MATH SCAND 60 (1987), 151 178

ON SUPERSINGULAR CURVES AND ABELIAN VARIETIES

TORSTEN EKEDAHL *

Introduction.

The present article contains a number of results on the theme of supersingular (s.s.) curves and as an inevitable consequence of supersingular abelian varieties. (By definition an abelian variety in positive characteristic is supersingular if the first crystalline cohomology group has all its slopes equal to 1/2 and a curve is supersingular if its Jacobian is). In [10] Ogus proves that there is a one-to-one correspondence between isomorphism classes of s.s. abelian varieties and isomorphism classes of F-crystals with all their slopes 1/2 together with a determinant (when the base field is algebraically closed and the dimensions are different from 1). We begin by studying the same problem when a polarization is also thrown in. Our first result will be that every polarization on a supersingular F-crystal is isomorphic to one coming from a polarization on the associated abelian variety. It is not true however that two non-isomorphic polarizations on a supersingular abelian variety give non-isomorphic polarizations on the associated F-crystal even if the polarizations are principal.

We make a closer study of this phenomenon in the case of principal polarizations on the product of s.s. elliptic curves. The usual techniques (Tamagawa number = 1) give a formula for the mass of the set of principal polarizations on such a product and we give a formula for the mass of the set of indecomposable principal polarizations and this enables us to completely determine when such a product admits an indecomposable principal polarization.

We then continue to consider the problem of the existence of s.s. curves. We show that if the genus is larger than $\frac{1}{2}(p^2-p)$ where p is the characteristic of the base field then there is no curve whose Jacobian is the product of s.s. elliptic curves of that genus. In addition to that I am only able to give some examples constructed from Fermat curves.

---

* Supported by a grant from the Swedisch Natural Science council.
Received February 8, 1985; in revised version January 1, 1986.

In chapter III we consider how to classify pencils of s.s. curves of genus 2. This result was at least implicitly obtained by Oort (cf. [12]). The only contribution I give is to make it explicit and also to give the result in a more general form. We then apply this result to the study of the total space of pencils over P^1 whose Jacobian is an abelian scheme.

The interested reader could do well to consult a series of papers by Ihukiyama, Katsura and Oort (to appear) which consider very related topics.

I would like to thank N. Katz for some interesting and even useful discussions on subjects pertaining to this paper and to the I.H.E.S. for providing the necessary ambiance.

1. Polarizations of s.s. abelian varieties.

1. Let K be a field and M a central simple algebra over K of dimension H. Recall that if $\mathrm{Trd}: M \to K$ is the reduced trace then $a \mapsto a^* := \mathrm{Trd}(a).1 - a$ is an involution of M over K. We extend this involution to $M_n(M)$ by $(a_{ij})^* = (a_{ji}^*)$. Symmetric elements, of $M_n(M)$ with respect to $(-)^*$, are then in $1-1$ correspondence with hermitian forms $(-,-): M^n \times M^n \to M$. Explicitly $\varphi \mapsto \langle -, \varphi(-)\rangle$ where $\langle -, -\rangle$ is the standard hermitian form for which the standard basis of M^n forms an orthonormal set. The group of unitary elements ($\varphi \in M_n(M), \varphi\varphi^* = 1$) are then the K-rational points of the algebraic group $\mathrm{Aut}(\langle -, -\rangle)$ of automorphisms of $\langle -, -\rangle$.

If $M = M_2(K)$ and $(-)^\dagger$ is the standard involution $(a_{ij})^\dagger = (a_{ji})$ on M and if

$$e = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M$$

then $a^* = e^{-1}a^\dagger e$. Hence if we put

$$M_n(M) \ni E = \begin{pmatrix} e & & 0 \\ & e & \\ 0 & & \ddots \end{pmatrix}$$

then $a \mapsto Ea$ gives a one-to-one correspondence between $*$-symmetric matrices and alternating matrices in $M_{2n}(K)$. Similarly, $\mathrm{Aut}(\langle -, -\rangle)$ is conjugate by E to $\mathrm{Sp}_{2n}(K)$ and $*$-hermitian forms on M^n correspond to alternating forms on K^{2n}. As $e \in \mathrm{GL}_2(\mathbf{Z})$ this works if we replace K by any commutative ring.

Going back to the case where M is just central simple I claim that there exists a unique polynomial function Pf: ($*$-symmetric elements of $M_n(M)$) $\to K$ such that $\mathrm{Pf}(1) = 1$ and $\mathrm{Pf}(a)^2 = \mathrm{Nrd}(a)$. Indeed, unicity being clear we may, by descent, assume that $M = M_2(K)$ and then we can put $\mathrm{Pf}(a) = \mathrm{pf}(Ea)$

where pf is the usual pfaffian on alternating matrices. By unicity we see that $\mathrm{Pf}(xax^*) = \mathrm{Nrd}(x)\cdot \mathrm{Pf}(a)$ for $x \in M_n(M)$. The correspondence above allows us to define Pf on hermitian forms. Note that if two forms have the same non-zero pfaffian then any isomorphism between them have reduced norm 1. Similarly, in the case of 2×2 matrices, when we replace K by any ring and non-zero by non-zero divisor.

2. For results and definitions concerning abelian varietes I will use [8] as standard reference. This will not always be mentioned. For our purposes [8] is lacking somewhat in the p-adic theory. I will solve this problem mostly by ignoring it, hence leaving to the reader the task of extending the results on the l-adic theory. Only at a few points will I discuss how to do this explicitly. (It is clearly §23 of [8] which is needed for this extension.)

Let us begin with a general discussion of polarizations: let k be a perfect field of characteristic $p > 0$, let A be an abelian variety over k and let $\hat{A}$ be its dual abelian variety. We put

$$H_1(A,l) := H^1(\hat{A}_{\bar{k}}, \mathbf{Z}_l(1)), \quad H_1(\hat{A},l) := H^1(A_{\bar{k}}, \mathbf{Z}_l(1))$$

as $\mathrm{Gal}(\bar{k}/k)$-modules and

$$H_1(A,p) := H^1_{\mathrm{cris}}(\hat{A}/W), \quad H_1(\hat{A},p) := H^1_{\mathrm{cris}}(A/W)$$

as F-crystals. If $\dim A = g$ the trace maps give identifications, for every prime r, $\det H_1(A,r) = \mathbf{Z}_r(g)$ (as $\mathrm{Gal}(\bar{k}/k)$-modules and F-crystals, respectively) where $\mathbf{Z}_p(g) := H^2_{\mathrm{cris}}(\boldsymbol{P}^1_k/W)^{\otimes g}$.

Recall that a polarization of degree n, $n > 0$, of A is a morphism $\varphi: A \to \hat{A}$ such that (over $\bar{k}$) there exists an ample linebundle $\mathscr{L}$ with $\chi(\mathscr{L}) = n$ and such that $\varphi = \varphi_{\mathscr{L}}: x \mapsto T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. Then φ is an isogeny of degree n^2 (and is sometimes called a polarization of degree n^2). By functoriality we get morphisms

$$\varphi_r: H_1(A,r) \to H_1(\hat{A},r).$$

Using the Riemann forms and the fact that they are alternating we get a morphism

$$\varphi'_r: \Lambda^2 H_1(A,r) \to \mathbf{Z}_r(1).$$

Note that when $\varphi = \varphi_{\mathscr{L}}$ then φ'_r corresponds under

$$\mathrm{Hom}(\Lambda^2 H_1(A,r), \mathbf{Z}_r(1)) = \mathrm{Hom}(\mathbf{Z}_r(1), \Lambda^2 H^1(A,r))$$

to the Chern-class of $\mathscr{L}$.

The trace maps enable us to speak of bases of the underlying $\mathbf{Z}_l$-, respectively W-module, of determinant 1. Two such bases differ by a linear transformation of determinant 1. As the pfaffian of an alternating form is unchanged under a base change of determinant 1 we may unambigously speak of $\mathrm{pf}(\varphi'_r)$.

LEMMA 2.1. $\mathrm{pf}(\varphi'_r) = n$.

We will first need another description of the pfaffian. If R is a commutative ring, M a free R-module of finite rank $2n$ and $\varphi: \Lambda^2 M \to R$ an alternating form, the pfaffian can be considered as a morphism $\mathrm{pf}(\varphi): \Lambda^{2n} M \to R$. I claim that $n!\mathrm{pf}(\varphi) = \varphi \wedge \varphi \ldots \wedge \varphi$ (n times). Indeed, we reduce to R a field and φ non-degenerate by universal example and then we choose a basis such that φ has standard form and compute

$$(x_1 \wedge y_1 + x_2 \wedge y_2 + \ldots + x_n \wedge y_n)^n = n!(x_1 \wedge y_1 \wedge x_2 \wedge y_2 \ldots x_n \wedge y_n).$$

This shows that $\mathrm{pf}(\varphi'_r)$ is $1/g!$ times the gth cup power of the Chern class of an $\mathscr{L}$ such that $\varphi = \varphi_{\mathscr{L}}$ (always possible as we may assume $k = \bar{k}$). We then use the Riemann-Roch formula (cf. [8, §20, Theorem 3]).

More generally, if $\varphi: \Lambda^2 H_1(A, r) \to \mathbf{Z}_r(1)$ is a morphism we may define its pfaffian which will be an element of $\mathbf{Z}_r$.

DEFINITION 2.2. i) An r-adic polarization of A is a morphism $\varphi: \Lambda^2 H_1(A, r) \to \mathbf{Z}_r(1)$ (in the appropriate category) with a non-zero pfaffian. Its degree is $\mathrm{pf}(\varphi)$. An isomorphism of polarizations φ and φ' is an automorphism of $H_1(A, r)$ taking φ to φ' and of determinant 1.

ii) A $\mathbf{Q}_r$-polarization of A is a morphism $\varphi: \Lambda^2 H_1(A, r) \otimes_{\mathbf{Z}} \mathbf{Q} \to \mathbf{Q}_r(1)$ (in the appropriate category) with a non-zero pfaffian. Its degree is $\mathrm{pf}(\varphi)$. Idem for isomorphisms.

iii) An adic polarization of A is a set $\{\varphi_r, r \text{ prime}\}$ of r-adic polarizations such that there exists an $n \in \mathbf{Z}$, $n > 0$, with $\mathrm{pf}(\varphi_r) = n$ for all n. Idem for degree and isomorphisms.

iv) An adelic polarization of A is a set $\{\varphi_r, r \text{ prime}\}$ a finite number of which are $\mathbf{Q}_r$-polarizations and the rest r-adic polarizations such that there exists an $n \in \mathbf{Z}, n > 0$, with $\mathrm{pf}(\varphi_r) = n$ for all n. Its degree is n. An isomorphism of φ and φ' is a set $\{\psi_r, r \text{ prime}\}$ a finite set of which are isomorphisms of $\mathbf{Q}_r$-polarizations and the rest are r-adic polarizations. (This set may be larger than the corresponding ones for φ and φ'.)

REMARK. By the results of 1 we see that if we consider two r-adic, $\mathbf{Q}_r$-adic, adic or adelic polarizations of the same degree then the condition of determinant 1 for a candidate for an automorphism between them is automatic.

By Lemma 2.1 we see that a polarization of A gives rise to an adic polarization of A of the same degree and isomorphisms of polarizations give rise to isomorphisms of the associated adic polarizations.

The elements of $\mathrm{Hom}(A, \hat{A})$ of the form (over $\bar{k}$) $\varphi_{\mathscr{L}}$ for some linebundle $\mathscr{L}$ are exactly those elements which are symmetric for the involution $\varphi \mapsto \varphi^* = \hat{\varphi}\mathrm{ev}$ where $\mathrm{ev}: A \to \hat{A}$ is the biduality isomorphism (cf. [8, §20 Theorem 2 and Remark 3]). Similarly the r-adic (etc.) polarizations are exactly the monomorphisms of $\mathrm{Hom}(H_1(A, r), H_1(\hat{A}, r))$ (etc.) symmetric for the involution $\varphi \mapsto \varphi^* = \hat{\varphi}\mathrm{ev}$.

