TOSHIYUKI KATSURA
FRANS OORT

# Families of supersingular abelian surfaces

*Compositio Mathematica*, tome 62, n° 2 (1987), p. 107-167
<http://www.numdam.org/item?id=CM_1987__62_2_107_0>

Compositio Mathematica 62: 107–167 (1987)



# Families of supersingular abelian surfaces

TOSHIYUKI KATSURA[1] & FRANS OORT[2]
[1]*Department of Mathematics, Yokohama City University, Yokohama, 236 Japan;*
[2]*Mathematical Institute, State University of Utrecht, Budapestlaan 6, 3508 TA Utrecht, The Netherlands*

Received 6 December 1985; accepted 1 October 1986

*Dedicated to Professor Masayoshi Nagata on his 60th birthday*

## Table of contents



## Introduction

Let $k$ be an algebraically closed field of characteristic $p > 0$. Let $\mathscr{A}_{2,1}$ be the coarse moduli scheme of principally polarized abelian surfaces over $k$. We study the set

$$V \subset \mathscr{A}_{2,1}$$

of principally polarized supersingular abelian surfaces over $k$. This paper is a continuation of the previous one by T. Ibukiyama, T. Katsura and F. Oort (cf. [5], which will be referred to as [IKO]).

The main point of this paper is to make explicit, and to exploit the methods of Oort [15] and of Moret-Bailly [11] for constructing families of (principally polarized) supersingular abelian surfaces over the projective line $\mathbf{P}^1$. We show that any component of the supersingular locus $V$ of $\mathscr{A}_{2,1}$ is the image of such a family (cf. Corollary 2.2). Furthermore, it follows that for any irreducible component $W$ of $V$ this construction determines a group $G \subset \mathrm{Aut}(\mathbf{P}^1)$ such that

$$\mathbf{P}^1 \to \mathbf{P}^1/G \simeq \tilde{W} \to W \subset V \subset \mathscr{A}_{2,1},$$

where $\tilde{W}$ is the normalization of $W$ (cf. Section 4). For $p \geqslant 3$ the group $G$ is a subgroup of the symmetric group $S_6$ of degree six (cf. Corollary 4.4). This enables us to relate the number of irreducible components of $V$ with a certain class number (cf. Theorem 5.7), and using a computation by K. Hashimoto and T. Ibukiyama (cf. [4], and see also Katsura and Oort [8]), we conclude that

$V$ is irreducible if and only if $p \leqslant 11$.

In Section 6, we compute the number of automorphisms of abelian surfaces when the polarization consists of the join of two supersingular elliptic curves. This information and methods of Igusa [7] and of [IKO] enable us to determine all ramification groups which appear in the morphisms

$$\mathbf{P}^1 \to \mathbf{P}^1/G \simeq \tilde{W}$$

(cf. Section 7). In this way we obtain a second proof for the (ir)reducibility of $V$, but in this way by purely geometric methods. We conclude by determining the groups $G$ which appear for small characteristics.

It seems that the structure of the supersingular locus $V$ of $\mathscr{A}_{2,1}$ has been described rather precisely in this way. We come back to this question for dimension three in our paper [8].

We like to thank Professors K. Ueno, T. Ibukiyama and K. Hashimoto for valuable conversations. The first author would like to thank Z.W.O. and organizers of the moduli project for giving him the opportunity to visit Utrecht. He also thanks the Mathematical Institute, University of Utrecht for warm hospitality and excellent working conditions. The second author thanks his Japanese colleagues and friends, the Japanese Society for the Promotion of Science (JSPS), and Kyoto University for warm hospitality, support, and excelent working conditions.

## §1. Preliminaries and construction of families

In this section, we fix notations and prove some easy lemmas which we need later. Then, we give a survey of the construction of families of supersingular abelian surfaces (cf. Oort [15]) and resume the properties of these families by virtue of Moret-Bailly [11].

Let $k$ be an algebraically closed field of characteristic $p > 0$, and let $X$, $Y$ be non-singular complete algebraic varieties over $k$. We denote by $k(X)$ the rational function field of $X$. For two Cartier divisors $D_1$ and $D_2$ on $X$, $D_1 \sim D_2$ (resp. $D_1 \equiv D_2$) means that $D_1$ is linearly equivalent (resp. algebraically equivalent) to $D_2$. We denote by $id_X$ the identity mapping from $X$ to $X$. For a morphism $f$ from $X$ to $Y$, we denote by $\deg f$ the degree of $f$. We mean by a curve a non-singular complete irreducible curve over $k$, unless otherwise mentioned. By the curve defined by an equation $f(x, y) = 0$ we mean the non-singular complete model of the curve defined by the equation $f(x, y) = 0$. For a curve $\tilde{C}$, we denote by $\tilde{C}^{(p)}$ the image of the Frobenius morphism of $\tilde{C}$. Conversely, for a curve $C = \tilde{C}^{(p)}$, we denote $\tilde{C}$ by $C^{(1/p)}$.

For an abelian variety $A$ over $k$ we denote by End $(A)$ the ring of endomorphisms of $A$. We denote by $\mathrm{Aut}_v(A)$ (resp. Aut $(A)$) the group of automorphisms of $A$ as a variety (resp. as an abelian variety). We have the natural exact sequence

$$0 \longrightarrow A \longrightarrow \mathrm{Aut}_v(A) \xrightarrow{\gamma} \mathrm{Aut}\,(A) \longrightarrow 0. \tag{1.1}$$

For an effective divisor $\Theta$ on $A$ we denote by $\mathrm{Aut}_v(A, \Theta)$ (resp. Aut $(A, \Theta)$) the subgroup of $\mathrm{Aut}_v(A)$ (resp. Aut$(A)$) whose elements induce automorphisms of the subscheme $\Theta$ (resp. whose elements $\theta$ preserve the polarization $\Theta$, i.e., $\theta^*(\Theta) \equiv \Theta$). For a group $G$ and elements $g_i$ ($i = 1, 2, \cdots, n$ with a positive integer $n$) of $G$, we denote by $\langle g_1, \cdots, g_n\rangle$ the subgroup of $G$ generated by $g_i$'s ($i = 1, 2, \cdots, n$). We denote by $|G|$ the order of $G$. We denote by $\iota$ the inversion of $A$. We set for an effective divisor $\Theta$ with $\iota^*(\Theta) = \Theta$

$$RA_v(A, \Theta) = \mathrm{Aut}_v(A, \Theta)/\langle\iota\rangle \quad \text{and} \quad RA(A, \Theta) = \mathrm{Aut}\,(A, \Theta)/\langle\iota\rangle.$$

The group $RA(A, \Theta)$ is called a reduced group of automorphisms of a polarized abelian variety $(A, \Theta)$.

Now, let $A$ be an abelian surface, and let $\Theta$ be a principal polarization on $A$. Then, $\Theta$ is given by a (not necessarily irreducible) curve of genus two, and $(A, \Theta)$ is isomorphic to the (generalized) Jacobian variety $(J(\Theta), \Theta)$. By Weil [21, Satz 2], we have two possibilities for $\Theta$:

(i) $\Theta$ is a non-singular complete curve of genus two,

(ii) $\Theta$ consists of two elliptic curves $E'$ and $E''$ which intersect transversally at a point.

In both cases, we have the isomorphism

$$\mathrm{Aut}_v(A, \Theta) \simeq \mathrm{Aut}\,(A, \Theta) \tag{1.2}$$

induced by $\gamma$ in (1.1). A smooth curve of genus two is a two-sheeted covering of the projective line $\mathbf{P}^1$. For such a curve $C$ we denote again by $\iota$ the generator of the Galois group of the algebraic extension $k(C)/k(\mathbf{P}^1)$. For a reducible curve $C = E' \cup E''$ as in (ii) we denote by $\iota$ the automorphism of $C$ which induces inversions of $E'$ and $E''$. In these cases, we denote by Aut $(C)$ the group of automorphisms of $C$, and we set

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

The group $RA(C)$ is called a reduced group of automorphisms of a (not necessarily irreducible) curve $C$ of genus two. The inversion $\iota$ of $C$ induces the inversion of the (generalized) Jacobian variety $J(C)$. Then, by (1.2) we have

$$\begin{gathered} \mathrm{Aut}\,(C) \simeq \mathrm{Aut}_v(J(C), C) \simeq \mathrm{Aut}\,(J(C), C) \\ \text{and} \\ RA(C) \simeq RA(J(C), C). \end{gathered} \tag{1.3}$$

We denote by $\mathbf{F}_{p^i}$ the finite field with $p^i$ elements. Throughout this paper, we fix a supersingular elliptic curve $E$ over $k$ such that

$$E \text{ is defined over } \mathbf{F}_p \text{ and End } (E) \text{ is defined over } \mathbf{F}_{p^2}. \tag{1.4}$$

For the existence of such a supersingular elliptic curve, see Waterhouse [20, Theorem 4.1.5].

For an abelian variety $A$, we denote by $A^t$ the dual of $A$. For an invertible sheaf (or a divisor) $L$ on $A$, we have the morphism $\varphi_L \colon A \to A^t$ defined by $x \mapsto T_x^*L \otimes L^{-1}$, where $T_x$ is the translation by an element $x$ of $A$. We set

$$K(L) = \mathrm{Ker}\ \varphi_L.$$

For abelian varieties $A$, $B$ and a homomorphism $f\colon B \to A$, we have the following commutative diagram:

$$\begin{array}{ccc} B & \xrightarrow{f} & A \\ {\scriptstyle \varphi_{f^*L}}\downarrow & & \downarrow{\scriptstyle \varphi_L} \\ B^t & \xleftarrow{f^t} & A^t \end{array}, \tag{1.5}$$

where $f^t$ is the dual homomorphism of $f$. For a product of $n$ supersingular elliptic curves, we have the following remarkable results.

THEOREM 1.1 (Deligne). *For any supersingular elliptic curves* $E_j$ $(j = 1, 2, \cdots, 2n$ with $n \geqslant 2)$, *the abelian variety* $E_1 \times \cdots \times E_n$ *is isomorphic to* $E_{n+1} \times \cdots \times E_{2n}$.

For the proof, see Shioda [19, Theorem 3.5].

We denote by $\alpha_p$ the local–local group scheme

$$\alpha_p = \operatorname{Spec} k[\alpha]/(\alpha^p)$$

of rank $p$ with a co-multiplication $\alpha \mapsto \alpha \otimes 1 + 1 \otimes \alpha$.

THEOREM 1.2 (Oort). *Let* $E'$ *be a supersingular elliptic curve. Then, any supersingular abelian surface* $A$ *is isomorphic to* $(E' \times E')/i(\alpha_p)$ *with a suitable immersion* $i\colon \alpha_p \hookrightarrow E' \times E'$.

