Advanced Studies in Pure Mathematics 10, 1987
Algebraic Geometry, Sendai, 1985
pp. 253–281

Supersingular Abelian Varieties of Dimension Two or Three and Class Numbers

Toshiyuki Katsura and Frans Oort

§ 0. Introduction

Let B be a definite quaternion algebra over the field $\boldsymbol{Q}$ of rational numbers with discriminant p. We assume that p is a prime number. Let U_g be the positive definite quaternion hermitian space of dimension g over B. We denote by H_g the class number of the principal genus of U_g (for the definition of the principal genus, see Hashimoto and Ibukiyama [6, Section 1]). Let k be an algebraically closed field of characteristic p. In Ibukiyama, Katsura and Oort [7, Theorem 2.10], we showed that the class number H_g $(g \geq 2)$ is equal to the number of isomorphism classes of principally polarized abelian varieties (X, Θ) of dimension g defined over k such that X is isomorphic to a product of supersingular elliptic curves (see also Shioda [23, Theorem 3.5] and Serre [22]).

When $g=1$, H_1 is nothing but the class number of the maximal orders of B. The explicit formula for H_1 was given by Eichler [3, Satz 2]. Then, Deuring proved that the class number H_1 is equal to the number of isomorphism classes of supersingular elliptic curves defined over k (Deuring [2], p. 266). Finally, Igusa calculated the number of isomorphism classes of supersingular elliptic curves defined over k by an algebraic method, and using Deuring's result, he gave a new proof of the explicit formula for H_1 (cf. Igusa [8]). In the first part of this paper, we calculate, by an algebraic method similar to the one in Igusa [8], the number of isomorphism classes of principally polarized abelian surfaces defined over k such that X is isomorphic to a product of supersingular elliptic curves. Hence, using the above result, we give a new proof of the explicit formula for H_2 which was given in Hashimoto and Ibukiyama [6].

Recall that an abelian variety is called supersingular if it is isogenous to a product of supersingular elliptic curves. Let $\mathscr{A}_{g,1}$ be the coarse moduli scheme of principally polarized abelian varieties of dimension g defined over k, and let V be the algebraic set in $\mathscr{A}_{g,1}$ whose points correspond to supersingular abelian varieties. We call V the supersingular locus

Received September 27, 1985.

of $\mathscr{A}_{g,1}$. In the case of dimension two, as was shown in Katsura and Oort [10], the number of irreducible components of V is equal to the class number of the non-principal genus of U_g (for the definition of the non-principal genus, see Hashimoto and Ibukiyama [6, (II)]). In the second part of this paper, we show that the number of irreducible components of the supersingular locus V in $\mathscr{A}_{3,1}$ is equal to H_3. Hence, using the explicit formula for H_3 by Hashimoto [5], we conclude that this locus V is reducible if and only if $p \geq 3$. We show also that the a-number of the generic member of every irreducible component of V is equal to one (cf. Theorem 6.5).

The authors would like to thank Professors K. Ueno, T. Ibukiyama and K. Hashimoto for useful conversations. The authors would also like to thank Professor Tadao Oda for his valuable advice and encouragement. The second author visited Japan during the fall of 1984, and most of his work for this paper was done at that time. The second author thanks his Japanese colleagues and friends for warm hospitality, and is grateful to the Japan Society for the Promotion of Science (JSPS) for financial support, and to Kyoto University for excellent working conditions.

§ 1. Curves of genus two

In this section, we recall basic facts and some results of our previous paper [7]. It should be noticed that all these facts were obtained by an algebraic method similar to the one in Igusa [8].

Let p be a prime number, and let B be a definite quaternion algebra over the field $\boldsymbol{Q}$ of rational numbers with discriminant p. We denote by $H_g = H_g(p, 1)$ the class number of the principal genus of the positive definite quaternion hermitian space of dimension g over B (for the definition, see Hashimoto and Ibukiyama [6, Section 1]). We use the following theorems.

Theorem 1.1 (Ibukiyama, Katsura and Oort [7]). *Let k be an algebraically closed field of characteristic p, and let E be a supersingular elliptic curve defined over k. Then, H_g is equal to the number of principal polarizations on E^g up to automorphisms of E^g.*

Theorem 1.2 (Deligne). *Let E_i $(i=1, 2, \cdots, 2g)$ be supersingular elliptic curves. Assume $g \geqq 2$. Then, $E_1 \times \cdots \times E_g$ is isomorphic to $E_{g+1} \times \cdots \times E_{2g}$.*

For the proof, see Shioda [23, Theorem 3.5].

Using these two theorems, we see that H_g is equal to the number of isomorphism classes of principally polarized abelian varieties (X, Θ) of

dimension g such that X is isomorphic to a product of supersingular elliptic curves.

Now, we assume $g=2$. Then, we can consider a principal polarization Θ as a complete (not necessarily irreducible) curve of genus two on X. According to Weil [24, Satz 2], we have the following two possibilities for Θ:

a) Θ is a non-singular complete curve of genus two and X is isomorphic to the Jacobian variety of Θ.

b) $\Theta=E_1+E_2$ consists of two elliptic curves E_1, E_2 which intersect transversally such that $X\simeq E_1\times E_2$.

It is easy to see that H_1 coincides with the number h of isomorphism classes of supersingular elliptic curves. Moreover, Igusa [8] showed that

$$h=\left\{1-\left(\frac{-3}{p}\right)\right\}\Big/3+\left\{1-\left(\frac{-4}{p}\right)\right\}\Big/4+(p-1)/12, \tag{1.1}$$

where $\left(\frac{l}{p}\right)$ denotes the Legendre symbol. Then, the number n of isomorphism classes of principally polarized supersingular abelian surfaces (X, Θ) which belong to Case b) is given by

$$n=h(h+1)/2 \tag{1.2}$$

(for details, see Ibukiyama, Katsura and Oort [7, Section 2.2]). A non-singular complete curve C of genus two has the canonical involution ι. We denote by $\mathrm{Aut}(C)$ the group of automorphisms of C. We call $\mathrm{RA}(C)=\mathrm{Aut}(C)/\langle\iota\rangle$ the reduced group of automorphisms of C. We say that a curve C of genus two is in Class (0) if the reduced group $\mathrm{RA}(C)$ of automorphisms is trivial. For $p\geqq 7$, we said that a curve C of genus two is in Class (i) ($i=0, 1, \cdots, 6$) if $\mathrm{RA}(C)$ contains the group in (i) (cf. Igusa [9], and Ibukiyama, Katsura and Oort [7]):

(1.3) (0) $\{0\}$, (1) $\boldsymbol{Z}/2\boldsymbol{Z}$, (2) S_3, (3) $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$, (4) D_{12}, (5) S_4, (6) $\boldsymbol{Z}/5\boldsymbol{Z}$.

In this paper, we say that a curve C of genus two is of type (i) ($i=0, 1, \cdots, 6$) if $\mathrm{RA}(C)$ is isomorphic to the group in (i). We denote by n_i ($i=0, 1, \cdots, 6$) the number of isomorphism classes of curves C of genus two of type (i) whose Jacobian variety $J(C)$ is isomorphic to a product of two supersingular elliptic curves. Then, for $p\geqq 7$, we already proved the following results (cf. Ibukiyama, Katsura and Oort [7]):

$$n_2=(p-1)/6-\left\{1-\left(\frac{-2}{p}\right)\right\}\Big/2-\left\{1-\left(\frac{-3}{p}\right)\right\}\Big/3, \tag{1.4}$$

$$n_3=(p-1)/8-\left\{1-\left(\frac{-1}{p}\right)\right\}/8-\left\{1-\left(\frac{-2}{p}\right)\right\}/4$$
$$-\left\{1-\left(\frac{-3}{p}\right)\right\}/2,$$
$$n_4=\left\{1-\left(\frac{-3}{p}\right)\right\}/2,$$
$$n_5=\left\{1-\left(\frac{-2}{p}\right)\right\}/2,$$
$$n_6=\begin{cases}0 & \text{if } p\equiv 1, 2 \text{ or } 3 \pmod 5,\\ 1 & \text{if } p\equiv 4 \pmod 5.\end{cases}$$

§ 2. Curves of genus two in Class (1)

In this section, we assume char. $k=p\geqq 7$. We use the notations in Ibukiyama, Katsura and Oort [7, Section 1]. Now, we consider the curves of genus two of type (1), (2) ,(3), (4) or (5). Since the reduced groups of automorphisms of these curves contain an element of order two, they are defined by the following equation:

$$C_{a,b}: y^2=(x^2-1)(x^2-a)(x^2-b) \tag{2.1}$$

with $a, b \in k$; $a\neq 0, 1$; $b\neq 0, 1$; $a\neq b$.

Lemma 2.1. *Let x be a local coordinate of A^1 in the projective line P^1. Let θ be the automorphism of order two of P^1 defined by*

$$\theta: x\longmapsto -x. \tag{2.2}$$

Then, the automorphisms of order two of P^1 which commute with θ are of the following form:

$$\eta_a(x)=\alpha/x \quad \text{with} \quad \alpha\in k^*, \quad \text{or} \quad \theta(x)=-x, \tag{2.3}$$

where k^* is the multiplicative group of non-zero elements of k.

Proof. Since the automorphisms of P^1 are of the form $(\alpha x+\beta)/(\gamma x+\delta)$ with $\alpha, \beta, \gamma, \delta \in k$, we can check this lemma by direct computation. q.e.d.

Lemma 2.2. *The reduced group $\mathrm{RA}(C_{a,b})$ of automorphisms of $C_{a,b}$ contains a subgroup which is isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$ if and only if $a=b^2$, $a^2=b$ or $ab=1$.*

Proof. The "if" part is trivial. Suppose that $\mathrm{RA}(C_{a,b})$ contains a subgroup which is isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$. Then, by (1.3), we see that $\mathrm{RA}(C_{a,b})$ is isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$, D_{12} or S_4. The automorphism θ defined by (2.2) gives an element of order two of $\mathrm{RA}(C_{a,b})$. By the structure of groups $\boldsymbol{Z}/2\boldsymbol{Z}\times\boldsymbol{Z}/2\boldsymbol{Z}$, D_{12} and S_4, we can find an element $\eta(\eta\neq\theta)$ of $\mathrm{RA}(C_{a,b})$ of order two which commutes with θ. By Lemma 2.1, η is of the following form:

$$\eta(x)=\alpha/x \quad \text{with} \quad \alpha\in k^*.$$

We see that η induces a permutation of the six branch points 1, -1, $\sqrt{a}$, $-\sqrt{a}$, $\sqrt{b}$ and $-\sqrt{b}$ of $C_{a,b}$ over $\boldsymbol{P}^1$. Since $\eta(1)=\alpha$, we conclude that $\alpha=\pm1$, $\pm\sqrt{a}$ or $\pm\sqrt{b}$. If $\alpha=\pm1$, then we have $\eta(\sqrt{a})=\pm(1/\sqrt{a})=\pm\sqrt{b}$ by $a\neq1$ and $a\neq b$. Hence, we have $ab=1$. If $\alpha=\pm\sqrt{a}$, then we have $\eta(\pm\sqrt{b})=(\pm\sqrt{a})/(\pm\sqrt{b})=\pm\sqrt{b}$. Hence, we have $a=b^2$. If $\alpha=\pm\sqrt{b}$, then by the same method, we have $a^2=b$. q.e.d.

