lambda)$, and $n_\lambda = t_\lambda - \psi_\lambda(\lambda) \in \overline{R}_\lambda$ is in the kernel of φ_λ. Thus $n_\lambda^{d_\lambda} = 0$, i.e. n_λ acts on V_λ as a nilpotent matrix N_λ. We see that t_λ acts on V_λ as a generalized Jordan cell $J(\lambda, N_\lambda)$.

Finally, we have to prove that if $\bigoplus_{\lambda\in\Lambda} J(\lambda, N_\lambda)$ is conjugate to $\bigoplus_{\lambda\in\Lambda} J(\lambda, N'_\lambda)$ over K, then for all $\lambda \in \Lambda$ the matrix N_λ is conjugate to N'_λ over $\overline{L}_\lambda$. Indeed, these matrices have the same dimension d_λ, and are conjugate by the Jordan decomposition theorem over $\overline{L}_\lambda$. □

Remark 2.3. We proved that $\overline{R}_\lambda \cong \overline{L}_\lambda[t]/(t-\lambda)^{d_\lambda}\overline{L}_\lambda[t]$. We use this isomorphism later.

2.3. Reduction step 1

For a polynomial $P \in \mathbb{Z}_\ell[t]$ denote by $\overline{P} \in \mathbb{F}_\ell[t]$ its reduction modulo ℓ, and by $P_1 \in \mathbb{Z}_\ell[t]$ the unitary separable polynomial with the same set of roots as P. We call P_1 *the minimal polynomial* of P. The Frobenius action on $V_\ell(A)$ is semisimple, thus the minimal polynomial f_1 of f is the minimal polynomial of the Frobenius action. It follows that $R \cong \mathbb{Z}_\ell[t]/f_1(t)\mathbb{Z}_\ell[t]$.

The Galois group $\operatorname{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ acts on the set Δ of roots of $\overline{f}_1$. Let $\Lambda \subset \Delta$ be the image of a section of the natural map $\Delta \to \Delta/\operatorname{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. By Theorem 2.2 applied to the action of Frobenius on $T_\ell(A)/\ell T_\ell(A)$ the matrix of F is conjugate to the sum of $J(\lambda, N_\lambda)$ for $\lambda \in \Lambda$. We generalize this result to Tate modules.

By the Hensel lemma [3, 18.5.13], we can decompose f_1 into the product of monic polynomials $f_\lambda \in \mathbb{Z}_\ell[t]$ such that $\overline{f}_\lambda$ is a power of an irreducible monic polynomial corresponding to $\lambda \in \Lambda$. We have a natural homomorphism of rings

$$\varphi : R \to \prod_{\lambda\in\Lambda} \mathbb{Z}_\ell[t]/f_\lambda(t)\mathbb{Z}_\ell[t].$$

Since P_λ is monic, $R_\lambda = \mathbb{Z}_\ell[t]/f_\lambda(t)\mathbb{Z}_\ell[t]$ is free and finitely generated $\mathbb{Z}_\ell$-module. By the Chinese remainder theorem φ is an isomorphism modulo ℓ. On the other hand, φ is a homomorphism of finitely generated free $\mathbb{Z}_\ell$-modules. It follows that φ is an isomorphism.

The module $T_\ell(A)$ is an R-module such that the image of t in R acts as Frobenius. Put $T_\lambda = R_\lambda T_\ell(A)$, then $T_\ell(A) = \bigoplus T_\lambda$. By Theorem 2.2, the matrix of the action of t on $T_\lambda/\ell T_\lambda$ is of the form $J(\lambda, N_\lambda)$ in some basis. We now sum up our observations.

Proposition 2.4. *There is an isomorphism of R-modules $T_\ell(A) \cong \bigoplus_{\lambda\in\Lambda} T_\lambda$ such that F acts on $T_\lambda/\ell T_\lambda$ with matrix $J(\lambda, N_\lambda)$ in some basis.*

2.4. Reduction step 2

Let L_λ be an unramified extension of $\mathbb{Q}_\ell$ with residue field $\mathbb{F}_\ell(\lambda)$. Denote by S_λ the ring of integers of L_λ.

Proposition 2.5. *There is an isomorphism $R_\lambda \cong S_\lambda[t]/gS_\lambda[t]$ for some $g \in S_\lambda[t]$ such that $g \equiv (t-\lambda)^d \bmod \ell S_\lambda$, where d is the multiplicity of λ in $\overline{f}_\lambda$.*

Proof. Let Δ_λ be the set of roots of $\overline{f}_\lambda$. Then

$$f_\lambda \equiv \prod_{\delta\in\Delta_\lambda} (t-\delta)^{d_\delta} \bmod \ell S_\lambda,$$

for some natural numbers d_δ. By the Hensel lemma, f_λ equals to a product of monic polynomials $g_\delta \in S_\lambda[t]$ such that

$$g_\delta \equiv (t-\delta)^{d_\delta} \bmod \ell S_\lambda,$$

where $\delta \in \Delta_\lambda$. Define the homomorphism of rings

$$R_\lambda \to R_\lambda \otimes_{\mathbb{Z}_\ell} S_\lambda$$

by $r \mapsto r \otimes 1$. By the Chinese remainder theorem,

$$R_\lambda \otimes_{\mathbb{Z}_\ell} S_\lambda \cong \prod_{\delta\in\Delta_\lambda} Z_\delta$$

where $Z_\delta \cong S_\lambda[t]/g_\delta S_\lambda[t]$. Take the projection $R_\lambda \otimes_{\mathbb{Z}_\ell} S_\lambda \to Z_\lambda$. We get a homomorphism $\varphi : R_\lambda \to Z_\lambda$. It is a homomorphism of free $\mathbb{Z}_\ell$-modules and an isomorphism modulo ℓ by Remark 2.3. We conclude that φ is an isomorphism. Put $g = g_\lambda$. □

Choose an element $\alpha \in S_\lambda$ such that $\overline{\alpha} = \lambda$. The polynomial $Q_\lambda(t) = g(t - \alpha)$ is the minimal polynomial of $F - \alpha$ acting on T_λ. Clearly, $Q_\lambda \equiv t^d \bmod \ell$, where $d = \deg Q_\lambda$. We have reduced our task to the following linear algebra problem.

2.5. The problem

Let L be an unramified extension of $\mathbb{Q}_\ell$, and let S be its ring of integers. Suppose we are given a polynomial $Q \in S[t]$ such that $Q \equiv t^d \bmod \ell$, where $d = \deg Q$. Let V be an L-vector space of dimension d, and let E be a semisimple linear transformation on V with characteristic polynomial Q. Denote by Q_1 the minimal polynomial of E. Put $R = S[t]/Q_1(t)S[t]$. We give a structure of an R-module on V such that t acts as E. Describe all isomorphism classes of finite R-modules of the form $T/\ell T$, where T is an arbitrary R-invariant S-lattice in V.