DEFINITION 2.3. A rational polarization of A is an element $\varphi \in \mathrm{Hom}^0(A, \hat{A})$ $(:= \mathrm{Hom}(A, \hat{A}) \otimes \mathbf{Q})$ such that for some $m \in \mathbf{Z}$, $m > 0$, $m\varphi \in \mathrm{Hom}(A, \hat{A})$ and $m\varphi$ is a polarization. Its degree is $\mathrm{Pf}(\varphi)$ where $\mathrm{Pf}(-)$ is the polynomial function on symmetric elements of $\mathrm{Hom}^0(A, \hat{A})$ whose value on $\varphi_{\mathscr{L}}$ (over $\bar{k}$) is $\chi(\mathscr{L})$. Two rational polarizations φ and φ' are isomorphic if $\varphi' = \hat{\psi}\varphi\psi$ for some $\psi \in \mathrm{Aut}^0(A)$ of degree 1.

If we fix some polarization φ_M then

$$\mathrm{Hom}^0(A, \hat{A}) \xrightarrow{\varphi_M^{-1}} \mathrm{End}^0(A, A)$$

is an isomorphism and the involution $(-)^*$ is mapped into the Rosati involution. Furthermore, the rational polarizations correspond to elements φ of $\mathrm{End}^0(A, A)$ which are symmetric for the Rosati involution and such that the polynomial $\varrho_\varphi(t)$ with $\varrho_\varphi(n) = \mathrm{Pf}'(n + \varphi)$ has all its roots negative, where Pf' is defined by transport from $\mathrm{Hom}^0(A, \hat{A})$.

It is now clear that there is a group scheme Aut_φ whose integral points are the automorphisms of φ, whose rational points are the automorphisms of the associated rational points and, if $\mathrm{End}_k(A, A) \otimes \mathbf{Z}_r = \mathrm{End}(H_1(A, r))$, whose $\hat{\mathbf{Z}}$-points are the automorphisms of the associated adic polarization and whose $\boldsymbol{A}^f$-points are the automorphisms of the associated adelic polarization. Hence the set of isomorphism classes of polarizations whose adic and rational polarizations are isomorphic to those of φ is in one-to-one correspondence with $\mathrm{Aut}_\varphi(\mathbf{Q}) \backslash \mathrm{Aut}_\varphi(\boldsymbol{A}^f) / \mathrm{Aut}_\varphi(\hat{\mathbf{Z}})$.

REMARK. The only part of this not explicitly proved in [8] is the fact that if $\mathscr{L}$ is a linebundle with $\chi(\mathscr{L}) \neq 0$ and $i(\mathscr{L}) = 0$ then $\mathscr{L}$ is ample. This however follows from the proof of the Theorem of §17 where in fact only these conditions are used to conclude that $\mathscr{L}^3$ is very ample.

3. Suppose now that $k = \bar{k}$. Recall that A is said to be supersingular if $H_1(A, p)$ has all its slopes equal to 1/2. This implies (cf. [10, §6]) that $\mathrm{End}(A) \otimes \mathbf{Z}_r = \mathrm{End}(H_1(A, r))$ for all r.

THEOREM 3.1. *Let A be supersingular. Then every adic polarization is isomophic to the adic polarization associated to a polarization.*

PROOF. The case of $\dim A = 1$ is trivial and left to the reader.

Let us now note that if φ and φ' are $\mathbf{Q}_r$-adic polarizations of the same degree then they are isomorphic. Similarly, if φ and φ' are r-adic polarizations, $r \neq p$, of the same degree which is an r-adic unit. For the case $r \neq p$ this is clear as we then deal with perfect alternating forms. For the p-adic part we know that A is isogenous to the product E^g (cf. [12], where E is a super singular elliptic curve. Let ψ be the polarization on A which is the pullback of the product polarization on E^g by such an isogeny. Using this polarization we see that φ and φ' corresponds to elements of

$$\mathrm{End}(H_1(A), H_1(A)) \otimes \mathbf{Q}_p = \mathrm{End}(A, A) \otimes \mathbf{Q}_p \simeq M_g(\mathrm{End}(E) \otimes \mathbf{Q}_p)$$

symmetric with respect to the Rosati involution on $\mathrm{End}(E) \otimes \mathbf{Q}_p$ extended in the usual way to $g \times g$-matrices. By [8, §21, Theorem 2] the Rosati involution on $\mathrm{End}(E; E) \otimes \mathbf{Q}_p$ is isomorphic to $a \mapsto \mathrm{Trd}\, a - a$. We thus see, applying the discussion of 1, that φ and φ' correspond to hermitian forms of rank g over $\mathrm{End}(E) \otimes \mathbf{Q}_p$. By diagonalization we are reduced to the case when φ and φ' are of rank 1 that is $\varphi(xe, ye) = ax^*y$ and $\varphi'(xe', ye') = a'x^*y$ where e and e' are base and $a, a' \in \mathbf{Q}_p^*$. Now as

$$K_{p^2} = W(\boldsymbol{F}_{p^2}) \otimes \mathbf{Q}_p$$

splits $\mathscr{A}$ we may embed $K_{p^2} \subseteq \mathscr{A}$ and then for $\lambda \in K_{p^2}$

$$\lambda^* \lambda = N_{K_{p^2}/\mathbf{Q}_p}(\lambda).$$

As $K_{p^2}/\mathbf{Q}_p$ is unramified every element in $\mathbf{Z}_p$ is a norm of an element in K_{p^2}. Changing bases of $\mathscr{A}e$ and $\mathscr{A}e'$ we may assume that $a' = p^r a$. Similarly, embedding $\mathbf{Q}_p(\sqrt{p})$ in $\mathscr{A}$ we get $f \in \mathscr{A}$ with $f^* f = p$ so again by changing bases we get $a' = a$ so φ is isomorphic to φ'.

Let us now construct a rational polarization of the same degree n as the given adic polarization φ'. Using the polarization ψ this corresponds to finding a symmetric element φ of $M_g(\mathrm{End}^0(E))$ such that the polynomial $\varrho_\varphi(t)$ with $\varrho_\varphi(m) = \mathrm{Pf}'(m + \varphi)$ has all its roots negative and $\varrho_\varphi(0) = n$. Now it is clear, by unicity, that $\mathrm{Pf}'(-) = \chi(\mathscr{M})\mathrm{Pf}(-)$ where $\mathrm{Pf}(-)$ is the function of section 1. If we put $r = n/\chi(\mathscr{M})$ and let φ be the matrix with diagonal entries $r, 1, 1 \ldots 1$ and zero off the diagonal then $\mathrm{Pf}(m + \varphi) = (m + \mathrm{r})(m + 1)^{g-1}$ and as $r > 0$ we get what we want.

By the first part of the proof the adic polarizations associated to φ and φ' are isomorphic. Hence there exists $\alpha \in G(\boldsymbol{A}^f)$, where G is the algebraic group of elements of reduced norm 1 of $\mathrm{End}(A)$, such that ψ takes $\varphi \otimes_{\mathbf{Q}} \boldsymbol{A}^f$ to $\varphi' \otimes_{\hat{\mathbf{Z}}} \boldsymbol{A}^f$. As G is a form of SL_{2g} it is semi-simple and simply connected. As $g > 1$ $G(\mathbf{R})$ is non-compact so that we can apply the strong approximation theorem (cf. [10]) and write $\psi = \psi_2^{-1}\psi_1$ where $\psi_1 \in G(\mathbf{Q})$ and $\psi_2 \in G(\hat{\mathbf{Z}})$. Applying ψ_2 to φ' and ψ_1 to φ we may assume that $\varphi \otimes_{\mathbf{Q}} \boldsymbol{A}^f = \varphi' \otimes_{\hat{\mathbf{Z}}} \boldsymbol{A}^f$. Thus φ is at the same time rational and adic so integral and hence a polarization whose associated adic polarization clearly is φ'.

4. Let us take a closer look at the problem of classifying l-adic and rational polarizations.

LEMMA 4.1. *Let $\langle -, - \rangle : \Lambda^2 M \to \mathbf{Z}_l$ be a non-degenerate alternating pairing. Then $\langle -, - \rangle$ is isomorphic to $\perp_i l^{n_i}(-, -)$, where $(-, -)$ is the standard perfect alternating pairing of rank 2. The set with multiplicities $\{n_i\}$ is determined by $\langle -, - \rangle$ and $pf(-, -\rangle = l^{\Sigma n_i}$ unit.*

Indeed, by dividing $\langle -, - \rangle$ by as high a power of l as possible we may assume that $\langle -, - \rangle$ is not divisible by l. Thus there exists $m_1, m_2 \in M$ such that $\langle m_1, m_2 \rangle$ is a unit and then m_1 and m_2 generate a hyperbolic plane which we may split off. We then continue with the complement. The unicity is left to the reader and the calculation of the pfaffian is clear.

We therefore get

COROLLARY 4.1.1. *The isomorphism classes of l-adic polarizations of degree n on A are in $1-$ to -1 correspondence with sequences $n_1 \leqq \ldots \leqq n_g$ of natural numbers such that $v_l(n) = \sum_{i=1}^{g} n_i$.*

As for rational polarizations they correspond to hermitian positive definite forms of rank g over $\mathscr{A} := \mathrm{End}^0(E, E)$. Any such form can be diagonalized and the diagonal coefficients are positive rational numbers. Using the well known fact, which is proved as above by embedding various quadratic fields into $\mathscr{A}$, that every positive rational number is the norm of an element of $\mathscr{A}$ we see that any such form is equivalent to the standard one. This gives

PROPOSITION 4.2. *All rational polarizations of the same degree are isomorphic.*

We now divide the isomorphism classes of polarizations of A into genus classes, two polarizations belonging to the same genus iff their associated rational and adic polarizations are isomorphic.

From (4.2) it follows that we need only check that their adic polarizations

are isomorphic and from (4.1.1) it follows that the only reasonably complicated genus invariant is its associated p-adic polarization.

As will be seen below a genus class may contain several isomorphism classes.

5. Let us further specialize to $A = E^g$, E an elliptic curve, and polarizations of degree 1 on A.

We begin by the p-adic polarizations. We thus have the F-crystal $M = E_{1/2}^g$ where

$$E_{1/2} := W_\sigma[F]/(F^2 - p)$$

and we want to classify $\varphi : \Lambda^2 M \to \mathbf{Z}_p(Z)$ with $\mathrm{pf}(\varphi) \neq 0$, $1_1, F_1, 1_2, F_2 \ldots, 1_g, F_g$ being a base of determinant 1.

Using the standard φ with $M = \perp_{i=1}^g E_{1/2}$ and $\langle 1, F\rangle = 1$ we transfer the problem to the study of $(\varphi_{ij}) = \varphi \in M_g(\mathscr{A})$, with $\mathscr{A} = \mathrm{End}_{F\text{-crys}}(E_{1/2})$, symmetric for $\varphi \to \varphi^* = (\varphi_{ji}^*)$, with $a^* \to \mathrm{Trd}\, a - a$ and $\mathrm{Pf}(\varphi) = 1$. Of course these correspond to perfect hermitian forms φ of rank g over $\mathscr{A}$.

PROPOSITION 5.1. *All principal p-adic polarizations on E^g are isomorphic to products* $\perp (E_{1/2}, \langle -, - \rangle)$.