By Lemma 2.2, we see that the curves of type (1) or (2) can be defined by (2.1) with $ab\neq1$, $a\neq b^2$ and $a^2\neq b$.

Lemma 2.3. *Assume $ab\neq1$, $a\neq b^2$ and $a^2\neq b$. Then, the curve $C_{a',b'}$ is isomorphic to $C_{a,b}$ if and only if (a', b') is equal to one of the following*:

$$(a, b),\ (1/a, 1/b),\ (a, a/b),\ (1/a, b/a),\ (b, a),\ (1/b, 1/a),$$
$$(b, b/a),\ (1/b, a/b),\ (a/b, a),\ (b/a, 1/a),\ (a/b, 1/b),\ (b/a, b).$$

Moreover, these twelve pairs are different from each other.

Proof. The "if" part is trivial. Suppose that we have an isomorphism

$$\tilde{\psi}\colon C_{a,b}\longrightarrow C_{a',b'}.$$

The curve $C_{a,b}$ (resp. $C_{a',b'}$) is a two-sheeted covering of $\boldsymbol{P}^1$, and $\tilde{\psi}$ induces an automorphism ψ of $\boldsymbol{P}^1$, which also induces a bijection from six branch points $\{1, -1, \sqrt{a}, -\sqrt{a}, \sqrt{b}, -\sqrt{b}\}$ to $\{1, -1, \sqrt{a'}, -\sqrt{a'}, \sqrt{b'}, -\sqrt{b'}\}$. By the assumptions $ab\neq1$, $a\neq b^2$, $a^2\neq b$, both curves $C_{a,b}$, $C_{a',b'}$ are of type (1) or (2). If the curve $C_{a',b'}$ is of type (1), then the element of order two in the reduced group of automorphisms is unique, and is given by (2.2). Therefore, we have $\psi\circ\theta\circ\psi^{-1}=\theta$. If the curve $C_{a',b'}$ is of type (2), then the elements of order two in the reduced group of automorphisms are conjugate to each other. Therefore, by a suitable choice of $\tilde{\psi}$, we can assume $\psi\circ\theta\circ\psi^{-1}=\theta$. Hence, in any case, we may assume

$$\psi \circ \theta \circ \psi^{-1} = \theta. \tag{2.4}$$

Thus, we see that ψ is a bijection from three pairs $\{\{1, -1\}, \{\sqrt{a}, -\sqrt{a}\}, \{\sqrt{b}, -\sqrt{b}\}\}$ to three pairs $\{\{1, -1\}, \{\sqrt{a'}, -\sqrt{a'}\}, \{\sqrt{b'}, -\sqrt{b'}\}\}$.

First, assume $\psi(\{1, -1\}) = \{1, -1\}$. Composing ψ with θ, if necessary, we may assume $\psi(1) = 1$ and $\psi(-1) = -1$. Then, the automorphism ψ of $\boldsymbol{P}^1$ is of the following form:

$$\psi(x) = \{(1+\varepsilon)x + (1-\varepsilon)\} / \{(1-\varepsilon)x + (1+\varepsilon)\}$$

with a suitable element ε of k^*. Since we have $\psi(\sqrt{a}) + \psi(-\sqrt{a}) = 0$ and $a \neq 1$, we have $\varepsilon = \pm 1$, that is,

$$\psi(x) = x \quad \text{or} \quad 1/x.$$

Hence, we have

$$\begin{cases} a' = a \\ b' = b, \end{cases} \quad \begin{cases} a' = b \\ b' = a, \end{cases} \quad \begin{cases} a' = 1/a \\ b' = 1/b \end{cases} \quad \text{or} \quad \begin{cases} a' = 1/b \\ b' = 1/a. \end{cases}$$

Secondly, assume $\psi(\{1, -1\}) = \{\sqrt{a'}, -\sqrt{a'}\}$. Composing ψ with θ, if necessary, we may assume $\psi(1) = \sqrt{a'}$ and $\psi(-1) = -\sqrt{a'}$. We consider the automorphism ψ' of $\boldsymbol{P}^1$ defined by

$$\psi' : x \longmapsto x/\sqrt{a'}.$$

Then, using this ψ', we see that the curve $C_{a',b'}$ is transformed into $C_{1/a',b'/a'}$, and we have a morphism $\psi' \circ \psi$ with $\psi' \circ \psi(1) = 1$ and $\psi' \circ \psi(-1) = -1$. Hence, by the same argument as above, we have

$$\begin{cases} a' = 1/a \\ b' = b/a, \end{cases} \quad \begin{cases} a' = 1/b \\ b' = a/b, \end{cases} \quad \begin{cases} a' = a \\ b' = a/b \end{cases} \quad \text{or} \quad \begin{cases} a' = b \\ b' = b/a. \end{cases}$$

Finally, assume $\psi(\{1, -1\}) = \{\sqrt{b'}, -\sqrt{b'}\}$. Then, by the same method as above, we have

$$\begin{cases} a' = a/b \\ b' = 1/b, \end{cases} \quad \begin{cases} a' = b/a \\ b' = b, \end{cases} \quad \begin{cases} a' = b/a \\ b' = 1/a \end{cases} \quad \text{or} \quad \begin{cases} a' = a/b \\ b' = a. \end{cases}$$

The last statement of this lemma follows by direct computation from our assumption. q.e.d.

Now, we consider two automorphisms of the curve $C_{a,b}$ defined by

$$\sigma\colon \begin{cases} x \longmapsto -x \\ y \longmapsto y, \end{cases} \qquad \tau\colon \begin{cases} x \longmapsto -x \\ y \longmapsto -y. \end{cases} \tag{2.5}$$

We denote by $\langle\sigma\rangle$ (resp. $\langle\tau\rangle$) the group generated by σ (resp. τ). We set $E_\sigma = C_{a,b}/\langle\sigma\rangle$ and $E_\tau = C_{a,b}/\langle\tau\rangle$, which are elliptic curves (cf. Igusa [9, Section 8]). We know the following lemma (cf. Ibukiyama, Katsura and Oort [7]).

Lemma 2.4. *The Jacobian variety $J(C_{a,b})$ is isomorphic to a product of two supersingular elliptic curves if and only if both E_σ and E_τ are supersingular elliptic curves.*

We set

$$\begin{cases} X = x^2, \\ Y = y. \end{cases}$$

Then, the elliptic curve E_σ is defined by the equation

$$Y^2 = (X-1)(X-a)(X-b).$$

By the coordinate change

$$\begin{cases} u = (X-a)/(1-a), \\ v = Y/(1-a)^{3/2}, \end{cases}$$

E_σ is thus defined by the equation

$$v^2 = u(u-1)\{u-(b-a)/(1-a)\}. \tag{2.6}$$

As for E_τ, set

$$\begin{cases} X = 1/x^2, \\ Y = (i/\sqrt{ab})(y/x^3), \end{cases}$$

where i is a primitive fourth root of unity. Then, the elliptic curve E_τ is defined by the equation

$$Y^2 = (X-1)\{X-(1/a)\}\{X-(1/b)\}.$$

By the coordinate change

$$\begin{cases} u = \{X-(1/a)\}/\{1-(1/a)\}, \\ v = Y/\{1-(1/a)\}^{3/2}, \end{cases}$$

E_τ is thus defined by the equation

$$v^2=v(v-1)\{v-(b-a)/b(1-a)\}. \tag{2.7}$$

For an elliptic curve E_λ defined by the equation

$$E_\lambda: y^2=x(x-1)(x-\lambda), \tag{2.8}$$

we consider the Legendre polynomial

$$\Phi(\lambda)=\sum_{i=0}^{(p-1)/2}\binom{(p-1)/2}{i}^2\lambda^i.$$

Then, we know that E_λ is a supersingular elliptic curve if and only if $\Phi(\lambda)=0$ (for instance, see Mumford [14, p. 216]). We consider two sets

$$S=\{(a, b)\,|\,a, b\in k;\ a\neq 0, 1;\ b\neq 0, 1;\ a\neq b, \text{ and } J(C_{a,b}) \text{ is isomorphic to a product of two supersingular elliptic curves}\},$$

$$S'=\{(\lambda, \mu)\,|\,\lambda, \mu\in k;\ \lambda\neq\mu;\ \Phi(\lambda)=\Phi(\mu)=0\}.$$

Then, by Lemma 2.4, we have a mapping $f: S\mapsto S'$ which sends (a, b) to (λ, μ) defined by

$$\begin{cases}\lambda=(b-a)/(1-a),\\ \mu=(b-a)/b(1-a).\end{cases} \tag{2.9}$$

By (2.9) and Lemma 2.4, we see that f is bijective. Since $\Phi(\lambda)$ is of degree $(p-1)/2$ without any multiple zeros (cf. Igusa [8]), we have

$$|S'|=\{(p-1)/2\}\{(p-1)/2\}-(p-1)/2=(p-1)(p-3)/4.$$

Since f is bijective, we thus have

$$|S|=(p-1)(p-3)/4. \tag{2.10}$$

We set

$$T=\{(a, b)\in S\,|\,ab=1,\ a=b^2 \text{ or } a^2=b\} \quad \text{and} \quad T'=f(T).$$

By the definition of f, we thus have

$$T'=\{(\lambda, \mu)\in S'\,|\,\mu=1/\lambda,\ \mu=1-\lambda \text{ or } \mu=\lambda/(\lambda-1)\}.$$

We have the following relation between the λ-invariant and the j-invariant of the elliptic curve defined by (2.8):

$$j=2^8(\lambda^2-\lambda+1)^3/\lambda^2(\lambda-1)^2.$$

If $\lambda=-1$, $1/2$ or 2, then we have $j=1728$. Therefore, these elliptic curves

E_{-1}, $E_{1/2}$, E_2 are supersingular if and only if $p\equiv 3 \pmod 4$. We denote by ζ a primitive sixth root of unity. If $\lambda=\zeta$ or ζ^5, then we have $j=0$. Therefore, these elliptic curves E_ζ, E_{ζ^5} are supersingular if and only if $p\equiv 2 \pmod 3$ (cf. for instance, Hartshorne [4, p. 334]). Using these facts, we can compute the number of elements of T' as follows:

$$|T'|=3(p-1)/2-2\left\{1-\left(\frac{-3}{p}\right)\right\}-3\left\{1-\left(\frac{-1}{p}\right)\right\}/2.$$