This follows from Theorem 1.1 and Oort [16, Corollary 7]. The proofs of the following lemmas are obvious (for Lemma 1.3, use Oort [16, Theorem 2]).

LEMMA 1.3. *Let* $A = E_1 \times E_2$ *be an abelian surface with supersingular elliptic curves* $E_1$ *and* $E_2$. *Let* $i\colon \alpha_p \hookrightarrow A$ *be an immersion such that* $B = A/i(\alpha_p)$ *is not isomorphic to a product of two elliptic curves. Then, the subgroup scheme which is isomorphic to* $\alpha_p$ *is unique in* $B$. *Moreover, the natural mapping* $A \to B \to B/\alpha_p$ *is nothing but the Frobenius morphism* $F_A$.

LEMMA 1.4. *Let* $A = E_1 \times E_2$ *be an abelian surface with supersingular elliptic curves* $E_1$ *and* $E_2$. *Let* $i\colon \alpha_\varrho \hookrightarrow A$ *be an arbitrary immersion. Set* $B = A/i(\alpha_p)$ *and let* $\pi_0\colon A \to B$ *be the natural projection. Set* $N = \pi_0(\alpha_p \times \alpha_p)$. *If an automorphism* $\theta$ *of* $B$ *induces an automorphism of* $N$, *then* $\theta$ *lifts to a unique automorphism* $\tilde{\theta}$ *of* $A$ *such that the following diagram commutes:*

$$\begin{array}{ccc} A & \xrightarrow{\tilde{\theta}} & A \\ {\scriptstyle \pi_0}\downarrow & & \downarrow{\scriptstyle \pi_0} \\ B & \xrightarrow{\theta} & B \end{array} \tag{1.6}$$

*Moreover, the order of* $\theta$ *is equal to the order of* $\tilde{\theta}$.

LEMMA 1.5. *Under the same notations as in Lemma 1.4, assume that* $B$ *is not isomorphic to a product of two elliptic curves. Then, any automorphism* $\theta$ *of* $B$ *lifts to an automorphism* $\tilde{\theta}$ *of* $A$ *such that the diagram* (1.6) *commutes.*

*Proof.* By the uniqueness of a subgroup scheme $\alpha_p$ in $B$, the automorphism $\theta$ induces an automorphism of $N$ in Lemma 1.4. Therefore, this corollary follows from Lemma 1.4. Q.E.D.

Now, we give a survey of the construction of families of supersingular abelian surfaces by virtue of Moret-Bailly [11]. We assume char $k = p \geqslant 3$. Let $E_1$ and $E_2$ be supersingular elliptic curves. We set $A = E_1 \times E_2$. We have the natural immersion

$$\alpha_p \times \alpha_p \hookrightarrow A = E_1 \times E_2. \tag{1.7}$$

We denote by $T_A$ the tangent space of $A$ at the origin, and by $S$ the projective line $\mathbf{P}(T_A)$ obtained from $T_A$. We set

$$\begin{aligned} K_S &= \alpha_p \times \alpha_p \times S \simeq \operatorname{Spec} k[\alpha]/(\alpha^p) \times \operatorname{Spec} k[\beta]/(\beta^p) \times S, \\ A_S &= E_1 \times E_2 \times S. \end{aligned} \tag{1.8}$$

We consider a subgroup scheme $H$ of $K_S = \operatorname{Spec} \mathcal{O}_S[\alpha, \beta]/(\alpha^p, \beta^p)$ defined by the equation $Y\alpha - X\beta = 0$, where $(X, Y)$ is a homogeneous coordinate of $S$. We set $\mathscr{X} = A_S/H$. Then, we have the following diagram:

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "\Delta"] & A_S \arrow[r, "\pi"] \arrow[dl, "pr_1"'] \arrow[dr, "pr_2"] & \mathscr{X} \arrow[r] \arrow[d, "q"] & 1 \text{ (exact)}, \\ & A & & S \simeq \mathbf{P}^1 & \end{tikzcd} \tag{1.9}$$

where $\Delta$ is the natural immersion, $\pi$ is the canonical projection, $pr_1$ and $pr_2$ are projections, and $q$ is the induced morphism. Using Moret-Bailly [11, p. 138–p. 139] and the fact that $p \geqq 3$, we see that there exists an invertible sheaf $L$ (resp. a divisor) on $A$ such that

$$\begin{aligned} &\text{(i) } L \text{ is symmetric, i.e., } \iota^*L \simeq L \text{ (resp. } \iota^*L = L\text{), and} \\ &\text{(ii) } K(L) \simeq \alpha_p \times \alpha_p. \end{aligned} \tag{1.10}$$

Then, there exists an invertible sheaf $M$ on $\mathscr{X}$ such that $\pi^*(M) = pr_1^*(L)$ (cf. Moret-Bailly [11, p. 130]). Using this $M$, we can construct an effective divisor $D$ on $\mathscr{X}$ over $S$ such that

$$\mathcal{O}_{\mathscr{X}}(D) \simeq M \otimes q^*\mathcal{O}_S((p-1)/2). \tag{1.11}$$

We can show that $D$ is a non-singular surface. Setting $D' = \pi^{-1}(D)$, we have

$$\mathcal{O}_{A_S}(D') \simeq pr_1^*(L) \otimes pr_2^*\mathcal{O}_S((p-1)/2). \tag{1.12}$$

For a point $x$ of $S$, we set

$$\mathscr{X}_x = q^{-1}(x),\ D_x = D \cap q^{-1}(x),\ (A_S)_x = pr_2^{-1}(x) \text{ and } H_x = \Delta^{-1}pr_2^{-1}(x).$$

We denote by $\Delta_x$ (resp. $\pi_x$) the homomorphism from $H_x$ to $(A_S)_x$ (resp. from $(A_S)_x$ to $\mathscr{X}_x$) induced by $\Delta$ (resp. $\pi$). We have $D_x^2 = 2$, hence, $D_x$ gives a principal polarization on $\mathscr{X}_x$. Therefore, $D_x$ is either a non-singular curve of genus two or a reducible curve composed of two elliptic curves which intersect transversally at a point. Thus, $q$: $\mathscr{X} \to S$ with $D$ is a family of principally polarized supersingular abelian surfaces. The number of degenerate fibers of $q|_D$: $D \to S$ is given by

$$5p - 5. \tag{1.13}$$

For the details of these facts, see Moret-Bailly [11].

*Remark 1.6*. In case char $k = 2$, we have also a similar family of principally polarized supersingular abelian surfaces to the one in (1.9) by another method (see Moret-Bailly [10]).

## §2. The locus of supersingular abelian surfaces

In this section, we assume char $k = p \geqslant 3$. Let $X$ be a finite union of varieties on which a finite group $G$ acts faithfully. Then, we call $X$ a Galois covering of $X/G$ with Galois group $G$. Let $\mathscr{A}_{2,1}$ (resp. $\mathscr{A}_{2,1,n}$, $(n, p) = 1$) defined over $k$. We have a Galois covering

$$\varphi_n\colon \mathscr{A}_{2,1,n} \to \mathscr{A}_{2,1}. \tag{2.1}$$

The Galois group is isomorphic to $PSp(4, \mathbf{Z}/n) = Sp(4, \mathbf{Z}/n)/\langle \pm 1 \rangle$ (cf. Mumford and Fogarty [13, p. 190]). In particular, in case $n = 2$, the Galois group is isomorphic to the symmetric group $S_6$ of degree six. We set $\varphi = \varphi_2$. As is well-known, the scheme $\mathscr{A}_{2,1,n}$ is a fine moduli scheme for $n \geqslant 3$ (cf. Mumford and Fogarty [13, p. 139]). We denote by $V$ (resp. $V_n$) the locus of supersingular abelian surfaces in $\mathscr{A}_{2,1}$ (resp. $\mathscr{A}_{2,1,n}$). Every component of $V$ and of $V_n$ is a rational curve (cf. Oort [15, p. 177]).

We consider an abelian surface $A = E_1 \times E_2$ with supersingular elliptic curves $E_1$ and $E_2$. Let $L$ be a polarization on $A$ which satisfies Condition (1.10). Then, as in Section 1, we get a family of principally polarized supersingular abelian surfaces $q: \mathscr{X} \to S$. This family is an abelian scheme. We consider a subscheme $\mathscr{X}[n] = \operatorname{Ker}[n]_{\mathscr{X}}$ over $S$, where $[n]_{\mathscr{X}}$ is the multiplication by an integer $n$ in $\mathscr{X}$. If $n$ is not divisible by $p$, then $q|_{\mathscr{X}[n]}$: $\mathscr{X}[n] \to S \simeq \mathbf{P}^1$ is an étale covering. Since $\mathbf{P}^1$ is simply connected, $\mathscr{X}[n]$ becomes a disjoint union of sections. Therefore, for the family $q: \mathscr{X} \to S$, we can put a level $n$-structure with a positive integer $n$ which is not divisible by $p$. Using this structure, we get a morphism

$$\psi_n: S \to \mathscr{A}_{2,1,n} \text{ (resp. } \psi = \psi_1: S \to \mathscr{A}_{2,1}). \tag{2.2}$$

Since the family $q: \mathscr{X} \to S$ is not a trivial family (cf. Oort [15] and Moret-Bailly [11, p. 131]), the image of this morphism gives a component of $V_n$ (resp. $V$). Conversely, we have the following theorem (see also Ekedahl [3, III, Theorem 1.1]).