If we choose a basis of T, the problem can be reformulated as follows. Let N be the matrix of the action of E on $T/\ell T$ in some basis over the finite field $S/\ell S$. It is a nilpotent matrix over $S/\ell S$, since $Q \equiv t^d \bmod \ell$. Is it possible to find a matrix M over S such that $Q(t) = \det(t - M)$, and $M \equiv N \bmod \ell$? We will refer to this question as *lifting of nilpotent matrix N to S with respect to Q*.

3. ℓ-Torsion of abelian varieties

Let S be the ring of integers in an unramified extension L of $\mathbb{Q}_\ell$. Assume we are given a finitely generated free S-module T endowed with an S-linear injective endomorphism E which induces on $T/\ell T$ a nilpotent endomorphism N. Let $Q(t) = \det(t - E)$. In this section we give a partial answer to the question: when is it possible to lift N to S with respect to Q? Using this result we get a classification of group schemes of the form $A[\ell]$ for A from a fixed isogeny class such that f_A is separable.

We associate to N a polygon of special type. For a sequence of natural numbers $m_1 \geq \cdots \geq m_r > 0$ we define *the Young polygon* $\mathrm{Yp}(m_1, \ldots, m_r)$ as the convex polygon with vertices $(\sum_{j=1}^{i} m_j, i)$ for $0 \leq i \leq r$. The *dimension of* $Y = \mathrm{Yp}(m_1, \ldots, m_r)$ is $\dim Y = \sum_{j=1}^{r} m_j$. The *height of* Y is $\mathrm{Ht}(Y) = r$.

There is a basis of $T/\ell T$ such that the matrix of N is a sum of Jordan cells of dimensions $m_1, \ldots, m_r$. Clearly, numbers $m_1, \ldots, m_r$ determine N uniquely up to conjugation. We associate to N the Young polygon $\mathrm{Yp}(N)$ given by the sequence $m_1, \ldots, m_r$. We also denote this Young polygon by $\mathrm{Yp}(E|T)$.

The Young polygon has $(0, 0)$ and (d, r) as its endpoints, and its slopes are $1/m_1, \ldots, 1/m_r$. For example, the following figure shows Young polygons for the zero matrix (Fig. 1) and the Jordan cell of dimension two (Fig. 2).

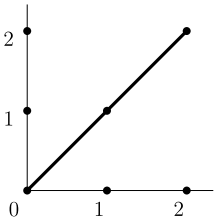

Fig. 1. Yp(1, 1).

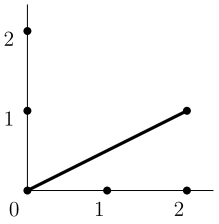

Fig. 2. Yp(2).

Denote by ν the normalized valuation on L, i.e. $\nu(\ell) = 1$. Suppose that $Q(t) = \sum_i Q_i t^{d-i}$. Take the lower convex hull of the points $(i, \nu(Q_i))$ for $0 \leq i \leq \deg Q$ in $\mathbb{R}^2$. The boundary of this region is called *the Newton polygon* $\mathrm{Np}(Q)$ *of* Q. Its vertices have integer coefficients, and $(0, 0)$ and $(d, \nu(Q_d))$ are its endpoints. The *slopes of* Q are the slopes of this polygon. Note that each slope has a multiplicity.

Theorem 3.1. *The Newton polygon* $\mathrm{Np}(Q)$ *lies on or above Young polygon* $\mathrm{Yp}(E|T)$.

Proof. Let $Q_1 \in S[t]$ be the minimal polynomial of E, and let $R = S[t]/Q_1(t)S[t]$. Let $x \in R$ be the image of t under the natural projection. The module T is naturally an R-module such that x acts as E.

Suppose $\mathrm{Yp}(E|T) = \mathrm{Yp}(m_1, \ldots, m_r)$. Take generators $v'_1, \ldots, v'_r$ of $T/\ell T$ over R such that

$$v'_1, xv'_1, \ldots, x^{m_1-1}v'_1, \ldots, v'_r, \ldots, x^{m_r-1}v'_r$$

is a Jordan basis for x. By the Nakayama lemma there exist generators $v_1, \ldots, v_r$ of T over R which lift $v'_1, \ldots, v'_r$. Let H be a matrix of x in the basis

$$v_1, xv_1, \ldots, x^{m_1-1}v_1, \ldots, v_r, \ldots, x^{m_r-1}v_r,$$

and let $H_{i_1,\ldots,i_m}$ be the determinant of the submatrix of H cut by the columns and rows with the numbers $i_1, \ldots, i_m$. The characteristic polynomial of x acting on T is

$$Q(t) = \sum_{m=0}^{d} Q_m t^{d-m},$$

and

$$Q_m = (-1)^m \sum_{i_1<\cdots<i_m} H_{i_1,\ldots,i_m}.$$

It follows that

$$\nu(Q_m) \geq \min_{i_1<\cdots<i_m} \nu(H_{i_1,\ldots,i_m}).$$

Let $m = m_1 + \cdots + m_{s-1} + a$, where $0 < a \le m_s$. We have to show that if $H_{i_1,\ldots,i_m} \neq 0$, then $\nu(H_{i_1,\ldots,i_m}) \ge s$. Note that if $i \neq m_1 + \cdots + m_j$ for all j, then the i-th column of H has 1 only in the position number $i+1$, and its other entries are zero. Thus if $i \in \{i_1, \ldots, i_m\}$, and $H_{i_1,\ldots,i_m} \neq 0$, then $i+1 \in \{i_1, \ldots, i_m\}$. If $i = m_1 + \cdots + m_j$ for some j, then ℓ divides the i-th column. We see that if $H_{i_1,\ldots,i_m} \neq 0$, then the set $\{i_1, \ldots, i_m\}$ is a union of *blocks*. Each block is an interval

$$\{i, i+1, \ldots, m_1 + \cdots + m_j\}$$

of length not greater than m_j. If $m > m_1 + \cdots + m_{s-1}$, then the set $\{i_1, \ldots, i_m\}$ contains no less than s blocks, and $\nu(H_{i_1,\ldots,i_m}) \ge s$. Thus if $(m, \nu(Q_m))$ is a vertex of $\mathrm{Np}(Q)$ then $\nu(Q_m) \ge s$, and $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(E|T)$. □

Theorem 3.2. *Let $R = S[t]/Q(t)S[t]$, and let $V = R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Let Y be a Young polygon such that $\mathrm{Np}(Q)$ lies on or above Y. Then there exists an R-lattice T in V such that $\mathrm{Yp}(x|T) = Y$.*

Proof. Recall that $Q = \det(t - x|V)$ is the minimal polynomial of the action of x on V. Let $Y = Y(m_1, \ldots, m_r)$. First, we find a lattice T in V over S such that $R \subset T \subset V$. After that we prove that T is an R-module.