We first want to prove that φ can be diagonalized. Clearly φ is not divisible by p. I now claim that this implies that there is some $x \in \mathscr{A}^g$ with $\varphi(x, x) \notin p\mathscr{A}$. If not then

$$\varphi(x, y) + \varphi(x, y)^* \in p\mathscr{A} \quad \text{for all } x, y \in \mathscr{A}^g.$$

As $\mathscr{A}/\mathrm{Rad}\,\mathscr{A} \simeq \boldsymbol{F}_{p^2}$ with $\bar{\lambda}^* = \bar{\lambda}^p$ we see that there is some $\lambda \in \mathscr{A}$ such that $\lambda^* - \lambda \notin \mathrm{Rad}\,\mathscr{A}$. Then

$$\varphi(\lambda x, y) + \varphi(\lambda x, y)^* = \lambda^* \varphi(x, y) + \lambda \varphi(x, y)^* \in p\mathscr{A}$$

so $(\lambda^* - \lambda)\varphi(x, y) \in p\mathscr{A}$ and as $\lambda^* - \lambda$ is a unit $\varphi(x, y) \in p\mathscr{A}$ for all x, y. Now $\varphi|\mathscr{A}x$ is perfect so we may split off $\mathscr{A}x$ and continue by induction. We now continue as for $\mathscr{A} \otimes \mathbf{Z}_p$-forms. We may thus assume that φ is of rank 1. As $\mathscr{A}$ is the unique maximal order we can embed $W(\boldsymbol{F}_{p^2}) \subseteq \mathscr{A}$ and so if $\varphi(xe, ye) = ax^*y$ we may find $\lambda \in W(\boldsymbol{F}_{p^2})$ such that $N_{W(\boldsymbol{F}_{p^2})/\mathbf{Z}_p}(\lambda) \cdot a = 1$. Changing basis from e to ye we get φ isomorphic to the standard form.

We thus see that in particular

PROPOSITION 5.2. *The principal polarizations on E^g form a single genus.*

Using section 2 we see that the set S of isomorphism classes of pairs (B, φ) where B is a s.s. abelian variety whose crystalline cohomology is isomorphic

to that of A and φ is a principal polarization on B is in 1-to-1 correspondence with $G(\mathbf{Q})\backslash G(\boldsymbol{A}^f)/G(\hat{\mathbf{Z}})$ where $G = \operatorname{Aut}\varphi'$ and where φ' is the standard polarization on $A = E^g$. We also see (cf. [8, §21]) that

$$G = \{A \in M_g(\mathscr{E}) : AA^* = 1\}$$

where $\mathscr{E} = \operatorname{End}(E)$ is a maximal order in a quaternion algebra over $\mathbf{Q}$ ramified exactly at p and ∞. Recall that the mass M_i of S_i is defined to be

$$\sum_{\varphi \in S_i} \frac{1}{\#\operatorname{Aut}\varphi(\mathbf{Z})}.$$

Using that the Tamagawa number of G is one, one can compute M_i and I quote the result from [3]:

$$M_n = \frac{\zeta(2)\zeta(4)\ldots\zeta(2n).1!.3!\ldots(2n-1)!}{(2\pi)^{n(n+1)}} \prod_{i=1}^{n} p^i + (-1)^i. \tag{5.3}$$

Using the formula for $\zeta(2i)$ this can be rewritten (cf. [13, VII. Proposition 7]

$$M_n = \frac{B_1}{4.1}\frac{B_2}{4.2}\cdot\cdots\cdot\frac{B_n}{4n}\cdot\prod_{i=1}^{n}(p^i+(-1)^i). \tag{5.4}$$

We will mainly be interested in indecomposable polarizations i.e. those not of the form $(B', \varphi') \perp (B'', \varphi'')$ so we begin by a discussion of how to compare the mass of all polarizations with the mass of the indecomposable ones.

6. To emphasize the purely combinatorial aspect of this comparison we will put ourselves in a more general situation.

DEFINITION 6.1. i) A graded groupoid is a groupoid $\mathscr{G}$ together with a function $\varphi : \pi_0(\mathscr{G}) \to \mathbf{N}$ from the set of isomorphism classes of objects of $\mathscr{G}$ to the natural numbers.

ii) $(\mathscr{G}, \varphi)$ is of finite type if $\operatorname{Aut}_{\mathscr{G}}(a)$ is finite for all $a \in \operatorname{ob}\mathscr{G}$ and φ has finite fibers.

iii) If $(\mathscr{G}, \varphi)$ is of finite type then its mass $\mathscr{M}(\mathscr{G})$ is

$$\sum_{a \in \pi_0(\mathscr{G})} \frac{t^{\varphi(a)}}{\#\operatorname{Aut}\mathscr{G}(a)} \in \mathbf{Q}[[t]].$$

iv) $(\mathscr{G}, \varphi)$ is positive if $\operatorname{Im}\varphi \subseteq \mathbf{Z}_+$.

Given a graded groupoid $(\mathscr{G}, \varphi)$ we define a new graded groupoid $P(\mathscr{G})$

as follows. Its objects are functions $\varphi: [n] \to \mathrm{ob}(\mathscr{G})$ for some $n \in \mathbf{N}$ where $[n] = \{0, 1, 2 \ldots n-1\}$. A morphism $\varphi_1 \to \varphi_2$ is an isomorphism of sets $\varrho: \mathrm{Dom}\,\varphi_1 \to \mathrm{Dom}\,\varphi_2$ together with morphisms $\varrho_i: \varphi_1(i) \to \varphi_2(\varrho(i))$ for all $i \in \mathrm{Dom}\,\varphi_1$. Composition is the obvious one. We have a functor $\perp: P(\mathscr{G}) \times P(\mathscr{G}) \to P(\mathscr{G})$ given on objects by $\mathrm{Dom}(\varphi_1 \perp \varphi_2) = [\sharp \mathrm{Dom}\,\varphi_1 + \sharp \mathrm{Dom}\,\varphi_2]$ and $\varphi_1 \perp \varphi_2(i) = \varphi_1(i)$ if $i < \sharp \mathrm{Dom}\,\varphi_1$, $\varphi_2(i - \sharp \mathrm{Dom}\,\varphi_1)$ if $i \geqq \sharp \mathrm{Dom}\,\varphi 1$. Then $\perp$ is a coherently associative and commutative product (cf. [1]) with unit $[0] \to \mathrm{ob}(\mathscr{G})$. We define a functor $\mathscr{G} \to P(\mathscr{G})$ by $a \mapsto (0, a) \in [1] \times \mathrm{ob}\,\mathscr{G}$. Furthermore, we grade $P(\mathscr{G})$ by

$$\varphi'(\psi: [n] \to \mathrm{ob}(\mathscr{G})) = \sum_{i \in [n]} \varphi(\psi(i)).$$

LEMMA 6.2. i) *If $\mathscr{G}$ is of finite type and positive then $P(\mathscr{G})$ is of finite type.*

ii) *Let $\mathscr{N}$ be a category with a coherently associative and commutative product $\oplus$ with unit 0 and let $\psi: \mathscr{G} \to \mathscr{N}$ be a functor. Up to natural equivalence there exists a unique $\psi': P(\mathscr{G}) \to \mathscr{N}$ commuting with products and units and such that $\psi = \psi' \circ \tau$. If $(\mathscr{N}, \varphi'')$ a graded groupoid such that $\varphi''(0) = 0$ $\varphi''(a \oplus b) = \varphi''(a) + \varphi''(b)$ and $\varphi = \varphi'' \circ \psi$ then $\varphi' = \varphi'' \circ \psi'$.*

iii) *ψ' is an equivalence of categories iff for all finite ordered sets $A_1, \ldots, A_n$ and $A'_1, \ldots, A'_m$ of $\mathrm{ob}\,\mathscr{G}$ all morphisms between $\psi(A_1) \oplus \psi(A_2) \ldots \oplus \psi(A_n)$ and $\psi(A'_1) \oplus \psi(A'_2) \ldots \psi(A'_m)$ can be written uniquely as a product of permutations of factors and isomorphisms coming from $\mathscr{G}$ and all objects of $\mathscr{N}$ are isomorphic to such a product.*

PROOF. It is clear that i) is true. An extension as in ii) is given by

$$\psi'(\varrho: [n] \to \mathrm{ob}\,\mathscr{G}) = (\psi(\varrho(0)) \oplus \psi(\varrho(1))) \oplus \psi(\varrho(2))) \ldots \psi(\varrho(n-1)))$$

and the rest of the proof is left to the reader.

We can now state and prove the intended result

PROPOSITION 6.3. *Let $\mathscr{G}$ be a positive graded groupoid of finite type. Then*

$$\mathscr{M}(P(\mathscr{G})) = \exp(\mathscr{M}(\mathscr{G})) \in \mathbf{Q}[[t]]. \tag{6.3.1}$$

For any graded groupoid $\mathscr{H}$ we define $\mathbf{Q}[[\mathscr{H}]]$, the ring of power series of finite monomials in the variables X_α, $\alpha \in \pi_0(\mathscr{H})$. If $X_{\alpha_1} X_{\alpha_2} \ldots X_{\alpha_r}$ is a monomial in $\mathbf{Q}[[\mathscr{H}]]$ we define its weight to be $\sum_{i=1}^{r} \varphi(\alpha_i)$ and we define the weight of an element of $\mathbf{Q}[[\mathscr{H}]]$ to be the minimum of the weights of all monomials occurring with non-zero coefficients in the given element. We can then define a topology on $\mathbf{Q}[[\mathscr{H}]]$ by saying that $a_i \to 0$ if their weights tends

to infinity. If $\mathscr{H}$ is of finite type then

$$\mathscr{H}(X) = \sum_{\alpha \in \pi_0(\mathscr{H})} X_\alpha$$

converges and if $\eta_{\mathscr{H}}$ denotes the continous ring homomorphism $\mathbf{Q}[[\mathscr{H}]] \longrightarrow \mathbf{Q}[[t]]$ such that

$$\eta_{\mathscr{H}}(X_\alpha) = \frac{t^{\varphi(\alpha)}}{\sharp \mathrm{Aut}(\alpha)},$$

then $\eta_{\mathscr{H}}(\mathscr{H}(X)) = \mathscr{M}(\mathscr{H})$. Now let $\mathscr{P}' : \mathrm{ob}(P(\mathscr{G})) \to$ monomials in $\mathbf{Q}[[\mathscr{G}]]$ be defined by

$$\mathscr{P}'(\psi : [n] \to \mathrm{ob}(\mathscr{G}) = \prod_{i \in [n]} X_{\psi(i)}.$$

This factors to give $\mathscr{P} : \pi_0(\mathscr{P}(\mathscr{G})) \to$ monomials in $\mathbf{Q}[[\mathscr{G}]]$. Let F: monomials in $\mathbf{Q}[[\mathscr{G}]] \to \mathbf{Q}[[\mathscr{G}]]$ take

$$X_{\alpha_1}^{n_1} X_{\alpha_2}^{n_2} \cdots X_{\alpha_r}^{n_r} \quad \text{to} \quad \frac{1}{n_1! n_2! \ldots n_r!} X_{\alpha_1}^{n_1} X_{\alpha_2}^{n_2} \cdots X_{\alpha_r}^{n_r}.$$

The composite $F \circ \mathscr{P}$ extends by continuity to a ring homomorphism

$$Q : \mathbf{Q}[[P(\mathscr{G})]] \to \mathbf{Q}[[\mathscr{G}]].$$

LEMMA 6.3.1. *The diagram*

$$\begin{array}{ccc} \mathbf{Q}[[P(\mathscr{G})]] & \xrightarrow{Q} & \mathbf{Q}[[\mathscr{G}]] \\ & {\scriptstyle \eta_{P(\mathscr{G})}} \searrow \quad \swarrow {\scriptstyle \eta_{\mathscr{G}}} & \\ & \mathbf{Q}[[t]] & \end{array}$$

PROOF. Let β be the class of $A = \tau(A_1) \perp \tau(A_2)^{n_2} \ldots \perp \tau(A_r)^{n_r}$ in $\pi_0(P(\mathscr{G}))$ where $A_i \in \mathrm{ob}\,\mathscr{G}$ are non-isomorphic. By definition

$$\mathrm{Aut}(A) = \mathrm{Aut}(A_1)^{n_1} \wr \Sigma_{n_1} \times \mathrm{Aut}(A_2)^{n_2} \wr \Sigma_{n_2} \times \ldots \times \mathrm{Aut}(A_r)^{n_r} \wr \Sigma_{n_r}$$

where the symmetric groups Σ_{n_i} act by permutation of factors. Hence

$$\eta_{P(\mathscr{G})}(X_\beta) = \sum_{i=1}^{r} \frac{t^{\varphi(A_i) \cdot n_i}}{(\sharp \mathrm{Aut}(A_i))^{n_i} \Leftrightarrow n_i!}.$$

Let α_i be the class of A_i. Then

$$Q(X_p) = \prod_{i=1}^{r} \frac{X_{\alpha_i}^{n_i}}{n_i!} \quad \text{and} \quad \eta_{\mathscr{G}}(X_{\alpha_i}) = \frac{t^{\varphi(\alpha_i)}}{\sharp \mathrm{Aut}(A_i)}.$$

Hence $\eta_{P(\mathscr{G})}(X_\beta) = \eta_{\mathscr{G}} \circ Q(X_\beta)$ and as all β in $\pi_0(\mathscr{P}(\mathscr{G}))$ are of this form we can conclude the Lemma.