THEOREM 2.1. *Any component of $V_n$ ($n \geqslant 2$, $(n, p) = 1$) can be obtained by the method in* (2.2) *with a suitable level n-structure and a polarization D as in* (1.11) *obtained from a suitable divisor L which satisfies Condition* (1.10). *Moreover, as L, we can take an effective divisor composed of two elliptic curves.*

*Proof.* Let $W$ be an irreducible component of $V_n$, $x$ a general point of $W$, and $(A_x, C_x, \eta_x)$ the principally polarized supersingular abelian surface with polarization $C_x$ and level $n$-structure $\eta_x$ which corresponds to the point $x$. By the generality of $x$, we see that $W$ is only one irreducible component of $V_n$ on which the point $x$ lies. Since the number of points in $\mathscr{A}_{2,1,n}$ which correspond to a product of two supersingular elliptic curves are finite (cf. Narasimhan and Nori [14], and also see [IKO, Theorem 2.10]), the abelian surface $A_x$ is not isomorphic to a product of two supersingular elliptic curves. Therefore, there exists in $A_x$ the unique subgroup scheme which is isomorphic to $\alpha_p$ (cf. Oort [16, Theorem 2]). We have the following diagram:

$$\begin{array}{ccc} A_x & \xrightarrow{\pi_x} & A_x/\alpha_p \\ {\scriptstyle \varphi_{C_x}} \downarrow & & \\ (A_x)^t & \xleftarrow{\pi_x^t} & (A_x/\alpha_p)^t, \end{array} \tag{2.3}$$

where $\pi_x$ is the canonical projection. We set $\varphi_{C_x}(C_x) = C$. Since $\varphi_{C_x}$ is an isomorphism, the divisor $C$ gives a principal polarization on $(A_x)^t$. It is clear that $A_x/\alpha_p$ and $(A_x/\alpha_p)^t$ are isomorphic to a product of two supersingular eliptic curves, and that $\pi_x \circ \varphi_C \circ \pi_x^t$ is nothing but the Frobenius morphism (see Lemma 1.3). We set $A = (A_x/\alpha_p)^t$ and $L = (\pi_x^t)^{-1}(C)$. We can assume that $C_x$ is symmetric. Then, the divisor $C$ and $L$ are also symmetric. Moreover, denoting by $F_A$ the Frobenius morphism of $A$, we have

$$K(L) \;=\; \operatorname{Ker} \varphi_L \;=\; \operatorname{Ker} \pi_x \circ \varphi_C \circ \pi_x^t \simeq \operatorname{Ker} F_A \simeq \alpha_p \times \alpha_p.$$

Therefore, the divisor $L$ satisfies Condition (1.10). Using this $L$ on $A$, we can construct a family $q\colon \mathscr{X} \to \mathbf{P}^1$ as in (1.9). By our construction, one of the fibres of this family is isomorphic to $(A_x, C_x) = (A, C)$. Now, we can choose the level $n$-structure of the family which coincides with $\eta_x$ at $(A_x, C_x)$. Then, the image of the morphism of $\psi_n$ which is obtained by this family as in (2.2) passes through the point $x$. By the uniqueness of the irreducible component of $V_n$ which passes through $x$, this image coincides with $W$. Hence, the former part of this theorem was proved.

Next, let $q\colon \mathscr{X} \to S$ be a family in (1.9), and let $D$ be a relative polarization on $\mathscr{X}$ obtained by the divisor $L$ on $A$ which satisfies Condition (1.10). By (1.13), the family $q|_D\colon D \to S$ has $5p - 5$ degenerate fibres. Each degenerate fibre consists of two elliptic curves which intersect each other transversally at a point. Let $C' = E' + E''$ be one of these fibres with elliptic curves $E'$ and $E''$. Then, using the notations in (1.9), we see that $\pi^{-1}(C')$ is linearly equivalent to $L$ as divisors on $A$ by (1.12). Therefore, to construct the family $q\colon \mathscr{X} \to S$, we can use $\pi^{-1}(C') = \pi^{-1}(E') + \pi^{-1}(E'')$ instead of $L$. Q.E.D.

COROLLARY 2.2. *Any component of $V$ can be obtained by the method in* (2.2) *with a polarization $D$ in* (1.11) *obtained from a suitable $L$ which satisfies Condition* (1.10). *Moreover, as $L$, we can choose an effective divisor composed of two elliptic curves.*

*Proof.* This follows from Theorem 2.1 and (2.1). Q.E.D.

THEOREM 2.3. (i) *For any point $x$ of $S$, the tangent mapping $(\mathrm{d}\psi_n)_x$ is injective for $n \geqslant 3$. In particular, every branch of the image of $\psi_n$ is non-singular for $n \geqslant 3$.*

(ii) *The morphism $\psi_n$ is generally an immersion for $n \geqslant 3$.*

*Proof.* (i) In this proof, we set $T = \operatorname{Spec}(k[\varepsilon]/(\varepsilon^2))$. Let $t: T \to S$ be a tangent at a point $x$ of $S$. We have the exact sequence

$$1 \longrightarrow H \times_S T \xrightarrow{\Delta'} A \times_k T \xrightarrow{\pi'} \mathscr{X} \times_S T \longrightarrow 1 \tag{2.4}$$

which is induced by (1.9). Suppose $(d\psi_n)_x(t) = 0$. Since $\mathscr{A}_{2,1,n}$ $(n \geqslant 3)$ is a fine moduli scheme, we have the natural homomorphism

$$\varrho: \mathscr{X} \times_S T \to \mathscr{X}_x \times_k T.$$

The morphism $\pi_x \times id_T$ coincides with $\varrho \circ \pi'$ on the closed fiber. Therefore, by the rigidity lemma (cf. Mumford and Fogarty [13, Proposition 6.1]), we have

$$\pi_x \times id_T = \varrho \circ \pi'.$$

This means that we have a factorization of $\Delta'$ such that the following diagram commutes:

$$\begin{tikzcd} \Delta': H \times_S T \arrow[r] \arrow[dr] & \alpha_p \times_k T \arrow[r] \arrow[d] & A \times_k T. \arrow[dl] \\ & T & \end{tikzcd} \tag{2.5}$$

Therefore, we conclude that we have a factorizationof $t$ such that $t$: $T \to \operatorname{Spec} k \to S$. Therefore, we have $t = 0$. Hence, the tangent mapping $(d\psi_n)_x$ is injective for $n \geqslant 3$.

(ii) We set $W = \psi_n(S)$, and denote by $\tilde{W}$ the normalization of $W$. Then, we have the following natural decomposition:

$$\begin{tikzcd} S \arrow[rr, "\psi_n"] \arrow[dr, "\tilde{\psi}_n"'] & & W, \\ & \tilde{W} \arrow[ur, "\Psi"'] & \end{tikzcd}$$

where $\Psi$ is the birational morphism obtained from the normalization of $W$. By (i), the tangent mapping $d\psi_n$ is injective at every point of $S$. Therefore, the mapping $d\tilde{\psi}_n$ is also injective at every point of $S$. Hence, the morphism $\tilde{\psi}_n$ is an étale morphism. Since $S$ is a non-singular rational curve, the curve $\tilde{W}$ is also a non-singular rational curve. Since the rational curve is simply connected, we conclude that $\tilde{\psi}_n$ is an isomorphism. Thus, the morphism $\psi_n$ is generically an immersion. Q.E.D.

The following theorem is due to N. Koblitz. He proved it, using the theory of deformation (see Koblitz [9, p. 193]).

THEOREM 2.4 (Koblitz). *Assume $n \geqslant 3$. Let $\psi_n(x)$ ($x \in S$) be a point which corresponds to a supersingular abelian surface ($A$, $C$, $\eta$) with principal polarization $C$ and level n-structure $\eta$.*

(i) *If $A$ is not isomorphic to a product of two supersingular elliptic curves, then there exists only one component of $V_n$ which passes through $\psi_n(x)$. Moreover, the locus $V_n$ of supersingular abelian surfaces in $\mathscr{A}_{2,1,n}$ is non-singular at $\psi_n(x)$.*

(ii) *If $A$ is isomorphic to a product of two supersingular elliptic curves, then there exist just $p+1$ branches of $V_n$ which passes through $\psi_n(x)$. These branches intersect each other transversally.*

*Remark 2.5.* By a method similar to the proof of Theorem 2.3, we can prove this theorem except the final statement of (ii). We omit details.

*Remark 2.6.* In case char $k = 2$, we can also construct $\psi_n$ with a positive integer $n$ ($n \geqslant 2$, $(n, p) = 1$) and $\psi$ in (2.2), using Remark 1.6, and we can show Theorems 2.1, 2.3, 2.4 and Corollary 2.2 by a similar method.

In Section 4, we treat the case of $\mathscr{A}_{2,1,2}$ (cf. Corollary 5.4).

THEOREM 2.7. *The number of irreducible components of $V$ is equal to the number of isomorphism classes of the families $a$: $\mathscr{X} \rightarrow S$ with relative polarization $D$ given as in* (1.9).

*Proof.* Let $\mathscr{F}$ be the set of representatives of isomorphism classes of the families $q$: $\mathscr{X} \rightarrow S$ with relative principal polarization $D$ given as in (1.9). We denote by $\mathscr{V}$ the set of irreducible components of $V$. By (2.2) we have a mapping

$$\mathscr{G} \rightarrow \mathscr{V}$$

By Theorem 2.1, this mapping is surjective. Let $q_i$: $\mathscr{X}_i \rightarrow S_i$ with relative polarization $D_i$ ($i = 1, 2$) be two families in $\mathscr{F}$ such that the images in $\mathscr{V}$ coincide. Let $x$ be a general point of the corresponding irreducible component of $V$. Then, we can find a point $x_1$ of $S_1$ (resp. $x_2$ of $S_2$) such that $\psi(x_1) = x$ (resp. $\psi(x_2) = x$) by the morphism $\psi$ as in (2.2). We have an isomorphism

$$\theta\colon ((\mathscr{X}_1)_{x_1}, (D_1)_{x_1}) \simeq ((\mathscr{X}_2)_{x_2}, (D_2)_{x_2}).$$

By the generality of $x$, neither $(\mathscr{X}_1)_{x_1}$ nor $(\mathscr{X}_2)_{x_2}$ is isomorphic to a product of two supersingular elliptic curves. Therefore, by Theorem 1.2 and Lemma 1.5, there exists an automorphism $\tilde{\theta}$ of $E \times E$ such that the following diagram commutes:

$$\begin{array}{ccc} E \times E & \xrightarrow{\tilde{\theta}} & E \times E \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ (\mathscr{X}_1)_{x_1} & \xrightarrow{\theta} & (\mathscr{X}_2)_{x_2}, \end{array}$$

where $\pi_1$ and $\pi_2$ are purely inseparable homomorphisms of degree $p$. By our construction, $\tilde{\theta}(\pi_1^{-1}((D_1)_{x_1}))$ is algebraically equivalent to $\pi_2^{-1}((D_2)_{x_2})$. Therefore, by a suitable translation $T_x$ with $x \in E \times E$, $T_x(\tilde{\theta}(\pi_1^{-1}((D_1)_{x_1})))$ is linearly equivalent to $\pi_2^{-1}((D_2)_{x_2})$. Since $\pi_1^{-1}((D_1)_{x_1})$ (resp. $\pi_2^{-1}((D_2)_{x_2})$) satisfies Condition (1.10), the family $q_1\colon \mathscr{X}_1 \to S_1$ (resp. $q_2\colon \mathscr{X}_2 \to S_2$) is reconstructed by the divisor $\pi_1^{-1}((D_1)_{x_1})$ (resp. $\pi_2^{-1}((D_2)_{x_2})$) (cf. the proof of Theorem 2.1). Hence, these two families are isomorphic to each other, that is, the mapping $\mathscr{F} \to \mathscr{V}$ is injective. Q.E.D.

## §3. Standard divisors

Let $k$ be an algebraically closed field of characteristic $p > 0$. Let $E_1$ and $E_2$ be elliptic curves defined over $k$.

*Definition 3.1.* We call an abelian surface $E_1 \times E_2$ with polarization $E_1 + E_2$ a principally polarized abelian surface of degenerate type.