Since f is bijective, we thus have

$$|T|=3(p-1)/2-2\left\{1-\left(\frac{-3}{p}\right)\right\}-3\left\{1-\left(\frac{-1}{p}\right)\right\}/2.$$

By Lemmas 2.2 and 2.3, we have

$$\begin{aligned} n_1+n_2&=(|S|-|T|)/12\\ &=(p-1)(p-3)/4-(p-1)/8+\left\{1-\left(\frac{-3}{p}\right)\right\}/6\\ &\quad+\left\{1-\left(\frac{-1}{p}\right)\right\}/8. \end{aligned}$$

Hence, by (1.4), we have the following:

Proposition 2.5.

$$\begin{aligned} n_1&=(p-1)(p-17)/48+\left\{1-\left(\frac{-2}{p}\right)\right\}/2+\left\{1-\left(\frac{-3}{p}\right)\right\}/2\\ &\quad+\left\{1-\left(\frac{-3}{p}\right)\right\}/8. \end{aligned}$$

§ 3. The class number of the principal genus for $g=2$

In this section, we assume char. $k=p\geqq 5$, unless otherwise mentioned. Let $\mathscr{A}_{g,d}$ (resp. $\mathscr{A}_{g,d,n}$, $(p,n)=1$) be the coarse moduli scheme of polarized abelian varieties of dimension g with polarization of degree d^2 (resp. with polarization of degree d^2 and level n-structure) defined over k. In case $n\geqq 3$, it is well-known that $\mathscr{A}_{g,d,n}$ is a fine moduli scheme (cf. Mumford and Fogarty [15, Section 7]). We consider in this section the case $g=2$, $d=1$ and $n=3$. Then we have a Galois covering

$$\varphi\colon \mathscr{A}_{2,1,3}\longrightarrow \mathscr{A}_{2,1}.$$

The Galois group is isomorphic to $\mathrm{PSp}(4, \boldsymbol{Z}/3\boldsymbol{Z})$ (cf. Mumford and

Fogarty [15, p. 190]). As is well-known, the order of this group is given by

$$|\mathrm{PSp}(4, \boldsymbol{Z}/3\boldsymbol{Z})| = 5 \cdot 3^4 \cdot 2^6.$$

We denote by $\mathscr{S}$ the set of points in $\mathscr{A}_{2,1,3}$ which correspond to abelian surfaces which are isomorphic to a product of two supersingular elliptic curves. We proved in Katsura and Oort [10] the following theorem by an algebraic method.

Theorem 3.1. $|\mathscr{S}| = 9(p-1)(p^2+1)$.

The group $\mathrm{PSp}(4, \boldsymbol{Z}/3\boldsymbol{Z})$ acts on $\mathscr{S}$. Let P be a point of $\mathscr{S}$, and (X, C) a principally polarized abelian surface which corresponds to $\varphi(P)$. We may assume as before that C is a (not necessarily irreducible) curve of genus two on X by the result of Weil mentioned in Section 1. The curve C has the canonical involution ι, which induces the inversion of X. We set

$$\mathrm{RA}(X, C) = \mathrm{Aut}(X, C)/\langle \iota \rangle.$$

Then, we have

(3.1) $\mathrm{RA}(C) \simeq \mathrm{RA}(X, C) \simeq$ the stabilizer at P of $\mathrm{PSp}(4, \boldsymbol{Z}/3\boldsymbol{Z})$.

Therefore, we have

(3.2) $$\sum_{(X,C)} 5 \cdot 3^4 \cdot 2^6 / |\mathrm{RA}(X, C)| = 9(p-1)(p^2+1),$$

where (X, C) runs through isomorphism classes of principally polarized abelian surfaces such that X is isomorphic to a product of two supersingular elliptic curves. The mass formula for supersingular elliptic curves is as follows:

(3.3) $$\sum_E 1/|\mathrm{RA}(E)| = (p-1)/12,$$

where E runs through isomorphism classes of supersingular elliptic curves. This is obtained by an algebraic method (cf. Igusa [8]). Using (3.2) and (3.3), by elementary calculation, we have the mass formula

(3.4) $$\sum_C 1/|\mathrm{RA}(C)| = (p-1)(p-2)(p-3)/2880,$$

where C runs through isomorphism classes of non-singular irreducible curves of genus two whose Jacobian varieties $J(C)$ are isomorphic to a product of two supersingular elliptic curves (cf. Ibukiyama, Katsura and Oort [7, Section 3]). We note that if we use $\mathscr{A}_{2,1,5}$ instead of $\mathscr{A}_{2,1,3}$, then we can prove (3.4) in the case of $p=2$, 3. If $p=2$ or 3, then the right-hand

side of (3.4) is equal to zero. This means that in the case of $p=2$ or 3, there exists no non-singular irreducible curve C of genus two such that $J(C)$ is isomorphic to a product of two supersingular elliptic curves. Hence, by (1.2) and Theorem 1.1, we have

$$H_2=1 \qquad \text{if } p=2 \text{ or } 3. \tag{3.5}$$

If $p=5$, we have the curve C defined by

$$y^2=x(x^4-1)$$

with $|\mathrm{RA}(C)|=120$ (cf. Igusa [9]). The Jacobian variety $J(C)$ is isomorphic to a product of two supersingular elliptic curves (cf. Ibukiyama, Katsura and Oort [7, Proposition 1.22]). Therefore, in the case of $p=5$, by (3.4) this curve C is the unique curve whose Jacobian variety $J(C)$ has such a property. Hence, by (1.2) and Theorem 1.1, we have

$$H_2=2 \qquad \text{if } p=5. \tag{3.6}$$

Now, we assume $p\geqq 7$. Then, by (1.3) and (3.3), we have

$$\begin{aligned} &n_0+n_1/2+n_2/6+n_3/4+n_4/12+n_5/24+n_6/5 \\ &\quad =(p-1)(p-2)(p-3)/2880. \end{aligned} \tag{3.7}$$

Therefore, by (1.4) and Proposition 2.5, we have the following:

Proposition 3.2.

$$\begin{aligned} n_0=&(p-1)(p^2-35p+346)/2880-\left\{1-\left(\frac{-1}{p}\right)\right\}\Big/32 \\ &-\left\{1-\left(\frac{-2}{p}\right)\right\}\Big/8-\left\{1-\left(\frac{-3}{p}\right)\right\}\Big/9 \\ &+\begin{cases} 0 & \text{if } p\equiv 1, 2, 3 \pmod 5, \\ -1/5 & \text{if } p\equiv 4 \pmod 5. \end{cases} \end{aligned}$$

By Theorem 1.1, we have

$$H_2=n+n_0+n_1+n_2+n_3+n_4+n_5+n_6.$$

Hence, by (3.5), (3.6), (1.4) and Propositions 2.5 and 3.2, we have the following:

Theorem 3.3. $H_2=1$ *if* $p=2$ *or* 3,
$H_2=2$ *if* $p=5$,

and for $p\geqq 7$, *we have*

$$H_2=(p-1)(p+12)(p+23)/2880$$
$$+\{(2p+13)/96\}\left\{1-\left(\frac{-1}{p}\right)\right\}+\{(p+11)/36\}\left\{1-\left(\frac{-3}{p}\right)\right\}$$
$$+\left\{1-\left(\frac{-2}{p}\right)\right\}/8+\left\{1-\left(\frac{-3}{p}\right)\right\}\left\{1-\left(\frac{-1}{p}\right)\right\}/12$$
$$+\begin{cases}0 & \text{if } p\equiv 1, 2, 3 \pmod 5,\\ 4/5 & \text{if } p\equiv 4 \pmod 5.\end{cases}$$

Remark 3.4. Ekedahl has proved the following result (and our claims for $g=2$ and $p\leq 3$ also follow from this: let C be a non-singular hyperelliptic curve of genus $g\geq 2$ over a field of characteristic p whose Jacobian variety is isomorphic to a product of supersingular elliptic curves. Then, $g\leq(p-1)/2$ (cf. T. Ekedahl, On supersingular curves and abelian varieties, preprint, Univ. Paris-Sud, Orsay (1984)).

§ 4. The flag type quotient and the theory of descent

In this section, we recall some basic facts on supersingular abelian varieties and prove easy lemmas on the descent of polarizations.

Let k be an algebraically closed field of characteristic $p\geqq 2$. Let S be a noetherian scheme over k, and let $f: G\to S$ be a group scheme over S. For a geometric point x on S, we denote by G_x the fibre $f^{-1}(x)$. For an open set U of S, we denote $f^{-1}(U)$ by G_U. Now, let $\mathscr{X}\to S$ be an abelian scheme over S. We denote by $\mathscr{X}[F^i]$ the kernel of the iterated Frobenius morphism $F^i: \mathscr{X}\to\mathscr{X}^{(p^i/S)}$ (cf. e.g. Oda [17, p. 78]). For the sake of simplicity, we write $\mathscr{X}^{(p^i)}$ instead of $\mathscr{X}^{(p^i/S)}$. For an integer n, we denote by $[n]_{\mathscr{X}}$ the multiplication by n in $\mathscr{X}$ over S. From here on, by a polarization μ on $\mathscr{X}$, we mean a polarization in the sense of Mumford and Fogarty [15, Definition 6.3], that is, μ is an S-homomorphism from $\mathscr{X}$ to $\mathscr{X}^t$ which satisfies usual conditions. For an abelian variety X over k, we denote by $\hat{X}$ the formal group associated with X.

For a polarized abelian variety (X, λ) over k of dimension g with polarization λ of degree d^2, we denote by $[(X, \lambda)]$ the point of $\mathscr{A}_{g,d}$ which corresponds to (X, λ). We denote by

$$V\subset\mathscr{A}_{g,d}$$

the locus of supersingular abelian varieties, that is, $[(X, \lambda)]\in V$ if and only if X is isogenous to a product of g supersingular elliptic curves (cf. Oort [20, Theorem 4.2]). We call V the supersingular locus.