Let $m = m_1 + \cdots + m_s$, and let $Q(t) = \sum_{i=0}^{d} Q_i t^{d-i}$. For $1 \le s \le r$ we put

$$v_{s+1} = \frac{x^m + \sum_{j=1}^{m} Q_j x^{m-j}}{\ell^s}.$$

In addition, let $v_1 = 1$, and let $v_{r+1} = 0$. Note that

$$v_1, xv_1, \ldots, x^{m_1-1}v_1, \ldots, v_r, \ldots, x^{m_r-1}v_r$$

have different degrees viewed as polynomials in x, and hence generate a lattice T over S.

Now we prove that T is an R-module. The point $(m - m_s, s-1)$ is a vertex of Y. By assumption, $\mathrm{Np}(Q)$ lies on or above Y, thus $(m - m_s, s-1)$ is not higher than $\mathrm{Np}(Q)$. It follows that ℓ^s divides Q_j for all $j > m - m_s$. Thus

$$u_s = \frac{\sum_{j=m-m_s+1}^{m} Q_j x^{m-j}}{\ell^s} \in S \cdot 1 \subset T.$$

Moreover,

$$x^{m_s} v_s = \ell(v_{s+1} - u_s) \in \ell T.$$

This proves that $xT \subset T$, and that $\mathrm{Yp}(x|T) = Y$. □

Example 3.3. Let $Q(t) = t^2 - \ell t - \ell$. Its Newton polygon is drawn in Fig. 2. Then we can lift the nonzero nilpotent Jordan cell (its Young polygon is equal to $\mathrm{Np}(Q)$). For example, take

$$M = \begin{pmatrix} 0 & \ell \\ 1 & \ell \end{pmatrix}.$$

Clearly, $Q(t) = \det(t - M)$. We cannot lift the zero matrix, because its Young polygon (see Fig. 1) is higher than $\mathrm{Np}(Q)$.

Note that if Q is not separable, then the action of x on V is not semisimple. By Theorems 3.1 and 3.2 we get

Corollary 3.4. *Suppose that Q is separable. One can lift N to S with respect to Q if and only if* $\mathrm{Np}(Q)$ *lies on or above* $\mathrm{Yp}(N)$.

Suppose that Q is not separable, and N is a nilpotent matrix such that $\mathrm{Np}(Q)$ lies on or above $\mathrm{Yp}(N)$. Then in general it is not possible to lift N to S with respect to Q. We discuss a partial solution of this problem in Section 5. Now we prove the following simple result.

Proposition 3.5. *Suppose $Q = P^r$, where $\deg P = 2$, and P is separable. Let $R = S[t]/P(t)S[t]$, and let $V = (R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^r$. There exists an S-lattice T in V such that x acts on $T/\ell T$ with Young polygon Y if and only if* $\mathrm{Np}(P^r)$ *lies on or above Y, and all slopes of Y are equal to* $1/2$ *or* 1. □

Proof. Let N be a nilpotent matrix with Young polygon Y. Suppose such a lattice T exists. Since $\deg P = 2$, any Jordan cell of N has dimension at most 2, thus all slopes of $\mathrm{Yp}(N)$ are equal to $1/2$ or 1. Conversely, there is a decomposition $N = \bigoplus N_i$ such that $\dim \mathrm{Yp}(N_i) = 2$. By Theorem 3.2 for any i there exists an S-lattice T_i such that x acts on $T_i/\ell T_i$ with the matrix N_i. Put $T = \bigoplus T_i$. □

We call a polynomial $f \in \mathbb{Z}_\ell[t]$ *distinguished* if $\overline{f}$ is a power of an irreducible polynomial. We now use notation of Section 2. Let $f_1 \in \mathbb{Z}_\ell[t]$ be the minimal polynomial of f. Choose a root λ of $\overline{f}$ and its lifting $\alpha_\lambda \in S_\lambda$. By Proposition 2.5,

$$R_\lambda = \mathbb{Z}_\ell[t]/f_1\mathbb{Z}_\ell[t] \cong S_\lambda[t]/gS_\lambda[t],$$

and $g \equiv (t - \lambda)^d \bmod \ell S_\lambda$. Put $Q_1(t) = g(t - \alpha_\lambda)$. Note that $Q_1(t)$ divides $f(t - \alpha_\lambda)$ over L_λ. Take a unitary polynomial $Q = Q_\lambda \in S_\lambda[t]$ of maximal degree such that $Q(t)$ divides $f(t - \alpha_\lambda)$ over L_λ, and the minimal polynomial of Q is Q_1. We could define Q in other way. Let V be a $\mathbb{Q}_\ell$-vector space endowed with semisimple linear transformation F such that $f(t) = \det(t - F)$. Then V is an L_λ-vector space, and $Q(t)$ is the characteristic polynomial of the L_λ-linear transformation $F - \alpha_\lambda$.

Recall that an étale group scheme is uniquely determined by the linear Frobenius action on the group of k^{alg}-points. Let Y be a Young polygon of dimension $\deg Q$ such that $\mathrm{Np}(Q)$ lies on or above Y, and let N be a nilpotent matrix such that $Y = \mathrm{Yp}(N)$. *A distinguished group scheme* is a finite étale group scheme $A(f, Y)$ over k such that $\dim_{\mathbb{F}_\ell} A(f, Y)(k^{alg}) = \deg f$, and F acts on $A(f, Y)(k^{alg})$ with the matrix $J(\lambda, N)$ in some basis. Note that for a given f the polynomial Q is uniquely determined modulo ℓ. Thus $A(f, Y)$ is uniquely determined by f and Y up to an isomorphism.