PROPOSITION 3.2. *The number of principally polarized supersingular abelian surfaces of degenerate type is up to isomorphism equal to $h(h + 1)/2$, where $h$ is the number of supersingular elliptic curves.*

*Proof.* This follows easily from Theorem 1.1. For details, see [IKO, Section 3]. Q.E.D.

The number $h$ of supersingular elliptic curves is explicitly given by

$$h = (p - 1)/12 + \left\{1 - \left(\frac{-3}{p}\right)\right\}\Big/3 + \left\{1 - \left(\frac{-4}{p}\right)\right\}\Big/4, \tag{3.1}$$

where $(l/p)$ denotes the Legendre symbol (cf. Deuring [1, p. 266] and Igusa [6]). For an element $a$ of $k$, we have the endomorphism of $\alpha_p = \operatorname{Spec} k[\alpha]/(\alpha^p)$:

$$a\colon \alpha_p \to \alpha_p$$

defined by

$$\begin{array}{ccc} a^*\colon k[\alpha]/(\alpha^p) & \to & k[\alpha]/(\alpha^p). \\ \cup\!\!\!\shortmid & & \cup\!\!\!\shortmid \\ \alpha & \longmapsto & a\alpha \end{array}$$

For two supersingular elliptic curves $E_1$ and $E_2$, we have an immersion

$$(1, a)\colon \alpha_p \hookrightarrow \alpha_p \times \alpha_p \subset E_1 \times E_2. \tag{3.2}$$

By $(1, \infty)$, we mean the immersion defined by $(0, 1)$. Since the image $(\lambda, \lambda a)(\alpha_p)$ with a non-zero element $\lambda$ of $k$ coincides with $(1, a)(\alpha_p)$, we can regard $(1, a)$ as a point on the projective line $S = \mathbf{P}^1$, and we call "$a$" a direction. An element $a$ of $k \cup \{\infty\}$ is called a good direction of $E_1 \times E_2$ if the quotient surface $(E_1 \times E_2)/(1, a)(\alpha_p)$ is isomorphic to a product of two supersingular elliptic curves. By Oort [15, Introduction], we have $p^2 + 1$ good directions for $E_1 \times E_2$. Let $C$ be a (not necessarily irreducible) curve of genus two which gives a symmetric principal polarization on $E_1 \times E_2$. By the same method as in Moret-Bailly [11, p. 139] for the case $E_1 + E_2$, there exists $p + 1$ directions $a$ among good directions such that the divisor $pC$ descends to $(E_1 \times E_2)/(1, a)\alpha_p$ as a divisor $L$ which satisfies Condition (1.10). Such $a$'s are called very good directions of $(E_1 \times E_2, C)$. It is easy to see that in case $C = E_1 + E_2$ neither 0 nor $\infty$ is a very good direction. In case $E_1 = E_2$, good directions are defined by

$$a^{p^2} = a \quad \text{or} \quad a = \infty \tag{3.3}$$

(cf. Oort [16, Introduction]). In case $E_1 = E_2$ and $C = E_1 + E_2$, very good directions are defined by

$$a^{p+1} = -1 \tag{3.4}$$

(cf. Moret-Bailly [11, p. 139]).

An element $\theta$ of $\operatorname{Aut}(E_1 \times E_2)$ acts on the set of directions of $E_1 \times E_2$ (resp. good directions of $E_1 \times E_2$), and if $\theta$ is an element of

Aut $(E_1 \times E_2, C)$, it acts on the set of very good directions of $(E_1 \times E_2, C)$ with symmetric principal polarization $C$ as follows:

if $\theta \circ (1, a) = (b_1, b_2)$ for a direction $a$ with elements $b_1, b_2$ of $k$, then the action of $\theta$ on the set is given by

$$a \mapsto b_2/b_1.$$

We write this action by $\theta(a) = b_2/b_1$. The action of an element $\theta'$ of $\mathrm{Aut}_v(E_1 \times E_2)$ on the set of directions of $E_1 \times E_2$ (resp. good directions of $E_1 \times E_2$, resp. very good directions of $(E_1 \times E_2, C)$ if $\theta' \in \mathrm{Aut}_v(E_1 \times E_2, C)$) is given by the action of $\gamma(\theta')$ (cf. (1.1)). For a very good direction $a$ of $(E_1 \times E_2, C)$, we denote by Aut $(E_1 \times E_2, C, a)$ the subgroup of Aut $(E_1 \times E_2, C)$ whose elements preserve the very good direction $a$. We set

$$RA(E_1 \times E_2, C, a) = \mathrm{Aut}\,(E_1 \times E_2, C, a)/\langle\iota\rangle$$

with the inversion $\iota$ of $E_1 \times E_2$.

Let $E$ be the elliptic curve in (1.4). We set

$$\tilde{A} = E \times E.$$

For an element $a$ of $k$, we consider an immersion

$$(1, a)\colon \alpha_p \hookrightarrow \alpha_p \times \alpha_p \subset E \times E = \tilde{A}. \tag{3.5}$$

Then, by (3.3), an element $a$ is a good direction if and only if $a \in \mathbf{F}_{p_2}$ or $a = \infty$.

LEMMA 3.3. *Under the notations as above, let $a$, $b$ be two good directions. Then, there exists an automorphism $\theta$ of $E \times E$ such that*

$$(1, a) = \theta \circ (1, b). \tag{3.6}$$

*Proof.* We consider the natural restriction

$$r\colon \mathrm{End}\,(E) \to \mathrm{End}\,(\alpha_p). \tag{3.7}$$

Then, by Oort [16, Lemma 5], we have $r(\mathrm{End}\,(E)) = \mathbf{F}_{p^2}$. We denote by id the indentity of End $(E)$. In case $a \neq \infty$ and $b \neq \infty$, we take an element

$u$ of End $(E)$ such that $r(u) = a - b$. Then, we have an automorphism

$$\begin{array}{cccc} \theta\colon E \times E & \longrightarrow & E \times E & \\ \cup\!\!\!\!\!\rule{0pt}{0pt} \ \ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} \mathrm{id} & 0 \\ u & \mathrm{id} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. & \end{array} \tag{3.8}$$

This automorphism satisfies (3.6). In case $a = \infty$ and $b \neq \infty$ (resp. $a \neq \infty$ and $b = \infty$), we take an element $u$ of End $(E)$ such that $r(u) = -b$ (resp. $r(u) = a$). Then, the automorphism

$$\theta = \begin{pmatrix} u & \mathrm{id} \\ \mathrm{id} & 0 \end{pmatrix} \left( \text{resp. } \theta = \begin{pmatrix} 0 & \mathrm{id} \\ \mathrm{id} & u \end{pmatrix} \right)$$

satisfies (3.6). In case $a = \infty$ and $b = \infty$, we can take

$$\theta = \begin{pmatrix} \mathrm{id} & 0 \\ 0 & \mathrm{id} \end{pmatrix}.$$

Q.E.D.

Let $\mathscr{E} = \{E_\lambda\}_{\lambda = 1, 2, \cdots, h}$ (for the definition of $h$, see (3.1)) be a set of representatives of isomorphism classes of supersingular elliptic curves defined over $k$. Using Theorem 1.1, for each pair $(E_m, E_n)$ $(E_m, E_n \in \mathscr{E}, m \leqslant n)$, we fix an isomorphism

$$\kappa_{m,n}\colon E_m \times E_n \xrightarrow{\sim} E \times E = \tilde{A}. \tag{3.9}$$

We also fix a very good direction $a$ of $(E \times E, E \times \{0\} + \{0\} \times E)$, and for each good direction $b$ of $E \times E$, we fix an automorphism $\theta_{a,b}$ which satisfies (3.6). Let $(E_m \times E_n, E_m + E_n, b)$ be a triple with a very good direction $b$ of $(E_m \times E_n, E_m + E_n)$. Then, by the isomorphism in (3.9), we can consider that this triple exists in $E \times E$. Moreover, $\kappa_{m,n}(b)$ becomes one of good directions of $E \times E$. For the sake of simplicity, we write again $(E_m \times E_n, E_m + E_n, b)$ instead of $(\kappa_{m,n}(E_m) \times \kappa_{m,n}(E_n), \kappa_{m,n}(E_m) + \kappa_{m,n}(E_n), \kappa_{m,n}(b))$. Using the automorphism $\theta_{a,b}$, we can turn $E_m \times E_n$ in $E \times E$ so that the very good direction $b$ of $(E_m \times E_n, E_m + E_n)$ may coincide with the direction $a$. By this method, we have $p + 1$ triples $(\theta_{a,b}(E_m) \times \theta_{a,b}(E_n), \theta_{a,b}(E_m) + \theta_{a,b}(E_n), a)$, using $(E_m \times E_n, E_m + E_n)$.

*Definition 3.4*. For supersingular elliptic curves $E_1'$ and $E_2'$ (resp. $E_1''$ and $E_2''$), let $b'$ (resp. $b''$) be a very good direction of $(E_1' \times E_2', E_1' + E_2')$ (resp.

$(E_1'' \times E_2'', E_1'' \times E_2''))$. A triple $(E_1' \times E_2', E_1' + E_2', b')$ is said to be isomorphic to a triple $(E_1'' \times E_2'', E_1'' + E_2'', b'')$ if there exists an isomorphism $\theta$ from $E_1' \times E_2'$ to $E_1'' \times E_2''$ such that $\theta(E_1' + E_2') = E_1'' + E_2''$ and $\theta(b') = b''$.

LEMMA 3.5. *Let $b$, $b'$ be very good directions of $(E_m \times E_n, E_m + E_n)$. The triple $(\tilde{A}, \theta_{a,b}(E_m) + \theta_{a,b}(E_n), a)$ is isomorphic to the triple $(\tilde{A}, \theta_{a,b'}(E_m) + \theta_{a,b'}(E_n), a)$ if and only if $(E_m \times E_n, E_m + E_n, b)$ is isomorphic to $(E_m \times E_n, E_m + E_n, b')$.*

*Proof.* Obvious.