We denote by α_p the local-local group scheme of rank p over k. For a commutative group scheme (or a formal group) X over k, we define

$$a(X) := \dim_k (\mathrm{Hom}\,(\alpha_p, X)),$$

where $\mathrm{Hom}\,(\alpha_p, X)$ is a right module over $\mathrm{End}\,(\alpha_p) \simeq k$ (this number was denoted by $\tau(X)$ in Oort [19, II, 12–3]). Let $Z \subset \mathscr{A}_{g,d}$ be an irreducible closed subset and let K be an algebraically closed field containing the function field $k(Z)$ of Z. We define

$$a(-/Z \subset \mathscr{A}_{g,d}) := a(X),$$

where (X, λ) is a polarized abelian variety corresponding to the k-generic point of Z. (cf. Norman and Oort [16, p. 431]); note that this implies that there exists a non-empty Zariski open set $Z^\circ \subset Z$ such that

$$[(Y, \mu)] \in Z^\circ \text{ if and only if } a(Y) = a(-/Z \subset \mathscr{A}_{g,d}).$$

For an abelian variety (or a formal group) X over k, we denote by

$$A(X) \subset X$$

the smallest subgroup scheme of X such that any homomorphism from α_p to X factors through $A(X)$; note that $A(X)$ exists for any abelian variety (or any formal group) X, and we have

$$A(X) \simeq (\alpha_p)^{a(X)}.$$

From here on, we fix a supersingular elliptic curve E defined over the finite field $\boldsymbol{F}_p$ with p elements (for the existence, see Deuring [2, p. 199–p. 200]).

Definition 4.1. *A flag type quotient* (*ftq*, for short) is a sequence of isogenies φ_i $(1 \leqq i \leqq g-1)$ of abelian varieties Y_i $(0 \leqq i \leqq g-1)$ of dimension g:

$$E^g = Y_{g-1} \xrightarrow{\varphi_{g-1}} Y_{g-2} \xrightarrow{\varphi_{g-2}} \cdots \longrightarrow Y_1 \xrightarrow{\varphi_1} Y_0 = Y \tag{4.1}$$

with $\mathrm{Ker}\,\varphi_i \simeq (\alpha_p)^i$ $(1 \leqq i \leqq g-1)$.

By Oda and Oort [18, Theorem 2.2] and Shioda [22, Theorem 3.5], we know that for any supersingular abelian variety X there exists a ftq ending at $Y_0 = X$. It should be noticed that our condition for ftq is weaker than the condition in Oda and Oort [18, Definition on p. 606].

Definition 4.2. *A principally polarized flag type quotient* (*ppftq* for short) is a ftq as in (4.1) with polarizations μ_i of Y_i $(0 \leqq i \leqq g-1)$ such that $\mu_0 = \lambda$ is an isomorphism from Y_0 to Y_0^t, and that $\varphi_i^*(\mu_{i-1}) = \mu_i$ $(1 \leqq i \leqq g-1)$ and $\mathrm{Ker}\,\mu_i \subset Y_i[F^i]$ $(0 \leqq i \leqq g-1)$. We denote this by

$$(Y_{g-1}, \mu_{g-1}) \xrightarrow{\varphi_{g-1}} (Y_{g-2}, \mu_{g-2}) \xrightarrow{\varphi_{g-2}} \cdots \xrightarrow{\varphi_1} (Y_0, \mu_0).$$

Lemma 4.3. *Under the notations as in Definition* 4.2, *assume* $g \geqq 2$. *Then,* $\operatorname{Ker} \mu_1 \simeq E^2[F] \simeq (\alpha_p)^2$ *and* $\operatorname{Ker} \mu_{g-1} \simeq E^g[F^{g-1}]$. *In particular,* $\deg \mu_1 = p^2$ *and* $\deg \mu_{g-1} = p^{g(g-1)}$.

Proof. By definition, we have $\deg \mu_{g-1} = p^{g(g-1)}$. Therefore, the latter part follows from $\operatorname{Ker} \mu_{g-1} \subset E^g[F^{g-1}]$ and $\deg F^{g-1} = p^{g(g-1)}$. Since μ_1 is a polarization, $\operatorname{Ker}(\mu_1)$ is isomorphic to its Cartier dual (cf. Mumford [14, p. 234, Corollary 2]). Since $\operatorname{Ker} \mu_1$ is killed by F, we see that $\operatorname{Ker} \mu_1$ is also killed by the Verschiebung V. Hence, by $\deg \mu_1 = p^2$, we have $\operatorname{Ker} \mu_1 \simeq (\alpha_p)^2$. q.e.d.

Lemma 4.4 (Oda and Oort [18, Theorem 2.2]). *Let* (X, λ) *be a principally polarized supersingular abelian variety, and assume* $a(X) = 1$. *Then, there exists a ppftq ending at* $(X, \lambda) = (Y_0, \mu_0)$. *Set*

$$Y^{(1)} = X^t/A(X^t), \quad Y^{(2)} = Y^{(1)}/A(Y^{(1)}), \quad \cdots, \quad Y^{(g-1)} = Y^{(g-2)}/A(Y^{(g-2)}),$$
$$Y_1 = (Y^{(1)})^t, \quad Y_2 = (Y^{(2)})^t, \quad \cdots, \quad Y_{g-1} = (Y^{(g-1)})^t.$$

Then, $Y_{g-1} \simeq E^g$ *and the ppftq ending at* (X, λ) *is uniquely given by*

$$(Y_{g-1}, \mu_{g-1}) \xrightarrow{\varphi_{g-1}} (Y_{g-2}, \mu_{g-2}) \xrightarrow{\varphi_{g-2}} \cdots \xrightarrow{\varphi_1} (Y_0, \mu_0),$$

where φ_i $(1 \leqq i \leqq g-1)$ *is the dual homomorphism of the canonical projection* $\varphi_i^t \colon Y^{(i-1)} \to Y^{(i)}$, *and where* $\mu_i = \varphi_i^*(\mu_{i-1})$ $(1 \leqq i \leqq g-1)$.

Now, we give two lemmas on the descent of polarizations.

Lemma 4.5. *Let* (X, μ) *be a polarized abelian variety over* k *such that* $\operatorname{Ker} \mu$ *contains a subgroup scheme* H *which is isomorphic to* α_p. *Then, the polarization* μ *descends to a polarization on* X/H.

Proof. This lemma follows from Mumford [14, p. 223, Lemma 1, and p. 231, Corollary to Theorem 2]. q.e.d.

Lemma 4.6. *Let* μ *be a polarization on* $Y = E^g$ *such that* $\operatorname{Ker} \mu \supset Y[F^2] = \operatorname{Ker}[p]_Y$. *Then, there exists a polarization* ρ *on* Y *such that* $\mu = F^*(\rho)$.

Proof. We consider the immersion γ_1 of α_p to the first factor of E^g. We denote by

$$\pi_1 \colon Y = E^g \longrightarrow (E/\gamma_1(\alpha_p)) \times E^{g-1} = Y_1$$

the canonical projection. Then, by Lemma 4.5, we can find a polarization μ_1 on Y_1 such that $\mu=\pi_1^*(\mu_1)$. By our choice of γ_1, it is easy to see that

$$\mathrm{Ker}\,\mu_1 \supset E^{g-1}[F^2].$$

Next, we consider the immersion γ_2 of α_p to the second factor E of $(E/\gamma_1(\alpha_p)) \times E^{g-1}$. Then, by Lemma 4.5, the polarization μ_1 descends to a polarization μ_2 on $(E/\gamma_1(\alpha_p))\times(E/\gamma_2(\alpha_p))\times E^{g-2}$ with $\mathrm{Ker}\,\mu_2 \supset \{0\}\times\{0\}\times E^{g-2}[F^2]$. We continue this procedure g times. Since $\mathrm{Ker}\,F \simeq (\alpha_p)^g$, we conclude that there exists a polarization ρ on Y such that $\mu=F^*(\rho)$. q.e.d.

§ 5. The construction of families

In this section, we construct families of principally polarized supersingular abelian threefolds. We keep the notation in Section 4. As in Section 4, we fix a supersingular elliptic curve E defined over $\boldsymbol{F}_p$. Let μ be a polarization on $Y=E^3$ such that

$$\mathrm{Ker}\,\mu = Y[F^2]. \tag{5.1}$$

We set

$$\boldsymbol{P}=\{\psi \mid \psi\colon (\alpha_p)^2 \hookrightarrow E^3=Y\}/k^*,$$

which is clearly isomorphic to the projective plane. We denote by $[\psi]$ the point of $\boldsymbol{P}$ which corresponds to an immersion ψ. We write $\mathrm{Im}\,\psi \subset Y$ for the image of ψ, and we set

$$Z_\psi = Y/\mathrm{Im}\,\psi.$$

We have the canonical projection $\pi\colon Y \to Z_\psi$.

Lemma 5.1. *Under the notation as above, for any ψ, there exists a polarization ρ_ψ on Z_ψ such that*

$$\mu=\pi^*(\rho_\psi).$$

Proof. Since the Frobenius morphism F of Y factors through π, this lemma follows from Lemma 4.6. q.e.d.

The following proposition is essentially due to Oda and Oort [18, Lemma 4.2], and our proof is inspired by Moret-Bailly [13, p. 138–p. 139].

Proposition 5.2. *Under the notation as above, there exists a non-singular curve $\Gamma(\mu)$ in $\boldsymbol{P}$ with*

$$\deg \Gamma(\mu)=p+1$$

such that $\operatorname{Ker}\rho_\psi \subset Z_\psi\ [F]$ *if and only if* $[\psi]\in\Gamma(\mu)$.

Proof. In order to carry out the computation, we use the contravariant Dieudonné module theory. Thus, the Dieudonné module $\mathcal{M}(\hat{E})=M$ is generated over the ring $W=W_\infty(k)$ of infinite Witt vectors by

$$e_1,\ Fe_1=Ve_1,\ e_2,\ Fe_2=Ve_2,\ e_3,\ Fe_3=Ve_3, \tag{5.2}$$

and the morphism ψ corresponds to a surjective homomorphism

$$k^2 \xleftarrow{\mathcal{M}(\psi)} M. \tag{5.3}$$

The Dieudonné module $\mathcal{M}(\hat{Z}_\psi)=\operatorname{Ker}(\mathcal{M}(\psi))$ is generated over W by

$$x_\psi,\ Fe_1,\ Fe_2,\ Fe_3,\ pe_1,\ pe_2,\ pe_3, \tag{5.4}$$

where $x_\psi=a_1e_1+a_2e_2+a_3e_3$ with $a_i\in W\ (i=1,2,3)$, and where $\alpha_i=a_i \bmod p \in W/pW\simeq k$ are thought of as the coordinates of $[\Psi]\in \boldsymbol{P}$. We set

$$\boldsymbol{K}=\operatorname{Ker}\mu.$$

By (5.1), we have

$$\mathcal{M}(\boldsymbol{K})\simeq M/F^2M\simeq M/pM. \tag{5.5}$$

The polarization μ gives a Riemann form on $\boldsymbol{K}$:

$$\boldsymbol{e}\colon \boldsymbol{K}\times\boldsymbol{K}\longrightarrow \boldsymbol{G}_m$$

(cf. Mumford [14, p. 222]). We denote by $(\operatorname{Ker}\pi)^\perp$ the subgroup scheme perpendicular to $\operatorname{Ker}\pi$ with respect to the form $\boldsymbol{e}$. Then, we have

$$\operatorname{Ker}\rho_\psi\simeq(\operatorname{Ker}\pi)^\perp/\operatorname{Ker}\pi$$