Corollary 3.6. *Let A be an abelian variety over k. Then $A[\ell]$ is isomorphic to a sum of distinguished group schemes.*

Proof. Let $f_A = \prod_{\lambda\in\Lambda} f_\lambda$ be a product of pairwise coprime distinguished polynomials. By Proposition 2.4, $T_\ell(A) \cong \bigoplus_{\lambda\in\Lambda} T_\lambda$. By Proposition 2.5, $R_\lambda \cong S_\lambda[t]/gS_\lambda[t]$. This gives a structure of an S_λ-module on T_λ. As before, let $\alpha_\lambda \in S_\lambda$ be a lifting of λ, and let Q_λ be the characteristic polynomial of the action of $F - \alpha_\lambda$ on T_λ. By Theorem 3.1, F acts on $T_\lambda/\ell T_\lambda$ with the matrix $J(\lambda, N_\lambda)$, where N_λ is a nilpotent matrix such that $\mathrm{Np}(Q_\lambda)$ lies on or above $\mathrm{Yp}(N_\lambda)$. Thus $A[\ell] \cong \bigoplus_{\lambda\in\Lambda} A(f_\lambda, \mathrm{Yp}(N_\lambda))$. □

Corollary 3.7. *Let A be an abelian variety over k. Suppose f_A is separable, and $f_A = \prod_{\lambda\in\Lambda} f_\lambda$ is a product of coprime distinguished polynomials. Then for any family of distinguished group schemes $A(f_\lambda, Y_\lambda)$ there exists an abelian variety B isogenous to A such that $B[\ell] \cong \bigoplus_{\lambda\in\Lambda} A(f_\lambda, Y_\lambda)$.*

Proof. By Proposition 2.4, $V_\ell(A) \cong \bigoplus_{\lambda\in\Lambda} V_\lambda$, where $V_\lambda = R_\lambda V_\ell(A)$ is an R_λ-module. Let α_λ be a lift of λ. By Theorem 3.2, there exists an S_λ-lattice $T_\lambda \subset V_\lambda$ such that $F - \alpha_\lambda$ acts on $T_\lambda/\ell T_\lambda$ with Young polygon Y_λ. Put $T = \bigoplus T_\lambda$. By Lemma 2.1, there exists a variety B such that $T \cong T_\ell(B)$. □

4. Young polygons and duality

By $\widehat{A}$ we denote the dual variety of an abelian variety A. Suppose f is a distinguished polynomial such that f divides f_A, and polynomials f and f_A/f have no common roots modulo ℓ. By Proposition 2.4, there exists a direct summand T of $T_\ell(A)$ such that F acts on T with characteristic polynomial f. The polynomial $\widehat{f}(t) = (\frac{t}{q})^{\deg f} f(\frac{q}{t})$ divides f_A. Clearly, $\widehat{f}(t)$ is distinguished. Denote the corresponding direct summand of $T_\ell(\widehat{A})$ by $\widehat{T}$.

Let λ be a root of $\overline{f}$, and let S be the ring of integers in an unramified extension of $\mathbb{Q}_\ell$ with residue field $\mathbb{F}_\ell(\lambda)$. By Proposition 2.5, T is an S-module. Clearly, q/λ is a root of $\widehat{f}(t)$, and $\widehat{T}$ is an S-module too.

Proposition 4.1. *Let $\alpha \in S$ be a lift of λ. Then* $\mathrm{Yp}(F - \alpha|T) = \mathrm{Yp}(F - q/\alpha|\widehat{T})$.

Proof. The Weil pairing $e : T_\ell(A) \times T_\ell(\widehat{A}) \to \mathbb{Z}_\ell$ is non-degenerate, and $e(Fx, Fy) = qe(x, y)$, where $x \in T_\ell(A)$ and $y \in T_\ell(\widehat{A})$ [7]. This yields that its restriction to $T \times \widehat{T}$ is

non-degenerate. By an integral version of Deligne trick [1, Lemma 3.1], there exists an S-linear pairing $e_S : T \times \widehat{T} \to S$ such that $e_S(Fx, Fy) = qe_S(x, y)$, and $e = Tr_{L/\mathbb{Q}_\ell} \circ e_S$, where L is the fraction field of S. We have

$$e_S(Fx, y) = e_S\big(Fx, F\big(F^{-1}y\big)\big) = e_S\big(x, \big(qF^{-1}\big)y\big).$$

Let $M = J(\lambda, N)$ be the matrix of the action of F on $T/\ell T$ in some basis over $S/\ell S$, and let $\widehat{M}$ be the matrix of the action of F on $\widehat{T}/\ell\widehat{T}$ in the dual basis. It follows that $\widehat{M}^t = qM^{-1}$, where $\cdot^t$ means transpose. One easily proves that for any cell of M corresponding to the Jordan cell of dimension d there exists a cell of $\widehat{M}$ corresponding to the same Jordan cell. The proposition follows. □

We now give an example of an abelian surface A such that the group of points $A(k)$ is not isomorphic to the group of points on the dual surface $\widehat{A}(k)$. Recall that $A(k)$ is a kernel of $1 - F : A \to A$, and the ℓ-component $A(k)_\ell = \ker(1 - F) : T_\ell(A) \to T_\ell(A)$.

Example 4.2. Let $q = 7$, and let $\ell = 5$. Suppose $f_a(t) = t^2+2t+7$ and $f_b(t) = t^2-3t+7$ are Weil polynomials of two elliptic curves. The polynomial $f = f_a f_b$ is the Weil polynomial of an abelian surface. Note that $f_a(t) \equiv f_b(t) \equiv (t-1)(t-q) \bmod 5$. Thus we have a decomposition $f = f_1 f_2$ over $\mathbb{Z}_5$, where $f_1 \equiv (t-1)^2 \bmod 5$, and $f_2 \equiv (t-q)^2 \bmod 5$. For any abelian surface B with Weil polynomial f we have a decomposition $T_5(B) \cong T_1 \oplus T_2$, where F acts on T_i with characteristic polynomial f_i for $i = 1, 2$. By Theorem 3.1, $F-1$ acts on $T_1/5T_1$ trivially and by Theorem 3.2, there exists a lattice T in $T_2 \otimes \mathbb{Q}$ such that $F - q$ acts on $T/5T$ non-trivially. In the first case the Young polygon of $F - 1$ is $\mathrm{Yp}(2)$, and in the second case the Young polygon of $F - q$ is $\mathrm{Yp}(1, 1)$. By Lemma 2.1, there exists an abelian surface A such that $T_5(A) \cong T_1 \oplus T_2$. By the previous proposition, $A(\mathbb{F}_7)_5 \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, and $\widehat{A}(\mathbb{F}_7)_5 \cong \mathbb{Z}/25\mathbb{Z}$.

5. Matrix factorizations

In this section we turn our attention to the case when the Weil polynomial is not separable. We reprove some known results on matrix factorizations in the arithmetic situation and apply them to Tate modules. Given a Tate module T with the Weil polynomial f and the minimal polynomial f_1 one can produce the unique (up to isomorphism) Tate module T' with the Weil polynomial $g = f_1^r/f$ for some r. If we are lucky, g does not have multiple roots. In this case, one can get some information on T from T' using Theorem 3.1. Moreover, one can reverse the construction and produce a Tate module T with a given Young polygon starting from T', which can be constructed using Theorem 3.2.