The proof of the proposition can now be finished. We have

$$Q(P(\mathscr{G})(X)) = \sum_{\substack{n_1 < n_2 < \ldots n_r \\ \alpha_1, \ldots, \alpha_r \in \pi_0(\mathscr{G})}} \frac{X_{\alpha_1}^{n_1} \ldots X_{\alpha_r}^{n_r}}{n_1! . n_2! \ldots n_r!} = \exp\left(\sum_{\alpha \in \pi_0(\mathscr{G})} X_\alpha \right) = \exp(\mathscr{G}(X)).$$

We now apply the lemma and the continous homomorphism $\eta_{\mathscr{G}}$ to get $\mathscr{M}(P(\mathscr{G})) = \exp(\mathscr{M}(\mathscr{G}))$.

COROLLARY 6.3.2. *Put*

$$M_i = \sum_{\substack{\alpha \in \pi_0(P(\mathscr{G})) \\ \varphi'(\alpha) = i}} \frac{1}{\sharp \mathrm{Aut}(\alpha)} \quad \textit{and} \quad M_i' = \sum_{\substack{\alpha \in \pi_0(\mathscr{G}) \\ \varphi(\alpha) = i}} \frac{1}{\sharp \mathrm{Aut}(\alpha)}.$$

Then for all n

$$(6.3.3) \quad nM_n = nM_n' + (n-1)M_{n-1}'M_1 + (n-2)M_{n-2}'M_2 \ldots + M_1'M_{n-1}.$$

PROOF. From the proposition we get $\exp(\sum M_i' t^i) = \sum M_i t^i$. Taking the logarithmic derivative on both sides gives

$$\sum i M_i' t^{i-1} = \frac{\sum i M_i t^{i-1}}{\sum M_i t^i}.$$

Now multiply by $\sum M_i t^i$ on both sides.

7. The following result is what is needed to apply the results of the last section to principal polarizations.

PROPOSITION 7.1. *Let $k = \bar{k}$ and let $(A_1, \varphi_1)(A_2, \varphi_2) \ldots (A_r, \varphi_r)$ and $(A_1', \varphi_1') \ldots (A_s', \varphi_s')$ be indecomposably principally polarized varieties over k. Then any isomorphism*

$$\psi : (A_1, \varphi_1) \perp (A_2, \varphi_2) \ldots (A_r, \varphi_r) \to (A_1', \varphi_1') \perp \ldots \perp (A_s', \varphi_s')$$

can be written uniquely as a product of isomorphisms between factors and permutations of factors.

PROOF. We can recover the indecomposable factors of a polarization by considering its theta divisor and for each irreducible component of it consider the connected component of the subgroup of the abelian variety whose translations leave this component stable. Gathering together the components of the theta divisor with the same such subgroup we get an indecomposable component (as the quotient of the abelian variety by this subgroup).

Hence if we let S be a set of isomorphism classes of abelian varieties stable under sums and direct factors such that for each dimension there is only a finite number of elements of S with this dimension we can let $\mathcal{G}(S)$ be the groupoid of pairs (A, φ) with $A \in S$ and φ an indecomposable principal polarization on A. Then $\mathcal{G}(S)$ graded by the dimension of A is a graded groupoid positive and of finite type and $P\mathcal{G}(S)$ is equivalent to the category of principal polarizations on elements of S.

Let us further specialize to the case that actually interests us, namely that where S is the set of classes of s.s. abelian varieties whose crystalline cohomology is isomorphic to that of E^g for some g and E an elliptic curve.

Note first that by [10, Corollary 6.7], S consists of E^g, $g \neq 1$, plus all s.s. elliptic curves.

Hence we get

THEOREM 7.2. *Let M'_n, $n \neq 1$, be the mass of indecomposable principal polarizations on E^n and $M'_1 = M_1$ (cf. (5.3)). Then*

$$(7.2.1) \qquad nM_n = nM'_n + (n-1)M'_{n-1}M_1 + (n-2)M'_{n-2}M_2 + \ldots + M'_1 M_{n-1}.$$

Using (5.4) we get

$$(7.3) \qquad M_1 = \frac{p-1}{24}, \quad M_2 = \frac{(p-1)(p^2+1)}{2^7 \cdot 3^2 \cdot 5}, \quad M_3 = \frac{(p-1)(p^2+1)(p^3-1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7},$$

$$(7.4) \qquad M'_1 = \frac{p-1}{24}, \quad M'_2 = \frac{(p-1)(p-2)(p-3)}{2^8 \cdot 3^2 \cdot 5},$$

$$M'_3 = \frac{(p-1)^2(p-2)(p^3+3p^2-6p+24)}{2^{10} \cdot 3^3 \cdot 5 \cdot 7}.$$

PROPOSITION 7.5. i) *M'_n is a polynomial in p of degree $\dfrac{n(n+1)}{2}$.*

ii) *$M'_n \geq 1/nM_n$ if $n > 6$ ($n > 4$ if $p \neq 2$).*

iii) *$M'_n \neq 0$ iff $(n, p) \neq (2, 2), (2, 3)$ or $(3, 2)$.*

PROOF. To prove i) we need only observe that by (5.4), M_n is a polynomial

in p of degree $n(n+1)/2$ so one proves by induction that M_n' is a polynomial of the same degree using (7.2.1) and the fact that by the induction hypothesis $iM_i'M_{n-1}$, $i < n$, has smaller degree than M_n. Let us continue to ii) and iii). We will need a lemma

LEMMA 7.5.1. i) *If* $n \geqq 3$ *then* $\dfrac{nM_n}{(n-1)M_{n-1}} \leqq \dfrac{(n+1)M_{n+1}}{nM_n}$.

ii) $3M_3M_2 \leqq M_5$, $2M_2'M_2 \leqq M_4$, $5M_5M_1 \leqq M_6$.

iii) If $p \neq 2$, $4M_4M_1 \leqq M_5$, $3M_3'M_1 \leqq M_4$, $M_1M_3 \leqq M_4$.

Before proving this we will see how it implies ii) and iii). It is clear that ii) will follow from (7.2.1) if we can prove that $iM_i'M_j \leqq M_{i+j}$ if $i+j \geqq 6$ ($i+j \geqq 4$ if $p \neq 2$).

The case $i+j = 4$ is taken care of by ii) and iii) of the lemma and as $M_i' \leqq M_i$ it suffices to show that $iM_iM_j \leqq M_{i+j}$ if $i+j \geqq 6$ ($i+j \geqq 5$ if $p \neq 2$). Again ii) and iii) takes care of $i+j = 6$ ($i+j = 5$) and i) allows us to pass from $iM_iM_j \leqq M_{i+j+0}M_j \leqq M_{i+j+1}$ and $iM_iM_{j+1} \leqq M_{i+j+1}$ as it implies that

$$\frac{(k+1)M_{k+1}}{kM_k} \leqq \frac{(l+1)M_{l+1}}{lM_l} \quad 3 \leqq k \leqq l.$$

By ii) we get iii) for $n \geqq 6$ ($n \geqq 4$ if $p \neq 2$) and (7.4) takes care of $n \leqq 3$ so it leaves only M_4' and M_5' for $p = 2$, which is done by explicit computation using, of course, (7.2.1) and (5.4).

We can now set out to prove the lemma. Using (5.4), i) for $n = 3$ says that

$$\frac{3B_3(p^3-1)}{2.4.3} \leqq \frac{4B_4(p^4+1)}{3.4.4}$$

and using $B_3 = 1/42$ and $B_4 = 1/30$ we get $15(p^3-1) \leqq 14(p^4+1)$ but

$$15(p^3-1) \leqq 14p(p^3-1) = 14(p^4-p) \leqq 14(p^4+1).$$

In a similar fashion one proves ii) and iii) so we are left with i) for $n \geqq 4$ which says that

$$\frac{2n\pi^2}{(n^2-1)(2n+1)} \leqq \frac{\zeta(2n+2)}{\zeta(2n)} \frac{p^{n+1}+(-1)^{n+1}}{p^n+(-1)^n}.$$

However,

$$\frac{\zeta(2n+1)}{\zeta(2n)} > \frac{1}{\zeta(2n)} \geqq \frac{1}{\zeta(4)} \geqq \frac{2}{3}$$

and I claim that

$$\frac{p^{n+1}+(-1)^{n+1}}{p^n+(-1)^n} \geqq \frac{3}{2}.$$

Indeed, this is equivalent to $p^n(2p-3) \geqq (-1)^n 5$ which is clearly a true inequality as $n > 4$. Hence

$$\frac{\zeta(2n+2)}{\zeta(2n)} \frac{p^{n+1}+(-1)^{n+1}}{p^n+(-1)^n} \geqq 1$$

so we will be finished if we can prove that

$$\frac{2n\pi^2}{(n^2-1)(2n+1)} \leqq 1.$$

Now

$$\frac{2n\pi^2}{(n^2-1)(2n+1)} \leqq \frac{\pi^2}{n^2-1}$$

which is < 1 for $n \geqq 4$.

2. Supersingular curves.

1. In section I, 7.5 we have completely answered the question of when the product of s.s. elliptic curves admits an indecomposable principal polarization. If the dimension of this product is 2 or 3, then, as is well known, every indecomposable principal polarization is obtained by endowing the abelian variety in question with a structure of Jacobian of à smooth, projective curve and taking its associated polarization.

Hence in these dimensions we have decided when the product of s.s. elliptic curves is a Jacobian. In higher dimensions much less is known. I will show that if the genus of a curve is greater than $\frac{1}{2}(p^2-p)$ then its Jacobian is never such a product. Apart from that I will only be able to give a systematic procedure for producing examples.

THEOREM 1.1. *Let C be a curve over k, algebraically closed of characteristic $p > 0$, of genus g. If its Jacobian is isomorphic to the product of* s.s. *elliptic curves then*

i) $g \leqq \frac{1}{2}(p^2-p)$

ii) $g \leqq \frac{1}{2}(p-1)$ if C is hyperelliptic and $(p,g) \neq (2,1)$.