We consider the set of divisors $\theta_{a,b}(E_m) + \theta_{a,b}(E_n)$, where $b$ runs through very good directions of $(E_m \times E_n, E_m + E_n)$. We say that $\theta_{a,b}(E_m) + \theta_{a,b}(E_n)$ is isomorphic to $\theta_{a,b'}(E_m) + \theta_{a,b'}(E_n)$ if there exists an element $\theta$ of $\mathrm{Aut}\,(E_m \times E_n, E_m + E_n)$ such that $\theta_{a,b'}(E_m) + \theta_{a,b'}(E_n) = \theta(\theta_{a,b}(E_m) + \theta_{a,b}(E_n))$. We denote by $\tilde{\mathscr{D}}(E_m, E_n)$ the set of representatives of isomorphism classes of divisors $\theta_{a,b}(E_m) + \theta_{a,b}(E_n)$ with very good directions $b$ of $(E_m \times E_n, E_m + E_n)$. The number of elements of $\tilde{\mathscr{D}}(E_m, E_n)$ is equal to the number of orbits of $RA(E_m \times E_n, E_m + E_n)$ in $p + 1$ very good directions of $(E_m \times E_n, E_m + E_n)$, which will be calculated in Section 6. We set

$$\tilde{\mathscr{D}} = \bigcup_{1 \leqslant m \leqslant n \leqslant h} \tilde{\mathscr{D}}(E_m, E_n). \tag{3.10}$$

By definition, any two triples $(\tilde{A}, C, a)$ and $(\tilde{A}, C', a)$ with $C, C' \in \tilde{\mathscr{D}}$ and $C \neq C'$ are not isomorphic to each other.

Now, we consider the following mapping:

$$\tilde{\pi}\colon \tilde{A} = E \times E \to (E \times E)/(1, a)(\alpha_p) = A. \tag{3.11}$$

Since $a$ is a very good direction of $E \times E$, the abelian surface $A$ is also isomorphic to $E \times E$. We set

$$\begin{aligned} \mathscr{D}(E_m, E_n) &= \{\tilde{\pi}(C)\colon C = \theta_{a,b}(E_m) + \theta_{a,b}(E_n) \in \tilde{\mathscr{D}}(E_m, E_n)\} \\ \mathscr{D} &= \bigcup_{1 \leqslant m \leqslant n \leqslant h} \mathscr{D}(E_m, E_n). \end{aligned} \tag{3.12}$$

Then, any divisor $L$ in $\mathscr{D}$ consists of two supersingular elliptic curves $E'$ and $E''$, that is, $L = E' + E''$, such that $E' \cap E'$ is equal to the subgroup scheme $\tilde{\pi}(\alpha_p \times \alpha_p) \simeq \alpha_p$ of $A$. All divisors in $\mathscr{D}$ satisfy Condition (1.10).

Moreover, by our choice, there does not exist any element of $\mathrm{Aut}_v(A)$ which transforms a divisor in $\mathscr{D}$ to another divisor in $\mathscr{D}$.

*Definition 3.6.* We call a divisor in $\mathscr{D}$ a standard divisor.

LEMMA 3.7. *Let $L' = E' + E''$ be an effective divisor on $A$ with supersingular elliptic curves $E'$ and $E''$ such that $L'$ satisfies Condition* (1.10). *Then, there exist a unique standard divisor $L$ on $A$ and an element $\theta$ of* $\mathrm{Aut}_v(A)$ *such that $\theta(L) = L'$.*

*Proof.* By Condition (1.10), two elliptic curves $E'$ and $E''$ intersect only at one point. Therefore, by a suitable translation $T_x$ of $A$, we can assume that $E_0' = T_x E'$ and $E_0'' = T_x E''$ intersect at the origin. The divisor $E_0' + E_0''$ also satisfies Condition (1.10). We can find elliptic curves $E_m$ and $E_n$ in $\mathscr{E}$ such that $E_0' \simeq E_m$ and $E_0'' \simeq E_n$. We may assume $m \leqslant n$. Using these isomorphisms, we have an isomorphism

$$\varrho\colon E_m \times E_n \simeq E_0' \times E_0''.$$

Let $\pi'\colon E_0' \times E_0'' \to A$ be the natural homomorphism. We set $\pi'' = \pi' \circ \varrho$. Then, we have the following exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \alpha_p \arrow[r, "i"] & E_m \times E_n \arrow[r, "\pi''"] \arrow[d, "\kappa_{m,n}", "\wr"'] & A \arrow[r] & 0 \text{ (exact)}, \\ & & \tilde{A} = E \times E & & \end{tikzcd} \tag{3.13}$$

where $i$ is an immersion. The immersion $i$ can be written as $i = (1, b)$ with a very good direction $b$ of $(E \times E, \kappa_{m,n}(E_m) + \kappa_{m,n}(E_n))$. We set $C = \theta_{a,b}(\kappa_{m,n}(E_m)) + \theta_{a,b}(\kappa_{m,n}(E_n))$. Then, by the definition of $\tilde{\mathscr{D}}$, there exists an element $\tilde{\theta}$ of $\mathrm{Aut}_v(\tilde{A})$ such that $\tilde{\theta}(C)$ is an element of $\tilde{\mathscr{D}}$. Hence, we have the following diagram:

$$\begin{tikzcd} E_m \times E_n \arrow[r, "\kappa_{m,n}"] \arrow[d, "\pi''"'] & \tilde{A} \arrow[r, "\theta_{a,b}"] & \tilde{A} \arrow[r, "\tilde{\theta}"] & \tilde{A} \arrow[d, "\tilde{\pi}"] \\ A \arrow[rrr, dashed, "\theta'"] & & & A, \end{tikzcd} \tag{3.14}$$

where $\theta'$ is the induces isomorphism. We set $L = \tilde{\pi}(\tilde{\theta}(C))$ and $\theta = T_x^{-1} \circ (\theta')^{-1}$. Then, we see $L \in \mathscr{D}$ and $\theta(L) = L'$. The uniqueness of $L$ follows from the definition of $\mathscr{D}$. Q.E.D.

Using Theorem 2.1, Lemma 3.7 and Remark 2.6, we have the following:

COROLLARY 3.8. *Any component of* $V_n$ $(n \geqslant 2, (n, p) = 1)$ *and of* $V$ *can be obtained by the method in* (2.2) *with a divisor in* $\mathscr{D}$.

## §4. Groups of automorphisms of families

In this section, we assume char $k = p \geqslant 3$, and we use the same notations as in Section 3. As in (1.9) in Section 1, using the abelian surface $A$ in (3.11), we have a family $q\colon \mathscr{X} \to S \simeq \mathbf{P}^1$ of principally polarized supersingular abelian surfaces with relative polarization $D$. We examine the group of automorphisms of this family which preserve the relative polarization $D$. The family $pr_2|_{D'}\colon D' = \pi^{-1}(D) \to S$ has $5p - 5$ reducible fibres. We can consider these reducible fibres as divisors on $A$. By (1.12) they are linearly equivalent to each other and satisfy Condition (1.10). We denote by $\mathscr{B}(\mathscr{X}, D)$ the set of such $5p - 5$ divisors on $A$. For the sake of simplicity, we set $\mathscr{B} = \mathscr{B}(\mathscr{X}, D)$. By Lemma 3.7, for any divisor $L'$ in $\mathscr{B}$ there exist an element $\theta$ of $\mathrm{Aut}_v(A)$ and a standard divisor $L$ of $\mathscr{D}$ such that $\theta(L) = L'$. We set

$$\left\{\begin{array}{rcl} \mathscr{D}(\mathscr{B}) & = & \{L \in \mathscr{D}\colon \text{there exist } L' \in \mathscr{B} \text{ and } \theta \in \mathrm{Aut}_v(A) \\ & & \text{such that } L' = \theta(L)\}, \\ \Gamma(\mathscr{B}) & = & \{\theta \in \mathrm{Aut}_v(A)\colon \text{the automorphism } \theta \text{ induces a} \\ & & \text{permutation of elements of } \mathscr{B}\}, \\ R\Gamma(\mathscr{B}) & = & \Gamma(\mathscr{B})/\langle \iota \rangle, \end{array}\right. \tag{4.1}$$

where $\iota$ is the invertion of $A$. It is clear that $\Gamma(\mathscr{B})$ and $R\Gamma(\mathscr{B})$ are finite groups. Since $\iota$ acts trivially on $\mathscr{B}$, the group $R\Gamma(\mathscr{B})$ acts on $\mathscr{B}$. For an element of $\mathscr{B}$ and an element $x = \theta(L)$ of $\mathscr{D}(\mathscr{B})$ with $\theta \in \mathrm{Aut}_v(A)$, it is easy to see that $R\Gamma(\mathscr{B})_x$ is isomorphic to $R\Gamma(\mathscr{B})_L$. Considering the orbits, we have the following equality:

$$5p - 5 = \sum_{x \in \mathscr{D}(\mathscr{B})} (|R\Gamma(\mathscr{B})|/|R\Gamma(\mathscr{B})_x|), \tag{4.2}$$

where $R\Gamma(\mathscr{B})_x$ denotes the stabilizer of $R\Gamma(\mathscr{B})$ at $x \in \mathscr{D}(\mathscr{B})$. In case $x = \tilde{\pi}(\theta_{a,b}(E_m) + \theta_{a,b}(E_n))$, by Lemma 3.5 we have an isomorphism

$$R\Gamma(\mathscr{B})_x = RA(E_m \times E_n, E_m + E_n, b). \tag{4.3}$$

In Section 6, we will calculate the order of $RA(E_m \times E_n, E_m + E_n, b)$. Using the exact sequence (1.1), we set

$$\Gamma(\mathscr{B})' = \gamma(\Gamma(\mathscr{B})). \tag{4.4}$$

It is easy to see that $\Gamma(\mathscr{B})$ does not contain translations. Therefore, we have

$$\Gamma(\mathscr{B}) \simeq \Gamma(\mathscr{B})'. \tag{4.5}$$

The group $\Gamma(\mathscr{B})'$ acts on the tangent space $T_A$ of $A$ at the origin. By the action, the group $\Gamma(\mathscr{B})'$ acts on $S = \mathbf{P}(T_A)$. Therefore, the group $\Gamma(\mathscr{B})'$ acts on the family $pr_2\colon A_S \to S$. Considering the restriction on the action of $\Gamma(\mathscr{B})'$ on $A_S$ to $\alpha_p \times \alpha_p \times S$, we have an action of $\Gamma(\mathscr{B})'$ on the family $pr_2|_H\colon H \to S$. Hence, we have an action of $\Gamma(\mathscr{B})'$ on the family $q\colon \mathscr{X} \to S$. This action preserves the relative polarization $D$. Conversely, suppose that $\sigma$ is an automorphism of the family $q\colon \mathscr{X} \to S$ which preserves the relative polarization $D$. Let $x$ be a point on $S$ such that $\mathscr{X}_x$ is not isomorphic to a product of two supersingular elliptic curves. Then, we have the isomorphism

$$\sigma_x\colon \mathscr{X}_x \to \mathscr{X}_{\sigma(x)}$$

which is induced by $\sigma$. By Lemma 1.5, we have the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{\tilde{\sigma}_x} & A \\ {\scriptstyle \pi_x}\downarrow & & \downarrow{\scriptstyle \pi_{\sigma(x)}} \\ \mathscr{X}_x & \xrightarrow{\sigma_x} & \mathscr{X}_{\sigma(x)}, \end{array} \tag{4.6}$$