Let S be the ring of integers in a finite unramified extension L of $\mathbb{Q}_\ell$. Fix a pair of polynomials $f, f_1 \in S[t]$ and a positive integer r. Let $R = S[t]/f_1 S[t]$, and let $\bar{S} = S/\ell S$. Denote by $x \in R$ the image of t under the natural projection from $S[t]$. We assume that $f_1 \equiv t^{d_1} \bmod \ell$, and $\deg f_1 = d_1$.

Definition 5.1. A *matrix factorization* (with respect to f, f_1 and r) is a pair (X, Y) of $r \times r$ matrices with coefficients in $S[t]$ such that $YX = f_1 \cdot I_r$ and $\det X = f$.

Suppose we are given a matrix factorization (X, Y). The matrix X defines a map of free $S[t]$ modules:

$$S[t]^r \xrightarrow{X} S[t]^r.$$

Its cokernel T is annihilated by f_1. It is equivalent to say that T is an R-module. We see that the matrix factorization (X, Y) corresponds to a finitely generated R-module T given by the presentation:

$$S[t]^r \xrightarrow{X} S[t]^r \to T \to 0. \tag{2}$$

Proposition 5.2. *The module T is free of finite rank d over S, and the characteristic polynomial of the action of x on T is equal to f.*

Proof. Since $f_1 \equiv t^{d_1} \bmod \ell$, and $\deg f_1 = d_1$, the ring R is generated as S-module by the elements $1, x, \ldots, x^{d_1-1}$. By definition, T is a finitely generated R-module, thus it is finitely generated over S.

Take the tensor product of the presentation (2) with $\bar{S}[t]$:

$$\bar{S}[t]^r \xrightarrow{\bar{X}} \bar{S}[t]^r \to T \otimes_S \bar{S} \to 0.$$

The ring $\bar{S}[t]$ is a principal ideal domain, thus there exist matrices M_1 and M_2 over $\bar{S}[t]$ such that $\det M_1 = \det M_2 = 1$ and $M_1 \bar{X} M_2$ is the diagonal matrix with determinant t^d. It follows that $M_1 \bar{X} M_2$ is the diagonal matrix $\operatorname{diag}(t^{m_1}, \ldots, t^{m_r})$ for some $m_1, \ldots, m_r \in \mathbb{N}$ such that $\sum m_i = d$. We get

$$T \otimes_S \bar{S} \cong \bigoplus_{i=1}^{r} \bar{S}[t]/t^{m_i} \bar{S}[t].$$

By the Nakayama lemma, T is generated by d elements over S.

Now take the presentation of $T \otimes_S L$:

$$L[t]^r \xrightarrow{X} L[t]^r \to T \otimes_S L \to 0.$$

As before, there exist matrices M_3 and M_4 over $L[t]$ such that $\det M_3 = \det M_4 = 1$, and $M_3 X M_4 = \operatorname{diag}(g_1, \ldots, g_r)$. Clearly,

$$T \otimes_S L \cong \bigoplus_{i=1}^{r} L[t]/g_i L[t],$$

and $\operatorname{rk} T = d$. This proves that T is free over S. To conclude the proof we note that the characteristic polynomial of the action of x on $L[t]/g_iL[t]$ is equal to g_i. □

The following proposition shows that modules over R give rise to matrix factorizations.

Proposition 5.3. *Let T be an R-module which is free of finite rank over S. Suppose that T is generated over R by r elements, and that $\operatorname{Yp}(x|T) = \operatorname{Yp}(m_1, \dots, m_r)$. Then there exists a matrix factorization (X, Y) such that T has the presentation (2), and*

$$X \equiv \operatorname{diag}\left(t^{m_1}, \dots, t^{m_r}\right) \bmod \ell.$$

Proof. Let $v_1, \dots, v_r$ be generators of T over R. Then $x^{m_i}v_i = \sum_j a_{ji}(x)v_j$, where $a_{ji} \in S[t]$ and $\deg a_{ji} < m_j$. Let X be the matrix with the entries $t^{m_i}\delta_{ji} - a_{ji}$. Define an R-module T' by the presentation:

$$S[t]^r \xrightarrow{X} S[t]^r \to T' \to 0.$$

Put $m = \sum_i m_i$. Then $\det X \equiv t^m \bmod \ell$, and from the inequalities $\deg a_{ji} < m_j$ it follows that $\det X$ is a polynomial of degree m. By Proposition 5.2, T' is a free S module of rank m. By definition of T', we have a surjective map of S-modules $T' \to T$. Since they have the same rank as S-modules, this map is an isomorphism, and, by Proposition 5.2, $\det X = f$.

Multiplying presentation (2) by f_1 we get the commutative diagram

$$\begin{array}{ccccccc} S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle 0} & & \\ S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \end{array}$$

Since $S[t]^r$ is free, there exists a matrix Y such that the diagram

$$\begin{array}{ccccccc} S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \\ & {\scriptstyle Y}\swarrow & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle 0} & & \\ S[t]^r & \xrightarrow{X} & S[t]^r & \longrightarrow & T & \longrightarrow & 0 \end{array}$$

commutes. It follows that $YX = f_1 I_r$. Thus, the pair (X, Y) is a matrix factorization. □

Example 5.4. Let $\deg f_1 = 3$, and let $f = f_1^2$. Suppose f_1 is separable. When there exists an R-module T such that x acts with $r = 3$ Jordan cells of dimension 2? By Proposition 5.3, such a module exists iff there exists a matrix factorization (X, Y) such that

$$X \equiv \operatorname{diag}(t^2, t^2, t^2) \bmod \ell.$$

The matrix factorization (Y, X) gives a module T' over R which is generated by 3 elements and the characteristic polynomial of x is equal to $\det Y = f_1^3/f = f_1$. Moreover, $Y \equiv \operatorname{diag}(t, t, t) \bmod \ell$. It follows that $\operatorname{Yp}(x|T') = \operatorname{Yp}(1, 1, 1)$. By Theorems 3.1 and 3.2, such a module T' exists iff $\operatorname{Np}(f_1)$ lies on or above $\operatorname{Yp}(x|T')$. Thus T exists iff $\operatorname{Np}(f_1)$ lies on or above $\operatorname{Yp}(1, 1, 1)$.