PROOF. Assume first that C is non-hyperelliptic and let $(J(C), \Theta)$ be its Jacobi-

an where Θ is the canonical polarization. Then $\mathrm{Aut}\, C \oplus \{\pm 1\} = \mathrm{Aut}(J(C), \Theta)$. Hence any descent for $(J(C), \Theta)$ gives by projection onto the first factor descent data for C so if $(J(C), \Theta)$ descends to some subfield of k then so does C and the jacobian of the descended curve is either isomorphic to the descent of $J(C)$ or the twist of it by multiplication by -1 over some quadratic extension.

There always exist a s.s. elliptic curve E over $\boldsymbol{F}_{p^2}$ whose Frobenius is multiplication by p. Hence the same is true for E^g and in particular

$$\mathrm{Hom}_{\boldsymbol{F}_{p^2}}(E^g, E^g) = \mathrm{Hom}_k(E^g, E^g)$$

so any polarization of E^g defined over k descends to $E^g/\boldsymbol{F}_{p^2}$. Therefore C descends to $\boldsymbol{F}_{p^2}$ with the Frobenius acting on $H^1_{\text{ét}}(C_{\boldsymbol{F}_{p^2}}, \mathbf{Z}_l)$ by multiplication by p or $-p$. Hence the number of rational points of C over $\boldsymbol{F}_{p^2}$ is either $1-2gp+p^2$ or $1+2gp+p^2$.

Suppose now that $g > \frac{1}{2}(p^2-p)$. The first case then gives

$$\#(C(\boldsymbol{F}_{p^2})) < 1-(p^2-p)p+p^2 = -p^3+p^2+1 < -2p^2+p^2+1 = 1-p^2 < 0$$

which is absurd.

The other case gives the Frobenius for C over $\boldsymbol{F}_{p^4}$ equal to p^2 and hence

$$1+2gp+p^2 = \#C(\boldsymbol{F}_{p^2}) \leqq \#C(\boldsymbol{F}_{p^4}) = 1-2gp^2+p^4$$

so $2g(p+p^2) \leqq p^4-p^2$ which contradicts $2g > p^2-p$.

REMARK. That the Frobenius can never be $\pm p$ for a curve over F_{p^2} of genus $> \frac{1}{2}(p^2-p)$ I learned from Serre (cf. [14]).

Let now C be hyperelliptic. Then $\mathrm{Aut}(C) = \mathrm{Aut}(J(C), \Theta)$ so as above we can descend C to $\boldsymbol{F}_{p^2}$ this time with the Frobenius equal to p. Hence $\#C(\boldsymbol{F}_{p^2}) = 1-2gp+p^2 \geqq 0$. Now I claim that $1-2gp+p^2$ is not equal to 1 unless $(p, g) = (2, 1)$.

Indeed, if this were the case then $2g = p$ which is clearly impossible if p is odd. If $p = 2$ we get $g = 1$ which is excluded by assumption. As $1-2gp+p^2$ is congruent to 1 modulo p we get $1-2gp+p^2 \geqq p+1$ (if $(p, g) \neq (2, 1)$) hence $p-1 \geqq 2g$ which is what we wanted as ii) clearly implies i) when C is hyperelliptic.

REMARK. a) We will see later that when $g = \frac{1}{2}(p^2-p)$ (respectively $g = \frac{1}{2}(p-1)$) then there is a curve (respectively hyperelliptic curve) of genus g in characteristic p whose Jacobian is the product of s.s. elliptic curves.

b) We saw in the proof that a curve C whose Jacobian is the product of s.s. elliptic curves descends to $\boldsymbol{F}_{p^2}$ with the Frobenius $\pm p$. Conversely

PROPOSITION. 1.2. *Let A be an abelian variety over $\boldsymbol{F}_{p^2}$, $q = p^n$ with its*

Frobenius being equal to multiplication by $\pm q$. *Then* $F^n = 0$ *on* $H^1(A, \mathcal{O}_A)$. *In particular, if* q *is a prime then* A *is the product of* s.s. *elliptic curves (over* $\boldsymbol{F}_{p^2}$).

PROOF. If we let F_{q^2} denote the Frobenius with respect to $\boldsymbol{F}_{q^2}$ and F the absolute Frobenius then $F^{2n} = F_{q^2}$ on $H^1_{\text{cris}}(A/W)$. Hence $F^{2n} = \pm p^n$. Now $p^n = F^n V^n$ and F is injective on $H^1_{\text{cris}}(A/W)$ so $F^n = \pm V^n$ but

$$H^1(A, \mathcal{O}_A) = H^1_{\text{cris}}(A/W)/VH^1_{\text{cris}}(A/W).$$

This proves the first part. The second part follows from [11]. (It would seem that [11] only gives the result over $\overline{\boldsymbol{F}_{p^2}}$ but we may choose E such that F_{p^2} is multiplication by the same integer as for A and then the isomorphism descends).

2. Let C be a ring, free of finite type as Z-module such that $C \otimes_{\mathbf{Z}} \mathbf{Q}$ is a semi-simple Q-algebra. Let $\bar{\mathbf{Q}}$ be an algebraic closure of Q and let S be the set of isomorphism classes of irreducible representations of $C \otimes_{\mathbf{Z}} \bar{\mathbf{Q}}$. The Galois group of $\bar{\mathbf{Q}}$ over Q will act on S_{ij}; if $C \to M_r(\bar{\mathbf{Q}})$ is a representative of $\alpha \in S$ and σ an automorphism of $\bar{\mathbf{Q}}$ then $C \to M_r(\bar{\mathbf{Q}}) \xrightarrow{\sigma} M_r(\bar{\mathbf{Q}})$ is a representative of $\sigma(\alpha)$. If K is an algebraically closed field of characteristic 0 containing $\bar{\mathbf{Q}}$ then extension of scalars identifies S with the set of isomorphism classes of irreducible representations of $C \otimes_{\mathbf{Z}} K$.

Similarly, if p is a prime such that $C \otimes_{\mathbf{Z}} \boldsymbol{F}_p$ is a semi-simple $\boldsymbol{F}_p$-algebra choosing an algebraic closure $\overline{\boldsymbol{F}_p}$ of $\boldsymbol{F}_p$ we can define S_p to be the set of isomorphism classes of irreducible representations of $C \otimes_{\mathbf{Z}} \overline{\boldsymbol{F}_p}$. This set is identified with the set of isomorphism classes of irreducible representations of $C \otimes_{\mathbf{Z}} k$ where k is any (algebraically closed) overfield of $\overline{\boldsymbol{F}_p}$. We also get an action of $\text{Gal}(\overline{\boldsymbol{F}_p}/\boldsymbol{F}_p)$ on S_p.

Let $K_p \subseteq \bar{\mathbf{Q}}$ be the maximal subfield of $\bar{\mathbf{Q}}$ unramified at p and let R_p be its ring of integers. A choice of maximal ideal, m, in R_p lying over p and a choice of isomorphism between R_p/m and $\overline{\boldsymbol{F}_p}$ give rise to an isomorphism between S and S_p in the following way. Let R_m be the localization of R_p at m. Any representation $\varrho: C \to M_r(\bar{\mathbf{Q}})$ is conjugate to some ϱ' with $\varrho'(C) \subseteq R_m$ and reduction modulo m gives us a representation $C \to M_r(\boldsymbol{F}_p)$. This gives us a well defined mapping $S \to S_p$ which is the searched for isomorphism. This isomorphism is compatible with the action of Galois groups.

Suppose now that k is an algebraically closed field such that $C \otimes_{\mathbf{Z}} k$ is semi-simple. Suppose further that we are given an abelian variety A over k and a morphism of rings $\varrho: C \to \text{End}_k(A)$ such that $H^1_{\text{DR}}(A/k)$ is a sum of pairwise non-isomorphic irreducible $C \otimes k$-modules.

REMARK. This situation is essentially a complex multiplication situation.

It can be shown that the simple factors of A have complex multiplication by the image, in the endomorphism ring, of the part of the center of $C \otimes \mathbf{Q}$ stabilizing that factor. Conversely, if A has complex multiplication by K, a finite extension of $\mathbf{Q}$, over k and if $(K \cap \mathrm{End}(A)) \otimes k$ is reduced then $(A, K \cap \mathrm{End}(A), K \cap \mathrm{End}\, A \to \mathrm{End}\, A)$ fulfills the condition above. If K is unramified at $p := \mathrm{char}\, k$ then after possibly changing A by an isogeny $(K \cap \mathrm{End}(A)) \otimes k$ can be supposed to be reduced.

The theory to be presented below may suitably generalized so as to cover the general case.

If we choose an embedding of $\overline{\boldsymbol{F}_p}$ in k ($\boldsymbol{F}_0 := \bar{\mathbf{Q}}$) we can identify the isomorphism classes of the irreducible factors of $H^1_{\mathrm{DR}}(A/k)$ as $C \otimes_{\mathbf{Z}} k$-module with a subset of S_p which we will denote S_p.

LEMMA 2.1. *S_ϱ is stable under the action of*

$$\mathrm{Gal}(\overline{\boldsymbol{F}_p}/\boldsymbol{F}_p) \quad (\boldsymbol{F}_0 := \mathbf{Q}).$$

Indeed, as the irreducible factors of a representation is determined by the value of its character on C it suffices to show that the values on C of the character of $H^1_{\mathrm{DR}}(A/k)$ lie in $\boldsymbol{F}_p$. This, of course, is well-known and follows from the trace formula.

We now divide S_ϱ into S^0_ϱ and S^1_ϱ where S^0_ϱ are the classes of irreducible representations occuring in $H^0(A, \Omega^1_{A/k})$ and S^1_ϱ the ones occuring in $H^1(A, \mathcal{O}_A)$. The canonical exact sequence

$$0 \to H^0(A, \Omega^1_A) \to H^1_{\mathrm{DR}}(A/k) \to H^1(A, \mathcal{O}_A) \to 0$$

shows that S_ϱ is the disjoint union of S^0_ϱ and S^1_ϱ. We call $(S_\varrho, S^0_\varrho, S^1_\varrho)$ the type of (A, C, ϱ).

REMARK. When $C \otimes \mathbf{Q}$ provides A with complex multiplication this is what is called the CM-type of $(A, C \otimes \mathbf{Q})$.

It is clear that these constructions are compatible with specialization in the following sense. If R is a discrete valuation ring with residue field k and $\bar{K}$ is an algebraic closure of the fraction field of K and if A is an abelian scheme over R with a ring homomorphism $\varrho: C \to \mathrm{End}_R(A)$ then we can consider (after having made some choices)

$$(S_p, S_{p,\varrho}, S^0_{p,\varrho}, S^1_{p,\varrho}) \quad \text{and} \quad (S_q, S_{q,\varrho}, S^0_{q,\varrho}, S^1_{q,\varrho})$$

where $p = \mathrm{char}\, K$ and $q = \mathrm{char}\, k$. After some further choices we can identify S_p and S_q and under this identification $(S_{p,\varrho}, S^0_{p,\varrho}, S^1_{p,\varrho})$ corresponds to $(S_{q,\varrho}, S^0_{q,\varrho}, S^1_{q,\varrho})$ and we have compatibility for Galois actions.

Having made these definitions we can specialize to the case when k is of positive characteristic p. Then $\mathrm{Gal}(\bar{\boldsymbol{F}}_p/\boldsymbol{F}_p)$ equals $\hat{\mathbf{Z}}$ with generator σ, the Frobenius automorphism. As $C \otimes k$ is semi-simple, $C \otimes W$, $W = W(k)$, is a separable W-algebra. Hence the isotypical decomposition

$$H^1_{\mathrm{DR}}(A/k) = \bigoplus_{\alpha \in S_\varrho} \bar{V}_\alpha$$

lifts to

$$H^1_{\mathrm{cris}}(A/W) = \bigoplus_{\alpha \in S_\varrho} V_\alpha.$$

Now F and V are σ, respectively σ^{-1}, linear and commutes with the action of C so it takes $V_\alpha(V_{\sigma\alpha})$ to $V_{\sigma\alpha}$ (respectively V_α).