which are obtained from (1.9) with $A = E \times E$ and an automorphism $\tilde{\sigma}_x$ of $A$. By assumption, we have $\sigma_x(D_x) \equiv D_{\sigma(x)}$. Since $\sigma_x(D_x)$ and $D_{\sigma(x)}$ are a principal polarization on $\mathscr{X}_{\sigma(x)}$, the divisor $\sigma_x(D_x)$ is transformed into $D_{\sigma(x)}$ by a suitable translation on $\mathscr{X}_{\sigma(x)}$. Therefore, the divisor $\tilde{\sigma}_x(\pi_x^{-1}(D_x))$ is transformed into $(\pi_{\sigma(x)})^{-1}(D_{\sigma(x)})$ by a suitable translation on $A$. Therefore, the composition of $\tilde{\sigma}_x$ and the translation is an element of $\Gamma(\mathscr{B})$, hence, $\tilde{\sigma}_x$ is an element of $\Gamma(\mathscr{B})'$. Let $\sigma'$ be an automorphism of the family $q\colon \mathscr{X} \to S$ which is induced by $\tilde{\sigma}_x$ as above. We consider the automorphism $\tau = \sigma' \circ \sigma^{-1}$. Then, $\tau$ induces the identity on $\mathscr{X}_x$. Therefore, by the rigidity lemma (cf. Mumford and Fogarty [13, Proposition 6.1]), $\tau$ is the identity on $\mathscr{X}$, that is, $\sigma = \sigma'$. Hence, the group $\Gamma(\mathscr{B})'$ is isomorphic to the group of automorphisms of the family $q\colon \mathscr{X} \to S$ which preserve the relative polarization $D$. By (4.5), we have the following theorem.

THEOREM 4.1. *The group of automorphisms of the family $q\colon \mathscr{X} \to S$ which preserve the relative polarization $D$ is isomorphic to the group $\Gamma(\mathscr{B})$.*

Let $n$ ($n \geqslant 2$) be an integer which is not divisible by $p$. As in Section 2, we choose a level $n$-structure on $q\colon \mathscr{X} \to S$. We denote by $G_n$ the Galois group of the covering $\varphi_n\colon \mathscr{A}_{2,1,n} \to \mathscr{A}_{2,1}$. Let $W_n$ (resp. $W$) be the component of $V_n$ (resp. $V$) which is obtained from the family $q\colon \mathscr{X} \to S$ with polarization $D$ and level $n$-structure as above. We set

$$G(W_n) = \{g \in G_n\colon g(W_n) \subset W_n\}.$$

Since $S$ is birationally equivalent to $W_n$ by Theorem 2.3 (ii), the group $G(W_n)$ acts on $S$. Since the stabilizer of $G(W_n)$ at a general point of $W_n$ is trivial (cf. Ibukiyama, Katsura and Oort [5, Propositions 1.3, 1.13 and Theorem 3.3]), $W_n/G(W_n)$ is birationally equivalent to $W$. Hence, we see that

$$S/G(W_n) \text{ is birationally equivalent to } W. \tag{4.7}$$

THEOREM 4.2. *Under the notations as above, the group $G(W_n)$ is isomorphic to $R\Gamma(\mathscr{B})$ for $n \geqslant 3$.*

*Proof.* Since $\mathscr{A}_{2,1,n}$ ($n \geqslant 3$) is a fine moduli scheme, we have the following cartesian diagram:

$$\begin{array}{ccc} \mathscr{X} & \longrightarrow & U \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle u} \\ S & \longrightarrow & \mathscr{A}_{2,1,n}, \end{array} \tag{4.8}$$

where $u\colon U \to \mathscr{A}_{2,1,n}$ is the universal family of principally polarized abelian surfaces with level $n$-structure. Let $G_U$ be the group of automorphisms of the family $u\colon U \to \mathscr{A}_{2,1,n}$ which preserve the relative polarization, and let $\iota_U$ be the inversion of this family. We denote by $G_{U,W}$ the subgroup of $G_U$ which consists of automorphisms of the family $u|_{u^{-1}(W_n)}\colon u^{-1}(W_n) \to W_n$.

$$G(W_n) \simeq G_{U,W}/\langle \iota_U \rangle.$$

Since $G_{U,W}$ acts on the family $q\colon \mathscr{X} \to S$ by (4.8), we have an injective homomorphism $G_{U,W} \hookrightarrow \Gamma(\mathscr{B})' \simeq \Gamma(\mathscr{B})'$, hence, $G(W_n) \hookrightarrow R\Gamma(\mathscr{B})$. Therefore, we have morphisms

$$S/G(W_n) \to S/R\Gamma(\mathscr{B}) \to W \subset \mathscr{A}_{2,1}.$$

By (4.7), we see that $S/G(W_n)$ is birationally isomorphic to $S/R\Gamma(\mathscr{B})$. Hence, $G(W_n)$ is isomorphic to $R\Gamma(\mathscr{B})$ for $n \geqslant 3$. Q.E.D.

Now, we investigate the level 2-structure.

THEOREM 4.3. *$G(W_2)$ is isomorphic to $R\Gamma(\mathscr{B})$.*

*Proof.* We have a Galois covering

$$\varphi_{2,4}\colon \mathscr{A}_{2,1,4} \to \mathscr{A}_{2,1,2} \tag{4.9}$$

(cf. Mumford and Fogarty [13, p. 140]). By a suitable choice of the level 4-structure, we have the following commutative diagram:

$$\begin{tikzcd} & W_4 \arrow[r] \arrow[d] & \mathscr{A}_{2,1,4} \arrow[d] \\ S \arrow[ur, "\psi_4"] \arrow[r, "\psi_2"] & W_2 \arrow[r] & \mathscr{A}_{2,1,2}, \end{tikzcd} \tag{4.10}$$

where $\psi_2(S) = W_2$ and $\psi_4(S) = W_4$. Corresponding to this diagram, we have the exact sequence of groups

$$1 \to N \to G(W_4) \to G(W_2) \to 1 \tag{4.11}$$

with a normal subgroup $N$ of $G(W_4)$. Let $\sigma$ be an element of $N$ which is not the identity. Since $W_4$ is birationally equivalent to $\mathbf{P}^1$, the automorphism $\sigma$ has a fixed point $x$ on $W_4$. Let $(A', C, \eta)$ be the principally polarized supersingular abelian surface with level 4-structure $\eta$ corresponding to $x$. We may assume that $C$ is a (not necessarily irreducible) curve of genus two and it is symmetric. Then, $\sigma$ induces an element $\sigma'$ of $RA(A', C)$. The group $RA(A', C)$ acts on the set of points of order two of $A'$. Since $\sigma$ is an element of $N$, $\sigma'$ fixes all points of order two of $A'$. Considering the list of automorphisms of curves of genus two in Igusa [7], this is impossible if $C$ is a non-singular irreducible curve of genus two. Therefore, $(A', C)$ and $\sigma'$ are of the following type:

$$\left\{\begin{array}{l} A' = E_1 \times E_2,\ C = E_1 + E_2 \text{ with supersingular elliptic} \\ \qquad \text{curves } E_1 \text{ and } E_2, \\[2ex] \sigma' = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \langle \iota \rangle, \end{array}\right. \tag{4.12}$$

where $-1$ (resp. 1) is the inversion of $E_1$ (resp. the identity of $E_2$). We set

$$\tau' = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

By Theorem 4.2, the automorphism $\sigma$ is induced by an element of $R\Gamma(\mathscr{B})$ with a suitable $\mathscr{B}$ as in (4.1). Therefore, by the construction of the family, there exists an automorphism $\tau$ of $A = E \times E$ with $E$ as in (1.4) such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\pi'} & A' \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau'} \\ A & \xrightarrow{\pi'} & A', \end{array}$$

where $\pi'$ is the morphism induced by the morphism $\pi$ as in (1.9). Here, we have Ker $\pi' \simeq \alpha_p$, and $(\pi')^{-1}(C)$ satisfies Condition (1.10) and $\tau((\pi')^{-1}(C))$ is algebraically equivalent to $(\pi')^{-1}(C)$. On the other hand, the automorphism $\tau'$ fixes two directions which are tangents to $E_1$ and $E_2$, respectively. Therefore, it is easy to see that $K((\pi')^{-1}(C))$ is isomorphic to either Ker $[p]_{E_1}$ or Ker $[p]_{E_2}$ (cf. Lemma 1.4), which is not isomorphic to $\alpha_p \times \alpha_p$. A contradiction. Hence, we have $N = \{1\}$, and $G(W_4) \simeq G(W_2)$. Now, this theorem follows from Theorem 4.1. Q.E.D.

COROLLARY 4.4. *$R\Gamma(\mathscr{B})$ is isomorphic to a subgroup of $S_6$.*

*Proof.* Since $G_2 \simeq PSp(4, \mathbb{Z}/2)$ is isomorphic to $S_6$ and $G(W_2)$ is a subgroup of $G_2$, this corollary follows from Theorem 4.3. Q.E.D.

COROLLARY 4.5. *Under the notations in Section 2, the morphism $\psi_2$ is generically an immersion.*

*Proof.* Since $G(W_2)$ is isomorphic to $G(W_4)$ as above, this corollary follows from Theorem 2.3 (ii). Q.E.D.

*Remark 4.6.* Considering the family commented in Remark 1.6, we see that Theorem 4.1 also holds in case $p = 2$, and that $S/\Gamma(\mathscr{B})$ is the normalization of $V$. We omit the details.

## §5. The number of irreducible components of $V_n$ and of $V$

Let $k$ be an algebraically closed field of characteristic $p \geqslant 3$, unless otherwise mentioned. Let

$$\mathscr{F} = \{q_\lambda\colon \mathscr{X}_\lambda \to S \text{ with relative polarization } D_\lambda\}_{\lambda=1,2,\cdots,H'}$$

be the set of representatives of isomorphism classes of the families with relative polarization $D_\lambda$ given as in (1.9). By Theorem 2.7, the number $H'$ is equal to the number of irreducible components of $V$. We set

$$\mathscr{B}_\lambda = \mathscr{B}(\mathscr{X}_\lambda, D_\lambda),\ \mathscr{D}_\lambda = \mathscr{D}(\mathscr{B}_\lambda),\ \Gamma_\lambda = \Gamma(\mathscr{B}_\lambda) \text{ and } R\Gamma_\lambda = R\Gamma(\mathscr{B}_\lambda). \tag{5.1}$$

As in (4.2),

$$5p - 5 = \sum_{x \in \mathscr{D}_\lambda} |R\Gamma_\lambda| / |(R\Gamma_\lambda)_x|. \tag{5.2}$$

We note that $\mathscr{D} = \bigcup_\lambda \mathscr{D}_\lambda$, and that for every $x \in \mathscr{D}$, there exists only one $\lambda$ such that $x \in \mathscr{D}_\lambda$. Therefore, using this correspondence, we have a surjective mapping:

$$\Lambda\colon \mathscr{D} \to \{1, 2, \cdots, H'\}. \tag{5.3}$$

Considering the action of $RA(E_m \times E_n, E_m + E_n)(E_m, E_n \in \mathscr{E}, m \leqslant n)$ on the set of $p + 1$ very good directions of $(E_m \times E_n, E_m + E_n)$, we have

$$p + 1 = \sum_{x \in \mathscr{D}(E_m, E_n)} |RA(E_m \times E_n, E_m + E_n)| / |(R\Gamma_{\Lambda(x)})_x|. \tag{5.4}$$

By the mass formula for supersingular elliptic curves (cf. Deuring [1, Sections 5 and 10]):

$$\sum_{E_m \in \mathscr{E}} 1/|\mathrm{Aut}\,(E_m)| = (p - 1)/24, \tag{5.5}$$

we have

$$\sum_{1 \leqslant m \leqslant n \leqslant h} 1/|RA(E_m \times E_n, E_m + E_n)| = \{(p - 1)/24\}^2 \tag{5.6}$$

(for details, see [IKO, Section 3.1]). We denote by $|V_n|$ the number of irreducible components of $V_n$.