6. ℓ-Torsion of abelian surfaces

In this section we classify isomorphism classes of ℓ-torsion subschemes of abelian surfaces. We use the following notation. Let $P = \prod_{\lambda\in\Lambda} P_\lambda$ be the decomposition of a polynomial $P(t) \in \mathbb{Z}_\ell[t]$ into a product of distinguished polynomials. Then $A(P, 0)$ is the group scheme $\bigoplus_{\lambda\in\Lambda} A(P_\lambda, Y_{\deg P_\lambda})$, where Y_n is the Young polygon of the zero matrix of dimension n.

Theorem 6.1. *Let A be an abelian surface over k with the Weil polynomial $f_A(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2$. Suppose first that f_A is separable, then we have the following five cases:*

(1) *if $f_A(t)$ is separable modulo ℓ, then $A[\ell] \cong A(f_A, 0)$;*
(2) *if $f_A(t) \equiv f_1f_2 \bmod \ell$, where $f_1 \equiv (t-\alpha)^2 \bmod \ell$, and f_2 is separable modulo ℓ, then $A[\ell] \cong A(f_2, 0) \oplus A(f_1, Y)$, where $\dim Y = 2$;*
(3) *if $f_A(t) \equiv f_1f_2 \bmod \ell$, where $f_i \equiv (t-\alpha_i)^2 \bmod \ell$, for $i = 1, 2$ and $\alpha_1 \not\equiv \alpha_2 \bmod \ell$, then $A[\ell] \cong A(f_1, Y_1) \oplus A(f_2, Y_2)$, where $\dim Y_1 = \dim Y_2 = 2$;*
(4) *if $f_A(t) \equiv h(t)^2 \bmod \ell$, where h is irreducible modulo ℓ, then $A[\ell] \cong A(f_A, Y)$, where $\dim Y = 2$. If $\ell \neq 2$, and ℓ^2 does not divide $a_1^2 - 4a_2 + 8q$, or $\ell = 2$, and 4 does not divide $a_1 + a_2 + 1 - 2q$, then $Y = \operatorname{Yp}(2)$;*
(5) *if $f_A(t) \equiv (t-\alpha)^4 \bmod \ell$, then $A[\ell] \cong A(f, Y)$, where $\dim Y = 4$.*

Suppose that f_A is not separable, then we have the following three cases:

(6) *$f_A = P^2$, where P is separable. Then*
   (a) *if P is separable modulo ℓ, then $A[\ell] \cong A(P, 0) \oplus A(P, 0)$;*
   (b) *if $P(t) \equiv (t-\alpha)^2 \bmod \ell$, then $A[\ell] \cong A(P, Y_1) \oplus A(P, Y_2)$, where $\dim Y_1 = \dim Y_2 = 2$.*
(7) *$f_A(t) = (t \pm \sqrt{q}\,)^2(t^2 - bt + q)$, where $P_1(t) = t^2 - bt + q$ is separable. Let $P_2(t) = (t \pm \sqrt{q}\,)^2$.*
   (a) *If $P_1 \not\equiv P_2 \bmod \ell$, and P_1 is separable modulo ℓ, then $A[\ell] \cong A(P_1, 0) \oplus A(P_2, 0)$.*
   (b) *If $P_1 \not\equiv P_2 \bmod \ell$, and $P_1(t) \equiv (t-\alpha)^2 \bmod \ell$, then $A[\ell] \cong A(P_1, Y) \oplus A(P_2, 0)$, where $\dim Y = 2$.*
   (c) *If $P_1 \equiv P_2 \bmod \ell$, then*

(i) *either* $A[\ell] \cong A(P_1(t)(t \pm \sqrt{q}\,), Y) \oplus A(t \pm \sqrt{q}, 0)$, *where* $\dim Y = 3$; *or*
(ii) *if* ℓ^2 *divides* $P_1(\mp\sqrt{q}\,)$, *then* $A[\ell] \cong A(P_1, Y) \oplus A((t \pm \sqrt{q}\,)^2, Y)$, *where* $Y = \mathrm{Yp}(2)$.

(8) *If* $f_A(t) = (t \pm \sqrt{q}\,)^4$, *then* $A[\ell] \cong A(f_A, 0)$.

Conversely, for any group scheme G *described above there exists an abelian variety* B *in the isogeny class of* A *such that* $B[\ell] \cong G$.

Proof. Assume that f_A is separable. Note that if $f_A(t) \equiv (t-\alpha)^3(t-\beta) \bmod \ell$, then $\alpha \equiv \beta \bmod \ell$. Thus by Corollaries 3.6 and 3.7 the cases (1)–(3) and (5) follow. In the case (4) we have $A[\ell] \cong A(f_A, Y)$, where $\dim Y = 2$, and Y is the Young polygon of the zero matrix if and only if $R = \mathbb{Z}_\ell[t]/f_A(t)\mathbb{Z}_\ell[t]$ is not a DVR. Indeed, if R is regular, then $T_\ell(A)$ is free, and hence the action of t on $T_\ell(A)/\ell T_\ell(A)$ is non-trivial. If R is not regular, then the integral closure $\mathcal{O}$ of R is an example of an R-module such that $\mathcal{O}/\ell\mathcal{O} \cong A(f_A, 0)(k^{alg})$. By the Dedekind lemma [8, 5.55], R is regular if and only if $(f_A - h^2)/\ell$ is prime to h modulo ℓ. An easy computation shows that the two polynomials are coprime if and only if ℓ^2 does not divide $a_1^2 - 4a_2 + 8q$ for $\ell \neq 2$, and 4 does not divide $a_1 + a_2 + 1 - 2q$ for $\ell = 2$.

Assume now that f_A is not separable. It follows from the classification of Weil polynomials (see [5]), that only the cases (6)–(8) are possible. The case (6) follows from the Proposition 3.5, and the case (8) is obvious since Frobenius acts as multiplication by $\mp\sqrt{q}$. By Corollary 3.6, the conditions of (7a), (7b) and (7c(i)) are necessary. Let us prove that they are sufficient. We have to construct Tate module T with the prescribed Frobenius action. Then by Lemma 2.1, there exists an abelian variety B in the isogeny class of A such that $T \cong T_\ell(B)$.

We give a construction for the case (7b). Put $T = T_1 \oplus T_2$, where T_i is a torsion-free module of rank 1 over $R_i = \mathbb{Z}_\ell[t]/P_i\mathbb{Z}_\ell[t]$. The module T_1 is uniquely determined, and T_2 can be constructed using Theorem 3.2. The case (7a) is similar.