PROPOSITION 2.2. *If $\alpha \in S^0_\varrho$ then $F\colon V_\alpha \to V_{\sigma\alpha}$ is an isomorphism and if $\alpha \in S^1_\varrho$ it equals p times an isomorphism.*

PROOF. We know that the kernel of $H^1_{\mathrm{cris}}(A/W) \to H^1(A, \mathcal{O}_A)$ is the image of V. Hence $\alpha \in S^0_\varrho$ iff V_α is in the image of V.

Furthermore, as $\bar{V}_\beta = V_\beta/pV_\beta$ is an irreducible $C \otimes k$-module for all $\beta \in S_\varrho$, F (respectively V): $V_\alpha \to V_{\sigma\alpha}$ (respectively: $V_{\sigma\alpha} \to V_\alpha$) is either an isomorphism or divisible by p. Now $FV = VF = p$ so either $F\colon V_\alpha \to V_{\sigma\alpha}$ is an isomorphism and $V\colon V_{\sigma\alpha} \to V_\alpha$ is an isomorphism times p or vice versa and we have just seen that $V\colon V_{\sigma\alpha} \to V_\alpha$ is an isomorphism iff $\alpha \in S^1_\varrho$.

Let $\overline{S^\varrho}$ denote the set of orbits of σ on S_ϱ. For each $\beta \in \overline{S_\varrho}$ we define the F-crystal $M_\beta := \bigoplus_{\alpha \in \beta} V_\alpha$, so that

$$H^1_{\mathrm{cris}}(A/W) = \bigoplus_{\beta \in \overline{S_\varrho}} M_\beta$$

as F-crystals, and $\overline{M_\beta} := M_\beta/VM_\beta$, so that

$$\bigoplus_{\beta \in \overline{S_\varrho}} \overline{M_\beta} = H^1(A, \mathcal{O}_A)$$

compatible with the action of Frobenius. To each orbit β we associate a number of invariants. First we put $\dim \beta$ equal to the dimension of $\bar{V}_\alpha$ for any $\alpha \in \beta$. Then we divide $\beta \cap S^1_\varrho$ into disjoints sets $\{\alpha_1, \sigma\alpha_1, \sigma^2\alpha_1, \ldots, \sigma^{r_1}\alpha_1\}$, $\{\alpha_2, \sigma\alpha_2, \ldots, \sigma^{r_2}\alpha_2\}$ ... where the α_i have the property that either $\sigma^{-1}\alpha_i$ and $\sigma^{r_i+1}\alpha_i$ belong to S^0_ϱ or $\sigma^{r_i+1}\alpha_i = \alpha_i$. We then associate to β the set, with multiplicities, $n_\beta = \{r_i : \alpha_i \neq \sigma^{r_i+1}\alpha_i\}$.

THEOREM 2.3. i) *M_β is an F-crystal of rank $\#\beta \cdot \dim \beta$ and all its slopes are $\#(\beta \cap S^0_\varrho)/\#\beta$ (here $\#(-)$ denotes cardinality).*

ii) *The F-nilpotent part of* M_β *is isomorphic to* $(\oplus_{i \in n_\beta} k[F]/(F^{i+1}))^{\dim \beta}$.

PROOF. This is clear from (2.2).

REMARK. In the CM-case i) is the Shimura-Taniyama relation. Using the extension of the results given here that was mentioned earlier one gets a proof of the Shimura-Taniyama relations in general.

We can now use ii) to decide when A is the product of s.s. elliptic curves. Indeed, this is, as was observed earlier, equivalent to F being 0 on $H^1(A, \mathcal{O}_A)$ and we see that this is true iff $\alpha \in S_\wp^1$ implies that $\sigma\alpha \in S^0$.

Suppose now that A is defined over some number field $K \subseteq \bar{\mathbf{Q}}$ still with $C \to \mathrm{End}_K A$ and $C \otimes \bar{\mathbf{Q}}$ having a multiplicity free action on $H^1_{\mathrm{DR}}(A_{\bar{\mathbf{Q}}}/\bar{\mathbf{Q}})$. Let $\mathcal{G} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, let $\mathcal{C} \subseteq \mathcal{G}$ be the subgroup of automorphisms acting trivially on the maximal CM-extension of $\mathbf{Q}$ and suppose that $\mathcal{C}$ acts trivially on $S_\wp$ or equivalently that for all $\alpha \in S_\wp$ the character values of α on the center of C generate a CM field (this turns out always to be the case but in the case we will consider it will be completely obvious). We can then unambiguously speak about the action of complex conjugation on $S_\wp$ which we will denote by τ. It is clear, by Hodge theory for instance, that τ will permute $S_\wp^0$ and $S_\wp^1$. Let $\mathcal{H}$ be the subgroup of $\mathcal{G}$ stabilizing (setwise) $S_\wp^0$ and $S_\wp^1$.

We assume that we have chosen a prime $\mathfrak{p}$ in $\bar{\mathbf{Q}}$ such that A has good reduction at $\mathfrak{p}$ and that $C \otimes_\sharp k(\mathfrak{p})$ is semi-simple. This gives us a well defined element σ, the Frobenius in $\mathcal{G}/\mathcal{N}$ where $\mathcal{N}$ is the Kernel of the permutation representation of $\mathcal{G}$ on $S_\wp$. By our criterion $A_{k(\mathfrak{p})}$ is the product of s.s. elliptic curves iff $\sigma(S_\wp^1) = S_\wp^0$. As τ has this property we get

PROPOSITION 2.4. *The reduction modulo* $\mathfrak{p}$ *of* A *is isomorphic to the product of* s.s. *elliptic curves iff*

$$\sigma \in \tau\mathcal{H}/\mathcal{N}.$$

The case we are interested in is when we have a curve C, smooth and projective, with a finite group G acting on C such that $\mathbf{Z}[G] \to \mathrm{End}(J(C))$ fulfills our conditions. As the character values in this case will generate a cyclotomic field our condition on C acting trivially is certainly fulfilled. Indeed, if the exponent of G is n the charcter values will always lie in the field obtained from $\mathbf{Q}$ by adjoining a primitive nth root unity. Hence we get

COROLLARY 2.4.1. *Let* C *be a curve over* K *with an action of a finite group* G *of exponent* n *such that all irreducible representations of* G *occurs at most once in* $H^1_{\mathrm{DR}}(C_{\bar{\mathbf{Q}}}/\bar{\mathbf{Q}})$. *If* $p \equiv -1(n)$ *and* C *has good reduction* $\bar{C}$ *modulo* p *then* $J(\bar{C})$ *is (geometrically) isomorphic to the product of* s.s. *elliptic curves.*

Pairs (C, G) as in the corollary seem to be very rare. Indeed, the only examples of curves of this type that I know of are obtained as abelian covers of $\boldsymbol{P}^1$ ramified at 3 points. This is the case we will now set out to discuss.

Let $C \to \boldsymbol{P}^1$ be an abelian cover of $\boldsymbol{P}^1$ ramified at 0,1 and ∞ over an algebraically closed field k of characteristic prime to the order of the covering. Let A denote the structure group and suppose $nA = 0$ with $(n, \operatorname{char} k) = 1$. Then such coverings are classified by elements of

$$H^1_{\text{ét}}(\boldsymbol{P}^1 \setminus \{0, 1, \infty\}, A) = \operatorname{Hom}(\boldsymbol{\mu}_n^2, A).$$

The covering is connected iff the corresponding homomorphism $\boldsymbol{\mu}_n^2 \to A$ is surjective which we will assume from now on. Hence it is the quotient of the covering corresponding to $\mathrm{id}: \boldsymbol{\mu}_n^2 \to \boldsymbol{\mu}_n^2$ by the kernel B of $\boldsymbol{\mu}_n^2 \to A$.

The covering $\{x^n + y^n = 1\} \to \{t = x^n\}$ is a connected $\boldsymbol{\mu}_n^2$-covering ramified at $\{0, 1, \infty\}$ so the associated mapping $\boldsymbol{\mu}_n^2 \to \boldsymbol{\mu}_n^2$ is a surjective homomorphism between finite groups of the same order and hence an isomorphism. It is clear that it takes $\boldsymbol{\mu}_n \oplus 0$ to $\boldsymbol{\mu}_n \oplus 0$ and $0 \oplus \boldsymbol{\mu}_n$ to $0 \oplus \boldsymbol{\mu}_n$ and if we make our identification

$$H^1_{\text{ét}}(\boldsymbol{P}^1 \setminus \{0, 1, \infty\}, \boldsymbol{\mu}_n) = \operatorname{Hom}(\boldsymbol{\mu}_n \oplus \boldsymbol{\mu}_n \ \sigma \ \boldsymbol{\mu}_n) = \mathbf{Z}/n \oplus \mathbf{Z}/n$$

such that

$$k[x, 1/x, 1/(x-1)]^\times \xrightarrow{\text{Kummer}} H^1_{\text{ét}}(\boldsymbol{P}^1 \setminus \{0, 1, \infty\}, \mu_n) \to \mathbf{Z}/n \oplus \mathbf{Z}/n$$

becomes $f \mapsto (\operatorname{ord}_0 f, \operatorname{ord}_1 f) \bmod n$ then it is clear that this isomorphism is the identity. The set $S(\mathbf{Z}[A])$ can be identified with the set of characters of A hence with the set of characters of μ_n^2 vanishing on B. Thus

$$S(\mathbf{Z}[A]) = \{(a, b) \in \mathbf{Z}/n \times \mathbf{Z}/n : \sigma^a \tau^b = 1 \ \forall (\sigma, \tau) \in B\}.$$

We can now determine the type of $(C, \mathbf{Z}[A], \mathbf{Z}[A] \to \operatorname{Jac}(C))$.

PROPOSITION 2.5. *Put*

$$S = \{(a, b) \in \mathbf{Z}/n \times \mathbf{Z}/n : a, b \neq 0; a + b \neq n\},$$

$$S^0 = \{(a, b) \in \mathbf{Z}/n \times \mathbf{Z}/n : a, b \neq 0; a + b < n\}$$

and

$$S^1 = \{(a, b) \in \mathbf{Z}/n \times \mathbf{Z}/n : a + b > n\}$$

where $a + b < n$ (respectively $a + b > n$) is to be interpreted as lifting the residues a, b to integers in the interval $[1, n-1]$ and then comparing the sum of those integers, with the integer n.

Then the type of $(C, \mathbf{Z}[A], \mathbf{Z}[A] \to \operatorname{Jac}(C))$ *is* $(S \cap S(\mathbf{Z}[A]), S^0 \cap S(\mathbf{Z}[A]), S^1 \cap S(\mathbf{Z}[A]))$.

PROOF. This is, of course, very well-known and is inserted only for the convenience of the reader. As the de Rham and Hodge cohomology of C is the fixed points of B on the de Rham and Hodge cohomology of the Fermat curve we reduce to the Fermat curve. By Hodge theory it suffices to determine the action on global 1-forms and then we use the basis $\{x^a y^b dx/(y^{n-1}): 0 \leqq a+b \leqq n-3\}$.

If we identify $\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$ with $(\mathbf{Z}/n)^\times$ then the action on S is given by multiplication on both factors. Thus we have reduced the problem of when C modulo p is the product of s.s. elliptic curves to a purely combinatorial problem. Indeed, we need to determine which elements of $(\mathbf{Z}/n)^\times$ stabilize $S^0 \cap S(\mathbf{Z}[A])$. When $(|A|, 6) = 1$ this has been done in [4], the answer is that such an element is almost always the identity in which case it is exactly the p which are congruent to -1 modulo the exponent of A we are looking for.