THEOREM 5.1. *Assume* $(n, p) = 1$. *Then,*

$$|V_n| = |PSp(4, \mathbb{Z}/n)|(p^2 - 1)/2880$$

*Proof.* The group $PSp(4, \mathbb{Z}/n)$ acts on the set of irreducible components of $V_n$ (cf. Section 2). Therefore, considering the stabilizer of each component, by Theorem 2.3 (ii) and Corollary 4.5 we have

$$\begin{aligned}
|V_n| &= \sum_{\lambda=1}^{H'} |PSp(4, \mathbb{Z}/n)|/|R\Gamma_\lambda| \quad \text{(by Theorems 4.2 and 4.3)} \\
&= \{|PSp(4, \mathbb{Z}/n)|/(5p - 5)\} \left\{ \sum_{\lambda=1}^{H'} \sum_{x \in \mathscr{D}_\lambda} 1/|(R\Gamma_\lambda)_x| \right\} \quad \text{(by 5.2))} \\
&= \{|PSp(4, \mathbb{Z}/n)|/(5p - 5)\} \left\{ \sum_{x \in \mathscr{D}} 1/|(R\Gamma_{\Lambda(x)})_x| \right\} \\
&= \{|PSp(4, \mathbb{Z}/n)|/(5p - 5)\} \left\{ \sum_{1 \leqslant m \leqslant n \leqslant h} \sum_{x \in \mathscr{D}(E_m, E_n)} 1/|(R\Gamma_{\Lambda(x)})_x| \right\} \\
&= \{|PSp(4, \mathbb{Z}/n)|/(5p - 5)\} \\
&\quad \times \left\{ \sum_{1 \leqslant m \leqslant n \leqslant h} (p + 1)/|RA(E_m \times E_n, E_m + E_n)| \right\} \quad \text{(by 5.4))} \\
&= \{|PSp(4, \mathbb{Z}/n)|(p^2 - 1)\}/2880 \quad \text{(by 5.6)).} \qquad \text{Q.E.D.}
\end{aligned}$$

COROLLARY 5.2. *Let $q$ be an odd prime number different from $p$. Then,*

$$|V_2| = (p^2 - 1)/4 \text{ and } |V_q| = q^4(q^4 - 1)(q^2 - 1)(p^2 - 1)/5760.$$

*Proof.* Since we have $|PSp(4, \mathbb{Z}/2)| = |S_6| = 720$ and $|PSp(4, \mathbb{Z}/q)| = q^4(q^4 - 1)(q^2 - 1)/2$, this corollary follows from Theorem 5.1. Q.E.D.

Let $\mathscr{S}_n$ be the set of points in $V_n$ which correspond to principally polarized supersingular abelian surfaces $(A, C, \eta)$ with principal polarization $C$ and level $n$-structure $\eta$ such that $A$ is isomorphic to a product of two supersingular elliptic curves.

THEOREM 5.3. *Assume* $(n, p) = 1$ *and* $n \geqslant 3$. *Then,*

$$|\mathscr{S}_n| = |PSp(4, \mathbb{Z}/n)|(p-1)(p^2+1)/2880.$$

*Proof.* For an abelian surface $E \times E$ with a supersingular elliptic curve $E$, we have $p^2 + 1$ good directions (see (3.3)). Therefore, by construction, on each family $q_\lambda \colon \mathscr{X}_\lambda \to S$ there exist just $p^2 + 1$ fibres $(\mathscr{X}_\lambda)_x$ which are isomorphic to $E \times E$ (cf. Theorem 1.1). If we consider the set $\mathscr{F}$ of all such families, by Theorems 2.3 (ii) and (2.4) (ii) each $p + 1$ such fibres correspond to the same point in $\mathscr{A}_{2,1,n}$ $(n \geqslant 3)$. Hence, by Theorem 5.1, the number $|\mathscr{S}_n|$ is equal to $\{(p^2+1)|PSp(4, \mathbb{Z}/n)|(p^2-1)/2880\}/(p+1) = |PSp(4, \mathbb{Z}/n)|(p-1)(p^2+1)/2880$. Q.E.D.

By the same way as in the proof of Corollary 5.2, we have the following:

COROLLARY 5.4. *Let* $q$ *be an odd prime number different from* $p$. *Then,*

$$|\mathscr{S}_q| = q^4(q^4-1)(q^2-1)(p-1)(p^2+1)/5760.$$

THEOREM 5.5. *Assume* $p \geqslant 3$. *Then,*

$$|\mathscr{S}_2| = (p-1)(p^2+5p-4)/4.$$

*Proof.* We consider the Galois covering in (4.9). Corresponding to this covering, we have an exact sequence of groups

$$1 \to \tilde{N} \to PSp(4, \mathbb{Z}/4) \to PSp(4, \mathbb{Z}/2) \to 1.$$

The group $\tilde{N}$ acts on $\mathscr{S}_4$, and we have $\mathscr{S}_2 \simeq \mathscr{S}_4/\tilde{N}$. Let $\sigma$ be an element of $\tilde{N}$ such that $\sigma$ has at least one fixed point in $\mathscr{S}_4$. Then, by the same method as in the proof of Theorem 4.2, we see that the fixed point corresponds to a principally polarized abelian surface $(A, C, \eta)$ with level 4-structure $\eta$ such that

$$\begin{cases} A = E_1 \times E_2 \text{ with supersingular elliptic curves } E_1 \text{ and } E_2, \\ C = E_1 + E_2, \text{ and} \\ \sigma \text{ induces either } \sigma' \text{ in (4.12) or the identity of } RA(A). \end{cases} \tag{5.7}$$

Conversely, if $(A, C)$ and $\sigma'$ are given as in (5.7), then $\sigma'$ gives an element $\sigma$ of $\tilde{N}$ which fixes a point in $\mathscr{S}_4$ corresponding to $(A, C, \eta)$ with principal polarization $C$ and any level 4-structure $\eta$. Therefore, by (1.13), (3.3) and Theorem 2.4 (ii), we have

$$\begin{aligned}|\mathscr{S}_2| &= \{(5p-5)|V_4|/(p+1)\}(2/|\tilde{N}|) \\ &\quad + \{\{(p^2+1)-(5p-5)\}|V_4|/(p+1)\}(1/|\tilde{N}|) \\ &= \{(p^2+5p-4)/(p+1)\}\{|V_4|/|\tilde{N}|\}.\end{aligned}$$

Since $|\tilde{N}| = |PSp(4, \mathbb{Z}/4)|/|PSp(4, \mathbb{Z}/2)| = |PSp(4, \mathbb{Z}/4)|/720$, by Theorem 5.1 we have the desired result. Q.E.D.

We now give an algebraic proof of the mass formula in our special case (cf. Eichler [2, Satz 1], see also Hashimoto and Ibukiyama [4, (I), Section 3]).

THEOREM 5.6. (*Eichler*). *The following equality holds*:

$$\sum_{(A,C)} 1/|RA(C)| = (p-1)(p^2+1)/2880, \tag{5.8}$$

*where $(A, C)$ runs through isomorphism classes of principally polarized supersingular abelian surfaces such that $A$ is isomorphic to a product of two supersingular elliptic curves.*

*Proof.* The group $G_3 = PSp(4, \mathbb{Z}/3)$ acts on the set $\mathscr{S}_3$. We denote by $\mathscr{S}_3'$ the set of representatives of orbits. Let $(A, C, \eta)$ be the principally polarized abelian surface with principal polarization $C$ and level 3-structure $\eta$ which corresponds to $x \in \mathscr{S}_3$. Then, the group $RA(C) \simeq RA(A, C)$ is isomorphic to the stabilizer $(G_3)_x$. Considering the orbits of $G_3$ in $\mathscr{S}_3$, by Corollary 5.4 we have

$$9(p-1)(p^2+1) = \sum_{s \in \mathscr{S}_3'} |G_3|/|(G_3)_x|.$$

Since $\mathscr{S}_3'$ corresponds to the set of representatives of isomorphism classes of $(A, C)$, we have the formula (5.8). Q.E.D.

Let $B$ be a definite quaternion algebra over the field $\mathbf{Q}$ of rational numbers with discriminant $p$. We regard $B^2$ as a left vector space over $B$. We denote by $H_2(1, p)$ the class number of the non-principal genus in $B^2$ (for details, see Shimura [18]). This number $H_2(1, p)$ is explicitly calculated in Hashimoto and Ibukiyama [4, (II)] (see also [IKO, Remark 2.17]). To prove the following theorem, Theorem 2.15 in [IKO] plays an important role.

THEOREM 5.7. *Assume* char $k = p > 0$. *The number* $H'$ *of irreducible components of* $V$ *is equal to* $H_2(1, p)$.