In the case (7c(i)) we construct the Tate module as the sum $T = T_1 \oplus T_2$, where T_1 is a module over $R_1 = \mathbb{Z}_\ell[t]/(t \pm \sqrt{q}\,)\mathbb{Z}_\ell[t]$, and T_2 is a module over $R_2 = \mathbb{Z}_\ell[t]/P_1(t)(t \pm \sqrt{q}\,)\mathbb{Z}_\ell[t]$. By Theorem 3.2, for any 3×3 nilpotent matrix N such that $\mathrm{Np}(P_1(t \mp \sqrt{q}\,)t)$ lies on or above $\mathrm{Yp}(N)$ there exists an R_2-module T_2 such that t acts on $T_2/\ell T_2$ with the matrix $N \mp \sqrt{q} I_3$. Then $T = R_1 \oplus T_2$ is the desired Tate module.

Suppose now that we have a module T from the case (7c(ii)). Let $P(t) = tP_1(t \mp \sqrt{q}\,)$. By Proposition 5.3, there exists a matrix factorization (X, Y) such that $\det X = f_A(t \mp \sqrt{q}\,)$ and $YX = P(t)$. Moreover, $X \equiv \mathrm{diag}(t^2, t^2) \bmod \ell$. Define T' by the presentation:

$$\mathbb{Z}_\ell[t]^2 \xrightarrow{Y} \mathbb{Z}_\ell[t]^2 \to T' \to 0. \tag{3}$$

Note that $\det Y = P(t)^2/f_A(t \mp \sqrt{q}\,) = P_1(t \mp \sqrt{q}\,)$, and $Y \equiv \mathrm{diag}(t, t) \bmod \ell$. Thus T' is a module over $R' = \mathbb{Z}_\ell[t]/P_1\mathbb{Z}_\ell[t]$. By Theorem 3.1, such a module exists iff $\mathrm{Np}(P_1(t \mp \sqrt{q}\,))$ lies on or above the Young polygon $\mathrm{Yp}(1, 1)$. It follows that if T exists then ℓ^2

divides $P_1(\mp\sqrt{q}\,)$. On the other hand if ℓ^2 divides $P_1(\mp\sqrt{q}\,)$, then we can construct a module T' over R' such that F acts on $T'/\ell T'$ with the matrix $\mp\sqrt{q}I_2$. By Proposition 5.3, there exists a matrix factorization (Y, X) such that $\det Y = P_1(t \mp \sqrt{q}\,)$ and $XY = P(t)$. Then the matrix factorization (X, Y) corresponds to a desired module T. □

7. Kummer surfaces

Suppose $p \neq 2$. Let A be an abelian surface, and let $\tau : A \to A$ be the involution $a \mapsto -a$. Let $p_A : A \to A/\tau$ be the quotient map. The variety A/τ is singular, and $p_A(A[2])$ is the singular locus. Let $\sigma : S \to A/\tau$ be the blow up of A/τ in $p_A(A[2])$. Then S is smooth. It is called a *Kummer surface*. In this section we compute zeta functions of Kummer surfaces in terms of the zeta functions of the covering abelian surfaces.

Let X be a variety over a finite field $\mathbb{F}_q$, and let N_d be the number of points of degree 1 on $X \otimes \mathbb{F}_{q^d}$. The zeta function of X is the formal power series

$$Z_X(t) = \exp\left(\sum_{d=1}^{\infty} \frac{N_d t^d}{d}\right).$$

In fact, $Z_X(t)$ is rational. For an abelian variety A we have the following formula:

$$Z_X(t) = \prod_{i=0}^{2g} P_i(t)^{(-1)^{i+1}}, \tag{4}$$

where $P_i(t) = \det(1 - tF | \bigwedge^i V_\ell(A))$. Note that if $f_A(t) = \prod(t - \omega_j)$, then

$$P_i(t) = \prod_{j_1 < \cdots < j_i} (1 - t\omega_{j_1} \cdots \omega_{j_i}).$$

In particular, $P_1(t) = t^{2g} f_A(\frac{1}{t})$, and $Z_A(t) = Z_B(t)$ if and only if A and B are isogenous.

First we prove a general formula for the zeta function of a Kummer surface S.

Theorem 7.1. *Let*

$$Z_A(t) = \prod_{i=0}^{4} P_i(A, t)^{(-1)^{i+1}}$$

be the zeta function of an abelian surface A. Then

$$Z_S(t) = (1 - t)^{-1} P(t)^{-1} \big(1 - q^2 t\big)^{-1}, \tag{5}$$

where

$$P(t) = P_2(A, t) \prod_{a \in A[2]} \big(1 - (qt)^{\deg a}\big). \tag{6}$$

In particular

$$\big|S(k)\big| = \frac{f_A(1) + f_A(-1)}{2} + q\big|A[2](k)\big|. \tag{7}$$

Proof. Since S is the blow up of X, we have

$$Z_X(t) = Z_S(t) \prod_{a \in A[2]} \big(1 - (qt)^{\deg a}\big).$$

Let us prove that

$$\big|X(\mathbb{F}_{q^r})\big| = \frac{f_r(1) + f_r(-1)}{2},$$

where $f_r = \det(t - F^r)$ is the Weil polynomial of $A_r = A \otimes \mathbb{F}_{q^r}$. Put

$$A(r) = A_r[2](\mathbb{F}_{q^r}).$$

By [7, IV.19.4], $f_A(n) = \deg(n - F)$ for $n \in \mathbb{Z}$, were deg means the degree of an isogeny. There are two types of possible fibers of the map p_A over a nonsingular $\mathbb{F}_{q^r}$-point of X.

(1) The fiber is a union of two points of degree 1. There are $\frac{f_r(1) - A(r)}{2}$ such fibers.
(2) The fiber is a point of degree 2. There are $\frac{f_r(-1) - A(r)}{2}$ such fibers.

This gives the desired equality.

Let $f_r(t) = t^4 + a_1(r)t^3 + a_2(r)t^2 + a_1(r)q^r t + q^{2r}$, then $a_2(r) = \operatorname{tr}(F^r | H^2(\overline{A}, \mathbb{Q}_\ell))$, and

$$\begin{aligned} Z_X(t) &= \exp\left(\sum_{r=1}^{\infty} \frac{(f_r(1) + f_r(-1))t^r}{2r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty} \frac{t^r}{r}\right) \exp\left(\sum_{r=1}^{\infty} \frac{a_2(r)t^r}{r}\right) \exp\left(\sum_{r=1}^{\infty} \frac{q^{2r}t^r}{r}\right) \\ &= (1-t)^{-1} P_2(A,t)^{-1} \big(1 - q^2 t\big)^{-1} \end{aligned}$$

The last equality follows from lemma C.4.1 of [4]. □

Now we classify the zeta functions of $A[2]$ in terms of the Weil polynomial f_A. Let b_r be the number of points of degree r on $A[2]$. Then $P(t) = P_2(A,t) \prod_r (1 - (qt)^r)^{b_r}$. We compute the numbers b_r using Theorem 6.1.