(cf. Mumford [14, p. 232, Lemma 2]). By (5.5), $\mathcal{M}(\boldsymbol{K})$ is a vector space over $W/pW\simeq k$, and by (5.2), the image of

$$\{e_1,\ e_2,\ e_3,\ Fe_1,\ Fe_2,\ Fe_3\} \tag{5.6}$$

is a basis of the Dieudonné module $\mathcal{M}(\boldsymbol{K})$ over k. We again denote by $\{e_1, e_2, e_3, Fe_1, Fe_2, Fe_3\}$ (resp. x_ψ) the image of $\{e_1, e_2, e_3, Fe_1, Fe_2, Fe_3\}$ (resp. x_ψ) in $\mathcal{M}(\boldsymbol{K})$. The homomorphism $\mathcal{M}(\psi)$ in (5.3) induces a homomorphism

$$\tilde{\psi}\colon \mathcal{M}(\boldsymbol{K})\longrightarrow k^2.$$

By (5.4) and (5.5), a basis of $\operatorname{Ker}\tilde{\psi}$ over k is given by

$$\{x_\psi, Fe_1, Fe_2, Fe_3\}. \tag{5.7}$$

We denote by $\mathcal{M}(\boldsymbol{K})^*$ the dual vector space of $\mathcal{M}(\boldsymbol{K})$. Then, in our case, $\mathcal{M}(\boldsymbol{K})^*$ is isomorphic to $\mathcal{D}(\mathcal{M}(\boldsymbol{K}))$ in Oda [17, Definition 3.5] as a $W[F, V]$-module. Therefore, we have a non-degenerate skew-symmetric bilinear form on $\mathcal{M}(\boldsymbol{K})^*\times\mathcal{M}(\boldsymbol{K})^*$ induced by $\boldsymbol{e}$. Hence, we have a non-degenerate skew-symmetric bilinear form

$$\boldsymbol{b}\colon \mathcal{M}(\boldsymbol{K})\times\mathcal{M}(\boldsymbol{K})\longrightarrow k$$

induced by $\boldsymbol{e}$ such that

$$\boldsymbol{b}(Fx, y)=\boldsymbol{b}(x, Vy)^p \tag{5.8}$$

for any elements x, y in $\mathcal{M}(\boldsymbol{K})$ (cf. Moret-Bailly [13, p. 138], and see also Oda [17, Section 3]). As is stated in Moret-Bailly [13], we can easily prove

$$\mathcal{M}(\operatorname{Ker}\rho_\psi)\simeq\mathcal{M}((\operatorname{Ker}\pi)^\perp/\operatorname{Ker}\pi)\simeq\operatorname{Ker}\tilde{\psi}/(\operatorname{Ker}\tilde{\psi})^\perp.$$

as $W[F, V]$-modules. Hence, we see that

$$\operatorname{Ker}\rho_\psi\subset Z_\psi[F] \qquad \text{if and only if } F(\operatorname{Ker}\tilde{\psi})\subset(\operatorname{Ker}\tilde{\psi})^\perp.$$

By (5.5), (5.6) and (5.8), we see that

$$F(\operatorname{Ker}\tilde{\psi})\subset(\operatorname{Ker}\tilde{\psi})^\perp \qquad \text{if and only if } \boldsymbol{b}(Fx_\psi, x_\psi)=0. \tag{5.9}$$

With respect to the basis (5,6), the bilinear form $\boldsymbol{b}$ is given by the 6×6 matrix (b_{ij}), where

$$b_{ij}=\boldsymbol{b}(e_i, e_j),\ b_{i+3,j}=\boldsymbol{b}(Fe_i, e_j),\ b_{i,j+3}=\boldsymbol{b}(e_i, Fe_j),\ b_{i+3,j+3}=\boldsymbol{b}(Fe_i, Fe_j)$$

for $1\leqq i\leqq3$, $1\leqq j\leqq3$. We consider the curve $\Gamma(\mu)$ in $\boldsymbol{P}$ defined by the equation:

$$\textstyle\sum_{i,j=1}^{3}\boldsymbol{b}(Fe_i, e_j)X_i^pX_j=0. \tag{5.10}$$

Then, by (5.4) and (5.9), we conclude that

Ker $\rho_\psi\subset Z_\psi[F]$ if and only if $[\psi]=(\alpha_i)$ satisfies Equation (5.10).

By (5.5) and (5.8), the 3×3 matrix $(\boldsymbol{b}(Fe_i, Fe_j))_{1\leqq i,j\leqq3}$ is the zero matrix. Since $\boldsymbol{b}$ is a non-degenerate bilinear form, we see that the 3×3 matrix $(\boldsymbol{b}(Fe_i, e_j))_{1\leqq i,j\leqq3}$ is regular. Hence, the hypersurface $\Gamma(\mu)$ defined by (5.10) is non-singular. q.e.d.

Lemma 5.3. *Let $\mathcal{G}$ be a formal group of dimension two over k which is isogenous to $(\hat{E})^2$.*

i) *If* $a(\mathscr{G})=1$, *then* $a(\mathscr{G}/H)=2$ *for the unique subgroup scheme* H *of* $\mathscr{G}$ *which is isomorphic to* α_p.

ii) *If* $a(\mathscr{G})=2$, *then* $\mathscr{G}\simeq(\hat{E})^2$.

Proof. This lemma follows from Oort [21, Corollary 7 and Theorem 2]. q.e.d.

Proposition 5.4. *Let* (X, λ) *be a principally polarized supersingular abelian threefold. Then, there exists a ppftq ending at* $(Y_0, \mu_0)=(X, \lambda)$.

Proof. We distinguish the cases:

(1) $a(X)=1$, (2) $a(X)=2$, (3) $a(X)=3$.

In Case (1), the conclusion follows from Lemma 4.4.

In Case (3), by Oort [21, Theorem 2] and Shioda [22, Theorem 3.5], we have $X\simeq E^3$. We set

$$Y_2=E^3,\ Y_0=X\simeq E^3,\ \Phi:=F: Y_2\longrightarrow Y_0,\ \text{and}\ \mu_2=\Phi^*(\lambda).$$

Then, we see $\operatorname{Ker}\mu_2=Y_2[F^2]$. We choose an immersion

$$\psi: (\alpha_p)^2\hookrightarrow Y_2,\qquad [\psi]\in\Gamma(\mu_2)\cdot$$

Then, by Proposition 5.2, there exists a polarization μ_1 on $Y_1=Y_2/\operatorname{Im}\psi$ with

$$\varphi_2: Y_2\longrightarrow Y_1,\ \varphi_2^*(\mu_1)=\mu_2,\ \text{and}\ \operatorname{Ker}\mu_1\simeq\alpha_p\times\alpha_p,$$

where φ_2 is the canonical projection. Since $\operatorname{Ker}\varphi_2\subset\operatorname{Ker}\Phi$, we have the natural morphism

$$\varphi_1: Y_1\longrightarrow Y_0$$

such that $\varphi_1\circ\varphi_2=\Phi$. It is clear that $\operatorname{Ker}\varphi_1\simeq\alpha_p$. We set

$$\mu_1=\varphi_1^*(\lambda).$$

Then, $(Y_2, \mu_2)\xrightarrow{\varphi_2}(Y_1, \mu_1)\xrightarrow{\varphi_1}(Y_0, \mu_0)=(X, \lambda)$ gives a *ppftq* ending at (X, λ) in Case (3).

In Case (2), we have $a(X^t)=2$ (cf. Oda and Oort [18, p. 599, Remark]). Since λ is a principal polarization, and since $g=3$ and $a(X)=2$, there exists a formal group $\mathscr{G}$ of dimension two with $a(\mathscr{G})=1$ such that $\hat{X}^t$ is isomorphic to $\mathscr{G}\times\hat{E}$ (cf. Oda and Oort [18, Proposition 4.1 and the proof of Corollary 4.3]). By $a(\mathscr{G})=1$, the formal group $\mathscr{G}$ has the unique subgroup scheme $\hat{H}$ which is isomorphic to α_p. We denote by H the subgroup

scheme in X^t which corresponds to $\hat{H}$ in $\hat{X}^t$. Since $a(\mathscr{G}/\hat{H})=2$ by Lemma 5.3, we have $a((\mathscr{G}\times\hat{E})/\hat{H})=3$. Therefore, we have $a(X^t/H)=3$. We set

$$Y_1=(X^t/H)^t.$$

Then, we have $a(Y_1)=3$ (cf. Oda and Oort [18, p. 599, Remark]). Therefore, we have isomorphisms $X^t/H\simeq E^3$ and $Y_1\simeq E^3$, and we have a commutative diagram:

$$\begin{array}{ccc} Y_1 & \xrightarrow{\varphi_1} & X \\ {\scriptstyle\mu_1}\downarrow & & \downarrow{\scriptstyle\lambda} \\ X^t/H & \xleftarrow{\varphi_1^t} & X^t, \end{array} \tag{5.11}$$

where φ_1^t is the canonical projection, where φ_1 is the dual of φ_1^t and where $\mu_1=\varphi_1^*(\lambda)$. Corresponding to this diagram, we have a commutative diagram of formal groups:

$$\begin{array}{ccc} \hat{Y}_1 & \xrightarrow{\hat{\varphi}_1} & \hat{X} \\ {\scriptstyle\hat{\mu}_1}\downarrow & & \downarrow{\scriptstyle\hat{\lambda}} \\ (X^t/H)^\wedge & \xleftarrow{\hat{\varphi}_1^t} & \hat{X}^t, \end{array} \tag{5.12}$$

where $\hat{\mu}_1$ (resp. $\hat{\lambda}$, resp. $\hat{\varphi}_1$, resp. $\hat{\varphi}_1^t$) is the homomorphism induced by μ_1 (resp. λ, resp. φ_1, resp. φ_1^t). Since $\hat{\lambda}$ is an isomorphism and $\hat{X}\simeq\mathscr{G}\times\hat{E}$, we see $\hat{X}^t=\mathscr{G}\times\hat{E}$. By our construction, the diagram (5.12) becomes the following:

$$\begin{array}{ccc} \hat{E}\times\hat{E}\times\hat{E} & \xrightarrow{\hat{\varphi}_1} & \mathscr{G}\times\hat{E} \\ {\scriptstyle\hat{\mu}_1=\begin{pmatrix}\mu_a & \mu_b\\ \mu_c & \mu_d\end{pmatrix}}\downarrow & & \downarrow{\scriptstyle\hat{\lambda}=\begin{pmatrix}\lambda_1 & \lambda_2\\ \lambda_3 & \lambda_4\end{pmatrix}} \\ \hat{E}\times\hat{E}\times\hat{E} & \xrightarrow{\hat{\varphi}_1^t} & \mathscr{G}\times\hat{E}, \end{array} \tag{5.13}$$

where λ_1 (resp. λ_2, resp. λ_3, resp. λ_4) is a homomorphism from $\mathscr{G}$ to $\mathscr{G}$ (resp. $\hat{E}$ to $\mathscr{G}$, resp. $\mathscr{G}$ to $\hat{E}$, resp. $\hat{E}$ to $\hat{E}$), and where μ_a (resp. μ_b, resp. μ_c, resp. μ_d) is a homomorphism from $\hat{E}\times\hat{E}$ (the first two factors) to $\hat{E}\times\hat{E}$ (the first two factors) (resp. $\hat{E}$ (the last factor) to $\hat{E}\times\hat{E}$ (the first two factors), resp. $\hat{E}\times\hat{E}$ (the first two factors) to $\hat{E}$ (the last factor), resp. $\hat{E}$ (the last factor) to $\hat{E}$ (the last factor)). It is easy to see that λ_3 is zero on the unique subgroup scheme α_p of $\mathscr{G}$. From this and the fact that λ is a principal polarization it follows that

$$\lambda_1\colon \mathscr{G}\simeq\mathscr{G} \quad\text{and}\quad \lambda_4\colon \hat{E}\simeq\hat{E}.$$