Let us finish this section with a few examples. As p always is congruent to -1 modulo $p+1$ we see that the Fermat curve of degree $p+1$ has a Jacobian isomorphic to the product of s.s. elliptic curves. As its genus is $\frac{1}{2}(p^2-p)$ we have an example that was promised earlier. I claim that the hyperelliptic curve $Y = \{y^2 = x^p - x\}$ likewise has a Jacobian of the type we are interested in. As $\mu_{2(p-1)}$ acts on it with quotient $\boldsymbol{P}^1$ and ramification at $\{0, 1, \infty\}$ we could apply our results. Another possibility is to note that $\mathbf{Z}/p$ acts on Y with quotient $\boldsymbol{P}^1$. As the genus is $(p-1)/2$ we see that $H^1_{\mathrm{cris}}(Y/W)$ is a module of rank 1 over $W[\mathbf{Z}/p]/(\sum_{g \in \mathbf{Z}/p} g) = R$ and as R is a discrete valuation ring it is a actually a free modulo of rank 1. Hence F and V which commute with R are of the form π^a-isomorphism repectively π^b-isomorphism where $\pi = [1]-1$, a generator of the maximal ideal of R. It is clear that then all the slopes of F on $H^1_{\mathrm{cris}}(Y/W)$ are $a/(p-1)$ and as $H^1_{\mathrm{cris}}(Y/W)$ is isogenous to its dual we get $a/(p-1) = \frac{1}{2}$. As $FV = p$ we get $a+b = p-1$ so $a = b$ and

$$F \cdot H^1_{\mathrm{cris}}(Y/W) = V \cdot H^1_{\mathrm{cris}}(Y/W)$$

so F is 0 on

$$H^1(Y, 0_Y) = H^1_{\mathrm{cris}}(Y/W)/V \cdot H^1_{\mathrm{cris}}(Y/W).$$

As the genus of Y is $(p-1)/2$ we have produced another of the promised examples.

As we know for which p there are curves of genus $\leqq 3$ whose Jacobian is the product of supersingular elliptic curves we can ask ourselves for which p abelian covers of $\boldsymbol{P}^1$ give us curves of genus 4 or 5 whose Jacobian again has this property. Let $\varphi: C \to \boldsymbol{P}^1$ be such a covering. We choose generators for the monodromy at 0,1 and ∞, α, β respectively γ such that $\alpha+\beta+\gamma = 0$. Let a, b and c be their orders. By changing coordinates for $\boldsymbol{P}^1$ we may assume

that $a \leqq b \leqq c$. As $\alpha+\beta+\gamma = 0$ we have $(b,c)\cdot a | bc$, $(a,c)\cdot b | ac$ and $(a,b)c | ab$. Put $r = (a,b,c)$, $rd = (a,b)$, $re = (a,c)$, $rf = (b,c)$. Then $a = rde$, $b = rdf$ and $c = ref$ and also $(d,e) = (d,f) = (e,f) = 1$. The condition $a \leqq b \leqq c$ also gives $d \leqq e \leqq f$. Let finally s be the index of the cyclic group generated by γ in the structure group A of φ. As (α,γ) and (β,γ) generate A we get $s|a$ and $s|b$ thus $s|rd$. Hurwitz' formula now gives $2g-2 = s(ref-(f/d+1+e/d))$ where $g = 4$ or 5.

It is straightforward and tedious to list all possibilities and I only give the result. I list (a,b,c,s):

$g = 4$: $(3, 5, 15, 1)$; $(2, 9, 18, 1)$; $(4, 6, 12, 1)$; $(3, 6, 6, 3)$;
$(5, 10, 10, 1)$; $(3, 12, 12, 1)$; $(2, 16, 16, 1)$; $(6, 6, 6, 2)$;
$(2, 10, 10, 2)$; $(9, 9, 9, 1)$.

$g = 5$: $(2, 11, 22, 1)$; $(11, 11, 11, 1)$;
$(6, 12, 12, 1)$; $(3, 15, 15, 1)$; $(2, 20, 20, 1)$;
$(4, 8, 8, 2)$; $(2, 12, 12, 2)$.

By direct inspection one shows that all tuples are actually realizable and that we get $F = 0$ on $H^1(C, \mathcal{O}_C)$ exactly when $p \equiv -1$ modulo the exponent of the structure group except in the cases $(3, 12, 12, 1)$, $(2, 16, 16, 1)$ and $(3, 15, 15, 15, 1)$ where we could also have $p \equiv -7 \bmod 12$, $-7 \bmod 16$ respectively $-4 \bmod 15$. Thus there exists an abelian cover of degree prime to p of $\boldsymbol{P}^1$ ramified at 3 points whose Jacobian is the product of s.s. elliptic curves of genus 3 exactly when

$$p \equiv -1 \bmod 15, 6, 10, 16, 9 \quad \text{or} \quad p \equiv -7 \bmod 16$$

and of genus 5 exactly when

$$p \equiv -1 \bmod 11, 12, 15, 20, 8 \quad \text{or} \quad p \equiv -4 \bmod 15.$$

PROBLEM. Does there exist a curve of genus 4 or 5 whose Jacobian is the product of s.s. elliptic curves for any $p \neq 2, 3$?

3. Pencils of s.s. curves of genus 2.

1. Let $X \to C$ be a semi-stable fibration of genus 2 curves with supersingular generic fiber. Recall [5], [6]) that given a polarization $\varphi: E^2 \to E^2$, E a s.s. elliptic curve, such that $\ker \varphi = \operatorname{Ker} F$ then Moret-Bailly constructs such a fibration $X_\varphi \to \boldsymbol{P}^1$. Our aim is to show that in a very precise sense these are the only possible fibrations of the above type. We will work over an algebraically closed field k (of characteristic $p > 0$).

THEOREM 1.1. *Let $X \to C$ be a stable non-isotrivial fibration, generically*

smooth, of genus 2 *curves with* C *a normal irreducible variety such that the generic fiber is supersingular. Then there exists an étale cover* $\tilde{C} \to C$ *of* C, *a polarization* $\varphi\colon E^2 \to E^2$ *with* $\ker\varphi = \ker F$, *a morphism* $\tilde{C} \to \mathbf{P}^1$ *and an isomorphism of fibrations of the pullback of* X *and* X_φ *to* $\tilde{C}$. *If there exists two such tuples* $(X \to C, \tilde{C} \to \mathbf{P}^1, \varphi)$ *and* $(X \to C, \tilde{C}' \to \mathbf{P}^1, \varphi')$ *then there is an automorphism of* E^2 *taking* φ *to* φ'.

PROOF. The first step is to construct $\tilde{C}$ such that the pullback $\tilde{X} \to \tilde{C}$ has the property that its Jacobian admits an isogeny of degree p from $E^2 \times \tilde{C}$. For this we will need the following lemma (cf. [12]).

LEMMA 1.1.1. *Let* Y *be a normal irreducible noehterian scheme and* A *and* B *two abelian schemes over* Y. *Suppose given a geometric point* $\bar{s} \to Y$ *whose image is the generic point and a homomorphism* $A_{\bar{s}} \to B_{\bar{s}}$.

Then there exists an étale cover $\tilde{Y} \to Y$, *a lifting* $\bar{s} \to \tilde{Y}$ *of* $\bar{s} \to Y$ *and a homomorphism* $A_{\tilde{Y}} \to B_{\tilde{Y}}$ *extending the given* $A_{\bar{s}} \to B_{\bar{s}}$.

PROOF. Indeed, we may consider the universal family of homomorphism from $A \to B$:

$$\begin{array}{ccc} A \times_Y Y' & \longrightarrow & B \times_Y Y' \\ & \searrow & \downarrow \\ & & Y' \longrightarrow Y \end{array}$$

One knows that Y' is a separated algebraic space locally of finite type over Y. The rigidity lemma (cf. [7: Corollary 6.2]) shows that φ is formally unramified and hence unramified. By hypothesis $\bar{s} \to Y$ lifts to $\bar{s} \to Y'$. Let Y be the closure of the image of $\bar{s}$. If we can show that $\tilde{Y} \to Y$ is an étale cover we are through. As we have seen it is unramified and as it is dominant, $\tilde{Y}$ is irreducible and as Y is normal it is étale. This shows that $\tilde{Y}$ is an open subscheme of the normalization of Y in the function field of $\tilde{Y}$ so it is of finite type and what is left is to show that $\tilde{Y} \to Y$ is proper. It is of finite type so we can check by the valuative criterion. Thus we reduce to the case when Y is the spectrum of discrete valuation ring and $\tilde{Y} \to Y$ is open and $\tilde{Y} \neq \emptyset$, but then by the properties of Néron models $\tilde{Y} = Y$.

To get our $\tilde{C}$ we need therefore only check two things. Namely that an isogeny $E^2 \times \bar{s} \to \mathrm{Jac}(X_{\bar{s}})$ of degree p exists for $\bar{s}$ some generic geometric point and that $\mathrm{Jac}(X/C)$ is an abelian scheme. The first part follows from [11, Corollary 7] and the second from [12, Proof of Theorem 1.1a].

Let us now consider our isogeny $\varphi\colon E^2 \times \tilde{C} \to \mathrm{Jac}(\tilde{X}/\tilde{C})$ where $\tilde{X} := X \times_C \tilde{C}$

and C is connected. The kernel of φ is of order p and fiber by fiber isomorphic to α_p as this is the only subgroup scheme of E^2 of order p. In particular it is of height 1 and thus completely determined by the position of its Lie algebra $\mathscr{L}$ inside of the Lie algebra of E^2 which is $\mathscr{O}_{\tilde{C}} \oplus \mathscr{O}_{\tilde{C}}$. As $\mathscr{L}$ is locally a direct factor of $\mathscr{O}_{\tilde{C}} \oplus \mathscr{O}_{\tilde{C}}$ there is a morphism $\psi: \tilde{C} \to \boldsymbol{P}^1$ such that $\mathscr{L} \subseteqq \mathscr{O}_{\tilde{C}} \oplus \mathscr{O}_{\tilde{C}}$ is the inverse image of $\mathscr{O}_{\boldsymbol{P}^1}(-1) \subseteqq \mathscr{O}_{\boldsymbol{P}^1}^2$. Let $\mathscr{M} \subseteqq E^2 \times \boldsymbol{P}^1$ be the height 1 subgroup scheme whose Lie algebra is $\mathscr{O}(-1)$ and let $\varrho: E^2 \times \boldsymbol{P}^1 \to \mathscr{J}$ be the isogeny obtained by taking the quotient by $\mathscr{M}$. Then clearly φ is isomorphic to the inverse image of ϱ and in particular $\mathrm{Jac}(\tilde{X}/\tilde{C})$ descends to $\boldsymbol{P}^1$. I claim that so does the fibration $\tilde{X} \to \tilde{C}$. Let us first show that $\mathrm{Jac}(\tilde{X}/\tilde{C})$ together with its polarization descends. The morphism ψ is not constant because if it were, then $\mathrm{Jac}(\tilde{X}/\tilde{C})$ would be a constant abelian scheme and $\tilde{X} \to \tilde{C}$ would be isotrivial by the Torelli theorem. Hence ψ is dominant and we may choose a geometric point of $\tilde{C}$ whose image in $\boldsymbol{P}^1$ is the generic point. By Lemma 1.1.1 there is an étale cover of $\boldsymbol{P}^1$ such that over this cover is a homomorphism $\mathscr{J} \to \mathscr{J}^*$ where $\mathscr{J}^*$ is the dual of $\mathscr{J}$, inducing on $\bar{s}$ the pullback of the polarization on $\mathrm{Jac}(\tilde{X}/\tilde{C})$. As $\boldsymbol{P}^1$ is simply connected $\mathscr{J} \to \mathscr{J}^*$ exists already on $\boldsymbol{P}^1$. The polarization on $\mathrm{Jac}(\tilde{X}/\tilde{C})$ and the pullback of $\mathscr{J} \to \mathscr{J}^*$ to $\tilde{C}$ give two homomorphisms $\mathrm{Jac}(\tilde{X}/\tilde{C}) \to \mathrm{Jac}(\tilde{X}/\tilde{C})^*$ whose pullback to $\bar{s}$ are the same so by rigidity they are equal.