Suppose first that f_A is separable, and assume that $f_A(t) \equiv (t+1)^4 \bmod 2$. Note that the slopes of $\operatorname{Np}(f_A(t+1))$ may be greater than 1. This may create many unnecessary

cases in the table below. However, we can use the polynomial $f(t) = f_A(t + \lambda)$ instead of $f_A(t+1)$, where $\lambda \equiv 1 \bmod \ell$, satisfying the property that slopes of $\mathrm{Np}(f(t))$ are less then or equal to 1. Equivalently, we take $\mathrm{Np}(f_A(t+1))$ and change all its slopes that are greater than 1 to 1. This operation simplifies the notation, and clearly, it does not change the final answer, since all the slopes of Young polygons are not greater than 1. (See Tables 1–4.)

Table 1
Case (5) of Theorem 6.1.

Slopes of $\mathrm{Np}(f(t))$	b_i
$(1/4)$	$b_1 = 2,\ b_2 = 1,\ b_4 = 3$
$(1/3, 1)$	$b_1 = 2,\ b_2 = 1,\ b_4 = 3$ $b_1 = 4,\ b_2 = 2,\ b_4 = 2$
$(1/2, 1/2)$	$b_1 = 2,\ b_2 = 1,\ b_4 = 3$ $b_1 = 4,\ b_2 = 2,\ b_4 = 2$ $b_1 = 4,\ b_2 = 6$
$(2/3, 1)$, $(1/2, 1, 1)$ or $(3/4)$	$b_1 = 2,\ b_2 = 1,\ b_4 = 3$ $b_1 = 4,\ b_2 = 2,\ b_4 = 2$ $b_1 = 4,\ b_2 = 6$ $b_1 = 8,\ b_2 = 4$
$(1, 1, 1, 1)$	$b_1 = 2,\ b_2 = 1,\ b_4 = 3$ $b_1 = 4,\ b_2 = 2,\ b_4 = 2$ $b_1 = 4,\ b_2 = 6$ $b_1 = 8,\ b_2 = 4$ $b_1 = 16$

If $f_A(t) \not\equiv (t+1)^4 \bmod 2$, then

Table 2
Cases (1)–(4) of Theorem 6.1.

$f_A(t) \bmod 2$	
$t^4 + t^3 + t^2 + t + 1$	$b_1 = 1,\ b_5 = 3$
$t^4 + t^3 + t + 1$ and 4 does not divide $f_A(1)$	$b_1 = 2,\ b_2 = 1,\ b_3 = 2,\ b_6 = 1$
$t^4 + t^3 + t + 1$ and 4 divides $f_A(1)$	$b_1 = 2,\ b_2 = 1,\ b_3 = 2,\ b_6 = 1$ $b_1 = 4,\ b_3 = 4$
$t^4 + t^2 + 1$ and 4 does not divide $a_1 + a_2 + 1 - 2q$	$b_1 = 1,\ b_3 = 1,\ b_6 = 2$
$t^4 + t^2 + 1$ and 4 divides $a_1 + a_2 + 1 - 2q$	$b_1 = 1,\ b_3 = 5$ $b_1 = 1,\ b_3 = 1,\ b_6 = 2$

If f_A is not separable, we have three cases of Theorem 6.1. Let $f_A(t) = P_A(t)^2$ then

Table 3
Case (6) of Theorem 6.1.

$P_A(t) \bmod 2$	
$t^2 + t + 1$	$b_1 = 1,\ b_3 = 5$
$t^2 + 1$ and 4 does not divide $P_A(1)$	$b_1 = 4,\ b_2 = 6$
$t^2 + 1$ and 4 divides $P_A(1)$	$b_1 = 4,\ b_2 = 6$ $b_1 = 8,\ b_2 = 4$ $b_1 = 16$

If $f_A(t) = (t \pm \sqrt{q})f(t)$, then

Table 4
Case (7) of Theorem 6.1.

$f(t)$ mod 2	
$t^2 + t + 1$	$b_1 = 4$, $b_3 = 4$
$t^2 + 1$	$b_1 = 8$, $b_2 = 4$
and 4 does not divide $f(1)$	$b_1 = 4$, $b_2 = 2$, $b_3 = 2$
$t^2 + 1$	$b_1 = 16$
and 4 divides $f(1)$	$b_1 = 8$, $b_2 = 4$
	$b_1 = 4$, $b_2 = 6$
	$b_1 = 4$, $b_2 = 2$, $b_3 = 2$

Finally, if $f_A(t) = (t \pm \sqrt{q})^4$, then $b_1 = 16$.

Acknowledgments

I am deeply grateful to Alexander Kuznetsov, who communicated his unfinished results on zeta functions of Kummer surfaces to me and provided many useful corrections on the early version of the paper. I thank Michael A. Tsfasman for his attention to this work. I am grateful to Alexey Zykin and referees for suggesting many useful corrections and comments on the paper.

References

[1] G. Banaszak, W. Gajda, P. Krason, On the image of l-adic Galois representations for abelian varieties of type I and II, Doc. Math. Extra Coats (2006) 35–75.
[2] M. Demazure, Lectures on p-Divisible Groups, Lect. Notes Math., vol. 302, Springer, 1972.
[3] A. Grothendieck, Éléments de géométrie algébrique IV. Étude locale des śchemas et des morphismes de schémas, Quatrième partie, Publ. Math. IHÉS 32 (1967) 5–361.
[4] R. Hartshorne, Algebraic Geometry, Grad. Texts Math., vol. 52, Springer-Verlag, New York, Heidelberg, 1977.
[5] D. Maisner, E. Nart, Abelian surfaces over finite fields as Jacobians, Exp. Math. 11 (3) (2002) 321–337, with an appendix by Everett W. Howe.
[6] J. Milne, Abelian varieties, http://www.jmilne.org/math/CourseNotes/av.html, 2008.
[7] D. Mumford, Abelian Varieties, Tata Inst. Fund. Res. Stud. Math., vol. 5, Oxford University Press, London, 1970.
[8] M. Pohst, H. Zassenhaus, Algorithmic Algebraic Number Theory, Encycl. Math. Appl., vol. 30, Cambridge University Press, Cambridge, 1997, revised reprint of the 1989 original.
[9] S. Rybakov, The groups of points on abelian varieties over finite fields, Cent. Eur. J. Math. 8 (2) (2010) 282–288, arXiv:0903.0106v4.
[10] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (2) (1966) 134–144.