Therefore, by the definition of $\hat{\varphi}_1^t$, we conclude

$$\operatorname{Ker} \hat{\mu}_1 \simeq \alpha_p \times \alpha_p \simeq \operatorname{Ker} \mu_a \subset \hat{E} \times \hat{E}.$$

Hence, by Oort [21, the argument on p. 40], we can find a subgroup scheme $\hat{I}$ of $\hat{E} \times \hat{E}$ such that $\hat{I}$ is isomorphic to α_p, and that $(\hat{E} \times \hat{E})/\hat{I} \simeq \hat{E} \times \hat{E}$. We denote by I the subgroup scheme of Y_1 which corresponds to $\hat{I}$ in $\hat{E}^3 \simeq \hat{Y}_1$. Then, by the choice of $\hat{I}$, we see

$$Y_1/I \simeq E \times E \times E.$$

Let $\pi\colon Y_1 \to Y_1/I$ be the canonical projection. Since

$$\operatorname{Ker} \pi \simeq \alpha_p \subset \operatorname{Ker} \mu_1 \simeq \alpha_p \times \alpha_p,$$

we can find a principal polarization ρ on Y_1/I such that

$$\mu_1 = \pi^*(\rho)$$

by Lemma 4.5. We set

$$Y_2 = (Y_1/I)^{(1/p)},$$

and we consider the Frobenius morphism $F\colon Y_2 \to Y_1/I$. Then, by the property of the Frobenius morphism, we can find a morphism

$$\varphi_2\colon Y_2 \longrightarrow Y_1$$

such that $F = \pi \circ \varphi_2$. We set

$$\mu_2 = F^*(\rho).$$

Then, we have

$$\mu_2 = \varphi_2^*(\mu_1) \quad \text{and} \quad \operatorname{Ker} \mu_2 \simeq Y[F^2].$$

Hence, we get a *ppftq*

$$(Y_2, \mu_2) \xrightarrow{\varphi_2} (Y_1, \mu_1) \xrightarrow{\varphi_1} (Y_0, \mu_0) = (X, \lambda)$$

ending at (X, λ). q.e.d.

Definition 5.5. Let S be a k-scheme. Let

$$\mathscr{Y}_2 \xrightarrow{\varphi_2} \mathscr{Y}_1 \xrightarrow{\varphi_1} \mathscr{Y}_0$$

be a sequence of abelian schemes $\mathscr{Y}_i$ $(i = 0, 1, 2)$ over S with polarizations

μ_i on $\mathscr{Y}_i$ $(i=0, 1, 2)$ (cf. Mumford and Fogarty [15, p. 120, Definition 6.3]) and homomorphisms φ_i $(i=1, 2)$ such that

$$\varphi_i^*(\mu_{i-1})=\mu_i \ (i=1, 2) \quad \text{and} \quad \operatorname{Ker} \mu_i \subset \mathscr{Y}_i[F^i] \ (i=0, 1. 2).$$

This sequence is called *a principally polarized flag type quotient over* S (*ppftq*/S, for short) if for every point x of S, there exists a Zariski open neighborhood $\mathscr{U}$ of x in S such that

$$\mathscr{Y}_{2,\mathscr{U}} \simeq E^3 \times \mathscr{U} \quad \text{and} \quad (\operatorname{Ker} \varphi_i)_{\mathscr{U}} \simeq (\alpha_p)^i \times \mathscr{U}.$$

Now, we construct a family of principally polarized supersingular abelian threefolds. We consider an abelian threefold $Y=E^3$ with polarization μ which satisfies Condition (5.1). Let $\Gamma(\mu)$ be the curve obtained in Proposition 5.2. We set

$$\mathscr{Y}'_2 = Y \times \Gamma(\mu),$$

and we consider the group scheme

$$p'_2 \colon \mathscr{Y}'_2 \longrightarrow \Gamma(\mu),$$

where p'_2 is the projection to the second factor $\Gamma(\mu)$. For a scheme S, we denote by id_S the identity mapping from S to S. We denote by μ'_2 the polarization of the abelian scheme $p'_2 \colon \mathscr{Y}'_2 \to \Gamma(\mu)$ defined by $\mu \times \mathrm{id}_{\Gamma(\mu)}$. Let $p''_2 \colon \mathscr{I} \to \Gamma(\mu)$ be a subgroup scheme of $p'_2 \colon \mathscr{Y}'_2 \to \Gamma(\mu)$ which satisfies the following two conditions:

(i) all geometric fibres are isomorphic to $\alpha_p \times \alpha_p$,

(ii) for the point $[\psi] \in \Gamma(\mu)$, the fibre $(p''_2)^{-1}([\psi])$ coincides with $\operatorname{Im} \psi$.

By the construction of $\Gamma(\mu)$, such a subgroup scheme exists. We set

$$\mathscr{Y}'_1 = \{Y \times \Gamma(\mu)\}/\mathscr{I}.$$

Let $\varphi'_2 \colon \mathscr{Y}'_2 \to \mathscr{Y}'_1$ be the canonical projection. Denoting by F the Frobenius morphism of the abelian scheme $p_2 \colon \mathscr{Y}'_2 \to \Gamma(\mu)$, we see that there exists a morphism χ from $\mathscr{Y}'_1$ to $\mathscr{Y}'^{(p)}_2$ such that the following diagram commutes:

$$\begin{array}{ccccc} E^3 \times \Gamma(\mu) & \simeq & \mathscr{Y}'_2 & \xrightarrow{\varphi'_2} & \mathscr{Y}'_1 \\ & & & {\scriptstyle F}\searrow \quad \swarrow{\scriptstyle \chi} & \\ & & E^3 \times \Gamma(\mu) & \simeq & \mathscr{Y}'^{(p)}_2 \end{array} . \tag{5.14}$$

By Lemma 4.6, the polarization μ'_2 on $\mathscr{Y}'_2$ descends to $\mathscr{Y}'^{(p)}_2$. Hence, by (5.14), there exists a polarization μ'_1 on $\mathscr{Y}'_1$ such that

$$\mu_2' = \varphi_2'^*(\mu_1').$$

Moreover, by construction, we have

$$\operatorname{Ker} \mu_1' \subset \mathscr{Y}_1'[F].$$

Let $A(\operatorname{Ker} \mu_1') \to \Gamma(\mu)$ be the smallest subgroup scheme of $\operatorname{Ker} \mu_1' \to \Gamma(\mu)$ having the following universal mapping property:

(5.15) for any affine open subset $\mathscr{U}$ of $\Gamma(\mu)$, and for any group scheme $G \to \mathscr{U}$ over $\mathscr{U}$ whose geometric fibres are isomorphic to α_p, and for any morphism $g: G \to (\operatorname{Ker} \mu_1')_{\mathscr{U}}$ over $\mathscr{U}$, there exists a morphism h from G to $(A(\operatorname{Ker} \mu_1'))_{\mathscr{U}}$ over $\mathscr{U}$ such that g factors through h.

By the theory of p-Lie algebras, which works over any integral domain of characteristic p (cf. Demazure and Gabriel [1, II. 7.4.3]), such a group scheme exists and is of rank two and height one over $\Gamma(\mu)$ by the construction of $\Gamma(\mu)$. We define

$$\mathscr{F}(\mu) = \boldsymbol{P}(\operatorname{Lie}(A(\operatorname{Ker} \mu_1') \longrightarrow \Gamma(\mu))).$$

We denote by

$$f: \mathscr{F}(\mu) \longrightarrow \Gamma(\mu) \tag{5.16}$$

the natural morphism.

Proposition 5.6. *$\mathscr{F}(\mu)$ is a non-singular variety of dimension two.*

Proof. This proposition follows from the above construction of $\mathscr{F}(\mu)$ and Proposition 5.2. q.e.d.

We set

$$\mathscr{Y}_i = \mathscr{Y}_i' \times_{\Gamma(\mu)} \mathscr{F}(\mu) \quad \text{and} \quad \mu_i = \mu_i' \times_{\Gamma(\mu)} id_{\mathscr{F}(\mu)} \ (i = 1, 2).$$

We have group schemes over $\mathscr{F}(\mu)$:

$$p_i: \mathscr{Y}_i \longrightarrow \mathscr{F}(\mu) \qquad (i = 1, 2),$$

where p_i's are the natural projections onto $\mathscr{F}(\mu)$. We have also the homomorphism

$$\varphi_2: \mathscr{Y}_2 \longrightarrow \mathscr{Y}_1$$

induced by φ_2'. Since $A(\operatorname{Ker} \mu_1') \to \Gamma(\mu)$ is a flat group scheme over $\Gamma(\mu)$ whose geometric fibres are isomorphic to $(\alpha_p)^2$, for any point x of $\Gamma(\mu)$ we can find a Zariski open neighborhood $\mathscr{U}(\mu)$ of x such that

$$(A(\mathrm{Ker}\,\mu_1'))_{\mathscr{U}(\mu)} \simeq (\alpha_p)^2 \times \mathscr{U}(\mu) \quad \text{and} \quad f^{-1}(\mathscr{U}(\mu)) \simeq \boldsymbol{P}^1 \times \mathscr{U}(\mu).$$

We set

$$\mathscr{T}(\mathscr{U}(\mu)) = f^{-1}(\mathscr{U}(\mu)). \tag{5.17}$$

Since $A(\mathrm{Ker}\,\mu_1) \simeq A(\mathrm{Ker}\,\mu_1') \times_{\Gamma(\mu)} \mathscr{F}(\mu)$, we have

$$\mathscr{Y}_{1,\mathscr{T}(\mathscr{U}(\mu))} \simeq (\alpha_p)^2 \times \mathscr{T}(\mathscr{U}(\mu)) \simeq (\alpha_p)^2 \times \boldsymbol{P}^1 \times \mathscr{U}(\mu).$$