To descend $\tilde{X} \to \tilde{C}$ we obssbserve that as $\psi: \tilde{C} \to \boldsymbol{P}^1$ is dominant and $\tilde{C}$ integral ψ is flat and hence $\psi': \tilde{C} \to \mathrm{Im}\,\psi(\tilde{C})$ is faithfully flat. Thus to descend $\tilde{X} \to \tilde{C}$ to $\mathrm{Im}\,\psi(\tilde{C})$ it suffices to give descent data for $\tilde{X} \to \tilde{C}$ with respect to $\tilde{C} \to \mathrm{Im}\,\psi(\tilde{C})$. In fact it suffices to show that $\tilde{X} \to \tilde{C}$ descends over $U \to \psi^{-1}(U)$ for some open subset U of $\mathrm{Im}\,\psi(\tilde{C})$ and that the descended fibration extends to the whole of $\boldsymbol{P}^1$ for then we would have two stable fibrations over $\tilde{C}$ isomorphic on an open subset and hence they would be isomorphic. (Use the fact that the scheme of isomorphisms would be unramified and proper (cf. [2, Theorem 1.11]).) By making U small enough we may assume that

$$\tilde{X}_{\psi^{-1}(U)} \to \varphi^{-1}(U)$$

is smooth and then the automorphism scheme for

$$\tilde{X}_{\psi^{-1}(U)} \to \psi^{-1}(U)$$

is equal to the automorphism scheme for its polarized Jacobian which already is descended.

We have therefore arrived at the point where we may assume that $C = \boldsymbol{P}^1$ and that there exists an isogeny $\varphi: E^2 \times \boldsymbol{P}^1 \to \mathrm{Jac}(X/\boldsymbol{P}^1)$ of degree p such that $\mathrm{Ker}\,\mathrm{Lie}(\varphi) = \mathscr{O}_{\boldsymbol{P}^1}(-1)$.

Pulling back the Jacobian polarization by φ gives us a polarization of degree p on $E^2 \times \boldsymbol{P}^1$ which necessarily is constant i.e. is of the form a polarization

ψ on E^2 times $\boldsymbol{P}^1$. The kernel of ψ contains $\ker \varphi_S$ for every point of $\boldsymbol{P}^1$ and as these fill up all of $\ker F$ we see that $\ker R \subseteq \ker \psi$ and as they have the same order they are equal. We hence get a Moret-Bailly family $X_\psi \to \boldsymbol{P}^1$. By construction there is an isogeny

$$\varphi' : E^2 \times \boldsymbol{P}^1 \to \mathrm{Jac}(X_\psi/\boldsymbol{P}^1)$$

and an isomorphism

$$\varrho : \mathrm{Jac}(X_\psi/\boldsymbol{P}^1) \to \mathrm{Jac}(X/\boldsymbol{P}^1)$$

such that $\varrho \circ \varphi' = \varphi$. Again by construction the pullback by φ of the polarization α of $X \to \boldsymbol{P}^1$ equals the pullback by φ' of the polarization β of $X_\psi \to \boldsymbol{P}^1$. Hence $\varphi'^*(\varrho^*(2)) = \varphi'^*(\beta)$ and as φ'^* is injective $\varrho^*(\alpha) = \beta$. This implies that at least over an open subset of $\boldsymbol{P}'$ the two families are isomorphic and then they are isomorphic being stable.

For the unicity we may assume that there is some dominating $\tilde{C}'' \to \boldsymbol{P}^1$ such that the pullback of two polarizations φ, φ' on E^2 are isomorphic. By Lemma 1.1.1 they are isomorphic over some étale cover of $\boldsymbol{P}^1$ and hence isomorphic.

2. We will now apply Theorem 1.1 to the study of semi-stable fibrations over $\boldsymbol{P}^1$ whose Jacobian has everywhere good reduction.

PROPOSITION 2.1. *Let $\pi : X \to \boldsymbol{P}^1$, X smooth, be a semi-stable non-isotrivial fibration by curves of genus at least 2 whose Jacobian fibration has everywhere good reduction. Then X is of general type unless the characteristic is two and the fibers have genus two and X is birationally equivalent to a product of two supersingular elliptic curves.*

PROOF. $R^1\pi_*\mathbf{Z}_l$ is by assumption a lisse sheaf. As $\boldsymbol{P}^1$ is simply-connected it is constant. Leray's spectral sequence then shows that

$$H^1(X, \mathbf{Z}_l) = H^0(\boldsymbol{P}^1, R^1\pi_*\mathbf{Z}_l) = H^1(X_{\bar{S}}, \mathbf{Z}_l)$$

for any fibre $X_{\bar{s}}$. Therefore the morphism $A \times \boldsymbol{P}^1 \to \mathrm{Pic}^0(X/\boldsymbol{P}^1)$, where

$$A := \mathrm{Pic}^\tau(X)_{\mathrm{red}},$$

is an isogeny and in particular if g is the genus of a fibre $g = q := \dim A$. Let us dispose of the case $g = 2$. As $X \to \boldsymbol{P}^1$ is non-isotrivial $\mathrm{Pic}^0(X/\boldsymbol{P}^1)$ is non-constant so A is an abelian surface that has a connected non-trivial family of finite subgroupschemes. If A is not supersingular there is in fact only a finite number of subgroup schemes of fixed order. Any such group scheme can be written uniquely as a sum of a p-group and p'-group where $p = \mathrm{chark}$. The statement is obvious for the p'-part so we may confine our-

selves to the p-part. Similarly, the étale and multiplicative parts are clear so we need only look at the biconnected part. If A is not supersingular this part of the p-divisible group of A is either zero (a trivial case) or isomorphic to the p-divisible group of a s.s. elliptic curve but there, for every n there is exactly one subgroup scheme of order p^n, the kernel of the Frobenius (there is a unique subgroup of order p hence it is contained in every non-trivial subgroup, dividing by it we conclude by induction).

We thus see that A is supersingular and by Theorem 1.1, $X \to \boldsymbol{P}^1$ is the pullback by a morphism $\pi: \boldsymbol{P}^1 \to \boldsymbol{P}^1$ of a Moret-Bailly family $X' \to \boldsymbol{P}^1$. If $p \neq 2$ Moret-Bailly [6] shows that $\omega_{X'}$ is ample. If $\deg \pi = r$ then $\omega_X = t^* \omega_{X'}(2r-2)$ where $t: X \to X'$ is the given map. Hence ω_X is still numerically positive and X is also of general type. As for characteristic 2 a Moret-Bailly family has X birational to the product of s.s. elliptic curves. What is left to be shown is that the pullback by a morphism $\boldsymbol{P}^1 \to \boldsymbol{P}^1$ of degree r greater than 1 is of general type. Moret-Bailly shows that $f: X' \to \boldsymbol{P}^1$ has 5 singular fibres each of which consists of two crossing elliptic curves hence the number of singular points for f is 5. He also shows that the degree of $f_* \omega_{X'/\boldsymbol{P}^2}$ is 1 and as X' is an abelian surface blown up at one point $C_1^2 = -1$. By [15],

$$C_1^2(X) = ([2\cdot]-5)(r-1)-1 = 7(r-1)-1$$

hence positive if $r > 1$. As X admits a generically finite map to an abelian variety X is not ruled so it is of general type.

We can now finish the argument. Now $q > 2$ so X is neither birational to a K3-surface nor to an abelian surface. By the classification of surfaces there is some fibration $\tilde{X} \to C$ with fibers of arithmetic genus $\leqq 1$ (rules, elliptic or quasi-elliptic) and a birational mapping $X \dashrightarrow \tilde{X}$. We see that $g(C) \geqq q(\tilde{X}) - 1 = q-1$. Let $T \subseteqq X$ be some fiber of $X \to \boldsymbol{P}^1$ such that $T \to \tilde{X}$ is defined. As $g(T) \geqq 2$ the morphism $T \to C$ is non-constant and we can factor it as $T \to C' \to C$ where $C' = C^{(p^n)}$ for some n so $C' \to C$ is purely inseparable and $T \to C'$ is separable. Hurwitz' formula gives

$$2q-2 = n(2g(c)-2)+\sum(e_i-1)$$

where n is the degree of $T \to C'$. The inequality $g(C) \geqq q-1$ gives $0 \geqq (n-1)(2g-2)-2+\sum(e_i-1)$ and as $q \geqq 3$ this is impossible unless $n = 1$ or $n = 2$ and $T \to C'$ is étale. Hence we get only a countable number of possibilities for T which forces $X \to \boldsymbol{P}^1$ to be isotrivial.

BIBLIOGRAPHY

1. P. Deligne and J. S. Milne, *Tannakian categories*, in *Hodge Cycles, Motives, and Shimura Varieties* (Lecture Notes in Math. 900), eds. P. De Ligne, J. S. Milne, A. Ogus, K.-Y. Shih, pp. 101–228. Springer-Verlag, Berlin - Heidelberg - New York, 1982.
2. P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. 36 (1969), 75–109.
3. K. Hashimoto and T. Ibukiyama, *On class numbers of positive definite quaternion hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 27 (1980), 549–560.
4. N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. 31 (1978), 1183–1205.
5. L. Moret-Bailly, *Polarisations de degré 4 sur les surfaces abéliennes*, CR. Acad. Sci. Paris Sér. I Math. 289 (1979), 787–790.
6. L. Moret-Bailly, *Familles de courbes et de variétés abéliennes sur* $\boldsymbol{P}^1$. I. *Sur des polarisations*, in *Séminaire sur les pinceaux de courbes de genre au moins deux*, pp. 109–124. Astérisque, 86. Soc. Math. France, Paris, 1981.
7. D. Mumford, *Geometric Invariant Theory*, (Ergeb. Math. Grenzgeb. 34), Springer-Verlag, Berlin - Heidelberg - New York, 1965.
8. D. Mumford, *Abelian Varieties* (Tata Inst. Fund. Res. Studies in Math. 5). Oxford Univ. Press, New York, London, 1970.
9. T. Oda and F. Oort, *Supersingular abelian varieties*, (Proc., Kyoto Univ., Kyoto, 1977), pp. 595–621. Kinokuniya Book Store, Tokyo, 1978.
10. A. Ogus, *Supersingular* K3*-crystals*, in *Journées de géometric algébrique de Rennes*, (Rennes, 1978), Vol. II, pp. 3–86, Astérisque, 64. Soc. Math. France, Paris, 1979.
11. F. Oort, *Which abelian surfaces are products of elliptic curves?* Math. Ann. 214 (1975), 35–47.
12. F. Oort, *Subvarieties of moduli spaces*, Invent. Math. 24 (1974) 95–119.
13. J.-P. Serre, *A course in Arithmetic*, (Graduate Texts in Math. 7), Springer-Verlag, Berlin - Heidelberg - New York, 1973.
14. J.-P. Serre, Course at Collège de France, 1983–84.

MATEMATISKA INSTITUTIONEN
STOCKHOLM UNIVERSITET
BOX 6701
11385 STOCKHOLM
SWEDEN