We denote by q the projection from $(\alpha_p)^2 \times \boldsymbol{P}^1 \times \mathscr{U}(\mu)$ onto $(\alpha_p)^2 \times \boldsymbol{P}^1$. We consider the subgroup scheme H of $(\alpha_p)^2 \times \boldsymbol{P}^1$ over $\boldsymbol{P}^1$ which was constructed in Moret-Bailly [13, p. 128]. We set

$$\mathscr{H} = q^{-1}(H).$$

Then, $\mathscr{H}$ is a subgroup scheme of $(\alpha_p)^2 \times \mathscr{T}(\mathscr{U}(\mu))$ over $\mathscr{T}(\mathscr{U}(\mu))$, hence a subgroup scheme of $\mathscr{Y}_{1,\mathscr{T}(\mathscr{U}(\mu))}$ over $\mathscr{T}(\mathscr{U}(\mu))$. For the sake of simplicity, we write $\mathscr{Y}_i$ instead of $\mathscr{Y}_{i,\mathscr{T}(\mathscr{U}(\mu))}$. We set

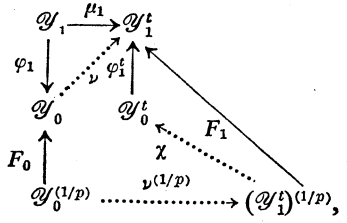
$$\mathscr{Y}_0 = \mathscr{Y}_1/\mathscr{H}.$$

This is a group scheme over $\mathscr{T}(\mathscr{U}(\mu))$. We denote by

$$\varphi_1 : \mathscr{Y}_1 \longrightarrow \mathscr{Y}_0$$

the canonical projection. We consider the following commutative diagram:

(5.18)



where F_0, F_1 are the Frobenius morphisms. Since $\mathrm{Ker}\,\varphi_1 \subset \mathrm{Ker}\,\mu_1$, we can find a homomorphism ν from $\mathscr{Y}_0$ to $\mathscr{Y}_1^t$. Therefore, we can find $\nu^{(1/p)}$ from $\mathscr{Y}_0^{(1/p)}$ to $(\mathscr{Y}_1^t)^{(1/p)}$. By the property of the Frobenius morphism, we can find a homomorphism χ from $(\mathscr{Y}_1^t)^{(1/p)}$ to $\mathscr{Y}_0^t$ such that $F_1 = \varphi_1^t \circ \chi$.

Lemma 5.7. *Under the notation as above,*

$$\mathrm{Ker}\,F_0 \subset \mathrm{Ker}\,(\chi \circ \nu^{(1/p)}). \tag{5.19}$$

Proof. Since on each fibre over $\mathscr{T}(\mathscr{U}(\mu))$, the polarization μ_1 descends

to a polarization on $\mathscr{Y}_0$ by Lemma 4.5, we see that (5.19) holds on each fibre over $\mathscr{T}(\mathscr{U}(\mu))$. This shows $\mathrm{Ker}\, F_0 \subset \mathrm{Ker}\,(\chi \circ \nu^{(1/p)})$. q.e.d.

Using this lemma, we can find a $\mathscr{T}(\mathscr{U}(\mu))$-homomorphism μ_0 from $\mathscr{Y}_0$ to $\mathscr{Y}_0^t$. By Lemma 4.5, this $\mathscr{T}(\mathscr{U}(\mu))$-homomorphism μ_0 is a principal polarization on $\mathscr{Y}_0$ in the sense of Mumford and Fogarty [15, Definition 6.3]. Hence, for every polarization μ on $Y=E^3$ such that $\mathrm{Ker}\,(\mu)=Y[F^2]$, we have constructed a ppftq/$\mathscr{T}(\mathscr{U}(\mu))$:

$$(\mathscr{Y}_2, \mu_2) \xrightarrow{\varphi_2} (\mathscr{Y}_1, \mu_1) \xrightarrow{\varphi_1} (\mathscr{Y}_0, \mu_0). \tag{5.20}$$

§ 6. The structure of the supersingular locus in $\mathscr{A}_{3,1}$

In this section, we keep the notation in Sections 4 and 5. We again assume $g=3$. We denote by V the supersingular locus in $\mathscr{A}_{3,1}$. Let E be a supersingular elliptic curve defined over $\boldsymbol{F}_p$, and let (E^3, μ) be a polarized abelian threefold with polarization μ which satisfies Condition (5.1): $\mathrm{Ker}\,(\mu)=Y[F^2]$. As in Section 5, using (E^3, μ), we can construct a family of principally polarized abelian threefolds over $\mathscr{T}(\mathscr{U}(\mu))$:

$$p_0 \colon \mathscr{Y}_0 \longrightarrow \mathscr{T}(\mathscr{U}(\mu)). \tag{6.1}$$

Therefore, by the property of the moduli variety $\mathscr{A}_{3,1}$, we have a morphism

$$g \colon \mathscr{T}(\mathscr{U}(\mu)) \longrightarrow \mathscr{A}_{3,1}. \tag{6.2}$$

We set

$$\mathscr{T}(\mathscr{U}(\mu))^\circ = \{x \in \mathscr{T}(\mathscr{U}(\mu)) \mid a(\mathscr{Y}_{0,x})=1\}.$$

Lemma 6.1. *$\mathscr{T}(\mathscr{U}(\mu))^\circ$ is a non-empty Zariski open subset of $\mathscr{T}(\mathscr{U}(\mu))$.*

Proof. Since $\mathscr{T}(\mathscr{U}(\mu))^\circ$ is a Zariski open subset, it suffices to prove that $\mathscr{T}(\mathscr{U}(\mu))^\circ$ is non-empty. By Oda and Oort [18, Theorem 2.4 (i) and Theorem 3.2], we can find a Zariski open subset $\mathscr{T}(\mathscr{U}'(\mu))$ and a point x of $\mathscr{T}(\mathscr{U}'(\mu))$ such that $a(\mathscr{Y}_{0,x})=1$. Hence, $\mathscr{T}(\mathscr{U}'(\mu))^\circ$ is a non-empty Zariski open subset. As in (6.2), we have two morphisms

$$g \colon \mathscr{T}(\mathscr{U}(\mu)) \longrightarrow \mathscr{A}_{3,1} \quad \text{and} \quad g' \colon \mathscr{T}(\mathscr{U}'(\mu)) \longrightarrow \mathscr{A}_{3,1}. \tag{6.3}$$

By the construction of our families, we see

$$g(\mathscr{T}(\mathscr{U}(\mu)) \cap \mathscr{T}(\mathscr{U}'(\mu))) = g'(\mathscr{T}(\mathscr{U}(\mu)) \cap \mathscr{T}(\mathscr{U}'(\mu))). \tag{6.4}$$

Hence, $\mathscr{T}(\mathscr{U}(\mu))^\circ$ is non-empty. q.e.d.

Proposition 6.2. *The closure of the image of g in* (6.2) *does not depend on the choice of open sets* $\mathcal{U}(\mu)$ *of* $\Gamma(\mu)$.

Proof. Let $\mathcal{U}(\mu)$ and $\mathcal{U}'(\mu)$ be two Zariski open sets of $\Gamma(\mu)$. As in (6.3), we have two morphisms g and g', and we see that (6.4) holds. Using the notation in (5.16), we see that $f^{-1}(\mathcal{U}(\mu)\cap\mathcal{U}'(\mu))$ is dense in $\mathcal{F}(\mu)$. Hence, we conclude that the closure of the image of g coincides with the closure of the image of g'. q.e.d.

Proposition 6.3. *The morphism g in* (6.2) *is of finite degree.*

Proof. By Lemma 6.1, the set $\mathcal{T}(\mathcal{U}(\mu))^\circ$ is a non-empty Zariski open set. Let x_1 and x_2 be two points of $\mathcal{T}(\mathcal{U}(\mu))^\circ$ such that $g(x_1)=g(x_2)$. We set

$$p_0^{-1}(x_j)=(X^{(j)}, \lambda^{(j)}) \qquad (j=1, 2)$$

where $X^{(j)}$ are abelian threefolds with principal polarization $\lambda^{(j)}$. Since $a(X^{(j)})=1$ $(j=1, 2)$, by Lemma 4.4, we have the unique ppftq of $(X^{(j)}, \mu^{(j)})$:

$$(E^3, \mu^{(j)})\longrightarrow(Y_1^{(j)}, \mu_1^{(j)})\longrightarrow(X^{(j)}, \lambda^{(j)}) \qquad (i=1, 2).$$

Since $g(x_1)=g(x_2)$, by the uniqueness of ppftq, there exists an automorphism θ: $E^3\to E^3$ such that $\mu^{(2)}=\theta^*(\mu^{(1)})$. Since the group Aut (E^3, μ) of automorphisms of E^3 which preserve the polarization μ is a finite group (Matsusaka [12, p. 72, Corollary 1]), the restriction of g to $\mathcal{T}(\mathcal{U}(\mu))^\circ$ is a finite morphism. Hence the morphism g is of finite degree. q.e.d.

Theorem 6.4. *Every irreducible component V′ of the supersingular locus V in* $\mathcal{A}_{3,1}$ *can be obtained as the closure of the image of g as in* (6.2) *with a suitable polarization* μ *on* E^3 *which satisfies Condition* (5.1). *In particular, the dimension of V′ is equal to two.*

Proof. Let $[(X, \lambda)]$ be a point of V' which is not contained in any other component of V. By Oda and Oort [18, Corollary 4.3], we have dim $V'\leqq 2$. By Proposition 5.4, we can construct a ppftq:

$$(E^3, \mu)\longrightarrow(Y, \mu_1)\longrightarrow(X, \lambda).$$

Starting from (E^3, μ), we can construct a family of principally polarized supersingular abelian threefolds over a Zariski open subset $\mathcal{T}(\mathcal{U}(\mu))$ as in (6.1). Then, the closure of the image of g as in (6.1) contains the point $[(X, \lambda)]$. Moreover, since the dimension of $\mathcal{T}(\mathcal{U}(\mu))$ is equal to two, we conclude by the assumption on the point $[(X, \lambda)]$ and Lemma 6.3 that the closure of the image of g coincides with our V', and that the dimension of V' is equal to two. q.e.d.

Theorem 6.5. *Every component V' of V satisfies*

$$a(-/V' \subset \mathscr{A}_{3,1}) = 1.$$

Proof. By Theorem 6.4, we can find a morphism g as in (6.2) such that the closure of the image of g coincides with V'. Since $\mathscr{T}(\mathscr{U}(\mu))^\circ$ is non-empty by Lemma 6.1, the image $g(\mathscr{T}(\mathscr{U}(\mu))^\circ)$ is non-empty. Hence, we have $a(-/V' \subset \mathscr{A}_{3,1}) = 1$. q.e.d.

Theorem 6.6. *There exists a bijective correspondence between the set of irreducible components of the supersingular locus V in $\mathscr{A}_{3,1}$ and the set of isomorphism classes of pairs (E^3, μ) with polarization μ such that* $\operatorname{Ker}\mu = E^3[F^2]$.

Proof. As in the proof of Theorem 6.4, for any irreducible component V' of V, we get (E^3, μ) with a polarization μ such that $\operatorname{Ker}\mu = E^3[F^2]$ and that the closure of the image of g as in (6.2) coincides with V'. Suppose, now, we have two polarizations $\mu^{(j)}$ $(j=1, 2)$ on E^3 with $\operatorname{Ker}\mu^{(j)} = E^3[F^2]$ such that the closures of the images of $\mathscr{T}(\mathscr{U}(\mu^{(j)}))$ $(j=1, 2)$ give the same irreducible component V' of V. Then, as in the proof of Proposition 6.3, we see that $(E^3, \mu^{(1)})$ is isomorphic to $(E^3, \mu^{(2)})$. q.e.d.

Let B be a definite quaternion algebra over the field $\boldsymbol{Q}$ of rational numbers with discriminant p, where p is the characteristic of k. Let U_3 be the positive definite quaternion hermitian space of dimension 3 over B. Then, we have the following theorem.

Theorem 6.7. *The number of irreducible components of the supersingular locus V in $\mathscr{A}_{3,1}$ is equal to the class number $H_3(p, 1)$ of the principal genus of U_3.*

Proof. Let μ be a polarization on E^3 with $\operatorname{Ker}\mu = E^3[F^2]$. Then, by Lemma 4.6, there exists a principal polarization λ on E^3 such that $F^*(\lambda) = \mu$. Conversely, for a principal polarization λ on E^3, we set $\mu = F^*(\lambda)$. Then, μ is a polarization on E^3 with $\operatorname{Ker}\mu = E^3[F^3]$. Moreover, it is clear that $(E^3, \lambda^{(1)})$ with principal polarization $\lambda^{(1)}$ is isomorphic to $(E^3, \lambda^{(2)})$ with principal polarization $\lambda^{(2)}$ if and only if $(E^3, F^*(\lambda^{(1)}))$ is isomorphic to $(E^3, F^*(\lambda^{(2)}))$. Hence, by Theorem 6.6, the number of irreducible components of V is equal to the number of isomorphism classes of principally polarized abelian threefolds (X, λ) such that $X \simeq E^3$. By Ibukiyama, Katsura and Oort [7, Theorem 2.10], the latter number is equal to $H_3(p, 1)$. q.e.d.

Corollary 6.8. The supersingular locus V in $\mathscr{A}_{3,1}$ is reducible if and only if $p \geqq 3$.

Proof. By Hashimoto [5], we have

$$H_3(2, 1)=1, \quad \text{and} \quad H_3(p, 1)>1 \quad \text{if } p\geqq 3.$$

Hence, this corollary follows from Theorem 6.7. q.e.d.

We add here some remarks which are easily proved by our method.

Remark 6.9. a) Considering the images of n-torsion points of $\mathscr{Y}_2$ over $\mathscr{F}(\mathscr{U}(\mu))$ in (5.20) with a positive integer n such that $(p, n)=1$, we get a level n-structure on $(\mathscr{Y}_0, \mu_0)$ over $\mathscr{F}(\mathscr{U}(\mu))$. Therefore, we get a morphism from $\mathscr{F}(\mathscr{U}(\mu))$ to $\mathscr{A}_{3,1,n}$ for each choice of the level n-structure.

b) By a suitable choice of $\mathscr{U}(\mu)$, we may assume that $\mathscr{F}(\mathscr{U}(\mu))^\circ$ is invariant under the natural action of $\mathrm{Aut}(E^3, \mu)$. Then, by a method similar to the proof of Proposition 6.3, we can show

$$\mathscr{F}(\mathscr{U}(\mu))^\circ/\mathrm{Aut}(E^3, \mu)\simeq \mathrm{Im}\, g$$

(see also Oda and Oort [18, Proposition 4.1]).

c) Let $[(X, \lambda)]$ be a point on the intersection of two components of $V\subset\mathscr{A}_{3,1}$. Then, we have $a(X)\geqq 2$.

d) The morphism g in (6.2) is not necessarily a finite morphism. For any point $[\psi]\in\mathscr{U}(\mu)\subset \boldsymbol{P}$, $\psi\colon (\alpha_p)^2\subsetneq E^3$, we set $Z_\psi=E^3/\psi((\alpha_p)^2)$. We have a natural homomorphism

$$i_\psi\colon E^3[F]/\psi((\alpha_p)^2)\simeq \alpha_p\hookrightarrow Z_\psi.$$

Clearly we have

$$Z_\psi/i_\psi(\alpha_p)\simeq E^3/E^3[F]\simeq E^3.$$

By Lemma 4.6, there exists a principal polarization λ on E^3 such that $\mu=F^*(\lambda)$. Then, the point on $\mathscr{T}(\mathscr{U}(\mu))$ which corresponds to (ψ, i_ψ) maps to the point $[(E^3, \lambda)]$ for any point $[\psi]$ of $\mathscr{U}(\mu)$. Thus

$$i(\mathscr{U}(\mu))=\{(\psi, i_\psi)\,|\,[\psi]\in\mathscr{U}(\mu)\}\subset\mathscr{F}(\mu)$$

is a section of $\mathscr{T}(\mathscr{U}(\mu))\to\mathscr{U}(\mu)$ and this section is contracted to the point $[(E^3, \lambda)]$.

Remark 6.10. Let V' be an irreducible component of the supersingular locus V in $\mathscr{A}_{3,d}$. What can be said about $\dim V'$, and about $a(-/V'\subset\mathscr{A}_{3,d})$?

a) If $d=1$, then we have

$$\dim V'=2 \quad \text{and} \quad a(-/V'\subset\mathscr{A}_{3,1})=1,$$

as we have seen in Theorems 6.4 and 6.5.

b) If $d=p^3$, then there exists a component V' with

$$\dim V'=3 \quad \text{and} \quad a(-/V'\subset \mathscr{A}_{3,p^3})=1$$

(cf. Oda and Oort [18, Corollary 3.4]). These are the numbers one could expect.

c) However, it seems difficult to describe the situation in general. We can easily prove:

if $d=p$, then every component $V'\subset \mathscr{A}_{3,p}$ satisfies

$$\dim V'=2 \quad \text{and} \quad a(-/V'\subset \mathscr{A}_{3,p})=2,$$

and

if $d=p^2$, then there exists a component $V'\subset \mathscr{A}_{3,p^2}$ such that

$$\dim V'=3 \quad \text{and} \quad a(-/V'\subset \mathscr{A}_{3,p^2})=1.$$

It seems difficult to guess the general behavior of these invariants for the strata in $\mathscr{A}_{g,d}$ if we stratify by isogeny type (for the case of stratification by p-rank, see Norman and Oort [16, Theorem 4.1]).

References

[1] M. Demazure and P. Gabriel, Groupes algébriques, I, Masson & Cie, Paris; North-Holland Publ. Cy, Amsterdam, 1970.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, **14** (1941), 197–272.

[3] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z., **43** (1938), 102–109.

[4] R. Hartshorne, Algebraic geometry, Grad. Texts Math., No. **52**, Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[5] K. Hashimoto, Class numbers of positive definite ternary quaternion hermitian forms, Proc. J. Acad., **59** (1983), 490–493.

[6] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, J. Fac. Sci. Univ. Tokyo Sect IA, **27** (1980), 549–601; (II) ibid. **28** (1982), 695–699.

[7] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, to appear in Compositio Math.

[8] J. Igusa, Class number of a definite quaternion with prime discriminant, Proc. Nat. Acad. Sci. U.S.A., **44** (1958), 312–314.

[9] ——, Arithmetic variety of moduli for genus two, Ann. of Math., **72** (1960), 612–649.

[10] T. Katsura and F. Oort, Families of supersingular abelian surfaces, to appear in Compositio Math.

[11] S. Lang, Abelian varieties, Interscience-Wiley, New York, 1959.

[12] T. Matsusaka, Polarized varieties, fields of moduli and generalized Kummer varieties of polarized abelian varieties, Amer. J. Math., **80** (1958), 45–82.

[13] L. Moret-Bailly, Familles de courbes et de variétés abéliennes sur P^1, Séminaire sur les pinceaux de courbes de genre au moins deux (L. Szpiro, ed.), Soc. Math. France Astérisque, No **86** (1981), Exp. 7, 109–124 and Exp. 8, 125–140.
[14] D. Mumford, Abelian varieties, Tata Inst. Fund. Research, Oxford Univ. Press, 1970.
[15] D. Mumford and J. Fogarty, Geometric invariant theory, Second enlarged edition, Berlin-Heidelberg-New York, 1982.
[16] P. Norman and F. Oort, Moduli of abelian varieties, Ann. of Math., **112** (1980), 413–439.
[17] T. Oda, The first de Rham cohomology groups and Dieudonné modules, Ann. Sci. Ecole Norm. Sup., 4^e serie, t. **2** (1969), 63–135.
[18] T. Oda and F. Oort, Supersingular abelian varieties, in Proc. Intern. Symp. on Algebraic Geometry, Kyoto, 1977 (M. Nagata, ed.), Kinokuniya Tokyo 1978, 595–621.
[19] F. Oort, Commutative group schemes, Lect. Notes in Math., **15**, Berlin-Heidelberg-New York, Springer-Verlag, 1966.
[20] ——, Subvarieties of moduli spaces, Invent. Math., **24** (1974), 95–119.
[21] ——, Which abelian surfaces are products of elliptic curves?, Math. Ann., **214** (1975), 35–47.
[22] J.-P. Serre, Nombres de points des courbes algébriques sur F_q, Séminaire de Théorie des Nombres (Bordeaux), Année 1982–1983, exposé n°22.
[23] T. Shioda, Supersingular $K3$ surfaces, in Algebraic Geometry, Proc. Copenhagen 1978 (K. Lønsted, ed.), Lect. Notes in Math., **732**, Berlin-Heidelberg-New York, Springer-Verlag (1979), 564–591.
[24] A. Weil, Zum Beweis des Torellischen Satzs, Nachr. Akad. Wiss. Göttingen Math. Phys. Kl (1957), 33–53.

T. Katsura
Department of Mathematics
Yokohama City University
Yokohama, 236
Japan

F. Oort
Mathematical Institute
State University of Utrecht
Budapestlaan 6
3508 TA Utrecht
The Netherlands