*Proof.* For $p = 2$, this follows from Igusa [7] (see also Section 8, (1)). Now, we assume $p \geqslant 3$. Let $E$ be a supersingular elliptic curve as in (1.4). We set $A = E \times E$. Let $a$ be a direction of $A$ such that $A' = (E \times E)/(1, a)(\alpha_p)$ is not isomorphic to a product of two supersingular elliptic curves. We consider the natural projection:

$$\pi: A \to A'.$$

We denote by NS($A$) (resp. NS($A'$)) the Néron–Severi group of $A$ (resp. $A'$). For an element $C'$ of NS($A'$), $C' > 0$ means that the divisor class $C'$ contains an effective divisor. We set

$$\mathscr{P}' = \{C' \in \mathrm{NS}(A'): (C')^2 = 2, C' > 0\}$$

and

$$\mathscr{P} = \pi^{-1}(\mathscr{P}') = \{\pi^{-1}(C'): C' \in \mathscr{P}'\}.$$

We define an equivalent relation $\approx$ on $\mathscr{P}$ as follows:

$$C_1 \approx C_2 (C_1, C_2 \in \mathscr{P}) \text{ if and only if } g^*(C_1) \equiv C_2 \text{ for some } g \text{ of Aut } (A).$$

By Oort [16, Theorem 2], we see that a representative divisor of any element of $\mathscr{P}$ satisfies Condition (1.10). Therefore, by (2.2) we have the natural mapping

$$\Phi: \mathrm{P}/\approx \;\to \{\text{irreducible components of } V\}.$$

By Theorems 1.1 and 1.2, on each irreducible component of $V$ there exists a point which corresponds to the abelian surface $A'$ with a suitable polarization $C'$. Considering the divisor $\pi^{-1}(C')$, we can reconstruct the original irreducible component as in the proof of Theorem 2.1. Therefore, the mapping $\Phi$ is surjective. Suppose that $C_1 = \pi^{-1}(C_1')$ and $C_2 = \pi^{-1}(C_2')$ are two effective divisors of $\mathscr{P}$ such that $\Phi(C_1) = \Phi(C_2)$. Then, by the

construction of the family in (1.9), we can find an effective divisor $L_1'$ of $\mathscr{P}'$ which satisfies the following two properties:
(i) $\pi^{-1}(L_1') = L_1$ is linearly equivalent to $C_1$,
(ii) there exists an element $g'$ of Aut $(A')$ such that $(g')^*(L_1')$ is algebraically equivalent to $C_2'$.
By Lemma 1.5, we can find an element of $g$ of Aut $(A)$ such that $\pi \circ g = g' \circ \pi$. Since $g^*(C_1)$ is linearly equivalent to $g^*(L_1)$ and $g^*(L_1)$ is algebraically equivalent to $C_2$, we conclude that $g^*(C_1)$ is algebraically equivalent to $C_2$. Hence, the mapping $\Phi$ is injective. Since we know that $|\mathscr{P}/\approx|$ is equal to $H_2(1, p)$ (cf. [IKO, Theorem 2.15]), the number of irreducible components of $V$ is equal to $H_2(1, p)$. Q.E.D.

THEOREM 5.8. *Assume* char $k = p > 0$. *The supersingular locus $V$ is irreducible if and only if $p \leqslant 11$.*

*Proof.* This follows from the explicit formula of $H_2(1, p)$ (cf. Hashimoto and Ibukiyama [4, (II)], and see also [IKO, Remark 2.17]). Q.E.D.

*Remark 5.9.* We will write explicitly the number $H_2(1, p)$ for small $p$'s in Table 4 in Section 7 (see also Hashimoto and Ibukiyama [4, (II), p. 698]).

## §6. Groups of automorphisms of principally polarized supersingular abelian surfaces of degenerate type

In this section, we assume char $k = p \geqslant 2$. Let $E_1$ and $E_2$ be two elliptic curves. Then, we have the following two cases:

$$\mathrm{Aut}\,(E_1 \times E_2, E_1 + E_2) \simeq \mathrm{Aut}\,(E_1) \times \mathrm{Aut}\,(E_2) \quad \text{if } E_1 \not\simeq E_2, \tag{6.1}$$

$$1 \to \mathrm{Aut}\,(E_1) \times \mathrm{Aut}\,(E_2) \to \mathrm{Aut}\,(E_1 \times E_2, E_1 + E_2) \to \mathbb{Z}/2 \to 1 \quad \text{(exact)} \quad \text{if } E_1 \simeq E_2. \tag{6.2}$$

Moreover, if $E_1 \simeq E_2$, then we have

$$\mathrm{Aut}\,(E_1 \times E_2, E_1 + E_2) \simeq \langle \mathrm{Aut}\,(E_1) \times \mathrm{Aut}\,(E_2), \sigma\rangle, \tag{6.3}$$

where $\sigma$ is the automorphism of $E_1 \times E_2$ defined by

$$\begin{array}{cccc} \sigma\colon & E_1 \times E_2 & \longrightarrow & E_1 \times E_2. \\ & \cup\!\!\!\!\shortmid & & \cup\!\!\!\!\shortmid \\ & (x, y) & \longrightarrow & (y, x) \end{array} \tag{6.4}$$

Here, we identify $E_1$ with $E_2$ through the isomorphism $E_1 \simeq E_2$. For an elliptic curve $E'$, we denote by $j(E')$ the $j$-invariant of $E'$. In case $p \neq 2, 3$, we denote by $E_\omega$ (resp. $E_i$) the elliptic curve defined by

$$E_\omega\colon Y^2 = X^3 - 1 \text{ (resp. } E_i\colon Y^2 = X^3 - X). \tag{6.5}$$

We have $j(E_\omega) = 0$ (resp. $j(E_i) = 1728$). As is well-known, we have

$$\mathrm{Aut}\,(E_\omega) \simeq \mathbb{Z}/6 \text{ (resp. } \mathrm{Aut}\,(E_i) \simeq \mathbb{Z}/4).$$

The elliptic curve $E_\omega$ (resp. $E_i$) is supersingular if and only if $p \equiv 2 \pmod 3$ (resp. $p \equiv 3 \pmod 4$). In case $p = 2$ (resp. $p = 3$), there exists a unique supersingular elliptic curve (cf. Deuring [1]). We denote by $\xi$ (resp. $\zeta$) a primitive twelfth root of unity (resp. a primitive eighth root of unity). By (3.4), we have the following lemmas.

LEMMA 6.1. *Assume $E_1 \simeq E_2$. Then, $\pm\sqrt{-1}$ are very good directions of $(E_1 \times E_2, E_1 + E_2)$ if and only if $p \equiv 1 \pmod 4$.*

LEMMA 6.2. *Assume $p \equiv 2 \pmod 3$ (resp. $p \equiv 3 \pmod 4$). Then, the elements $\xi, \xi^3, \xi^5, \xi^7, \xi^9, \xi^{11}$ (resp. $\zeta, \zeta^3, \zeta^5, \zeta^7$) are very good directions of $(E_\omega \times E_\omega, E_\omega \times \{0\} + \{0\} \times E_\omega)$ (resp. $(E_i \times E_i, E_i \times \{0\} + \{0\} \times E_i)$) if and only if $p \equiv 5 \pmod{12}$ (resp. $p \equiv 3 \pmod 8$).*

The group $RA(E_1 \times E_2, E_1 + E_2)$ acts on the set of $p + 1$ very good directions of $(E_1 \times E_2, E_1 + E_2)$. For a very good direction $a$ of $(E_1 \times E_2, E_1 + E_2)$, the stabilizer at $a$ is given by $RA(E_1 \times E_2, E_1 + E_2, a)$. Since we know the structure of the group of automorphisms of an elliptic curve (cf. Deuring [1, Section 5]), by (6.1), (6.2) and above lemmas, we have the following list for supersingular elliptic curves $E_1$ and $E_2$.

In Table 1 we set $A = E_1 \times E_2$ and $C = E_1 + E_2$. We denote by $a$ a very good direction of $(A, C)$.

## §7. Automorphisms of families and ramification groups

In this section, we assume char $k = p \geqslant 3$, unless otherwise mentioned. Let $E$ be a supersingular elliptic curve as in (1.4). Throughout this section, $E'$ and $E''$ mean suitable supersingular elliptic curves.

Let $W$ be an irreducible component of $V$ in $\mathscr{A}_{2,1}$. By Corollary 2.2, there exists a family

$$q\colon \mathscr{X} \to S = \mathbf{P}^1 \text{ with a relative polarization } D \tag{7.1}$$

*Table 1.*

Case (I) $E_1 \not\simeq E_2$

| | | $\lvert RA(A, C)\rvert$ | $\lvert RA(A, C, a)\rvert$ | Number of orbits of very good directions | Number of elements in each orbit |
|---|---|---|---|---|---|
| $p \geqslant 5$ | $E_1 \not\simeq E_\omega, E_\iota$<br>$E_2 \not\simeq E_\omega, E_\iota$ | 2 | 1 | $(p+1)/2$ | 2 |
| | $E_1 \not\simeq E_\omega, E_\iota$<br>$E_2 \simeq E_w$<br>$(p \equiv 2 \pmod 3)$ | 6 | 1 | $(p+1)/6$ | 6 |
| | $E_1 \not\simeq E_\omega, E_\iota$<br>$E_2 \simeq E_\iota$<br>$(p \equiv 3 \pmod 4)$ | 4 | 1 | $(p+1)/4$ | 4 |
| | $E_1 \simeq E_\omega$<br>$E_2 \simeq E_\iota$<br>$(p \equiv 11 \pmod{12})$ | 12 | 1 | $(p+1)/12$ | 12 |
| $p = 2$ or 3 | No such cases | | | | |

Case (II) $E_1 \simeq E_2$

| | | | $\lvert RA(A, C)\rvert$ | Very good direction $a$ | $\lvert RA(A, C, a)\rvert$ | Number of orbits of very good directions | Number of elements in each orbit |
|---|---|---|---|---|---|---|---|
| $p \geqslant 5$ | $E_1 \not\simeq E_\omega, E_\iota$ | $p \equiv 1 \pmod 4$ | 4 | $a = \pm\sqrt{-1}$ | 2 | 1 | 2 |
| | | | | $a \neq \pm\sqrt{-1}$ | 1 | $(p-1)/4$ | 4 |
| | | $p \equiv 3 \pmod 4$ | 4 | any | 1 | $(p+1)/4$ | 4 |
| | $E_1 \simeq E_\omega$ | $p \equiv 5 \pmod{12}$ | 36 | $a = \xi, \xi^3, \xi^5, \xi^7, \xi^9, \xi^{11}$ | 6 | 1 | 6 |
| | | | | $a \neq \xi, \xi^3, \xi^5, \xi^7, \xi^9, \xi^{11}$ | 3 | $(p-5)/12$ | 12 |
| | | $p \equiv 11 \pmod{12}$ | 36 | any | 3 | $(p+1)/12$ | 12 |
| | $E_1 \simeq E_\iota$ | $p \equiv 3 \pmod 8$ | 16 | $a = \zeta, \zeta^3, \zeta^5, \zeta^7$ | 4 | 1 | 4 |
| | | | | $a \neq \zeta, \zeta^3, \zeta^5, \zeta^7$ | 2 | $(p-3)/8$ | 8 |
| | | $p \equiv 7 \pmod 8$ | 16 | any | 2 | $(p+1)/8$ | 8 |
| $p = 3$ | $j(E_1) = 0$ | | 144 | any | 36 | 1 | 4 |
| $p = 2$ | $j(E_1) = 0$ | | 576 | any | 192 | 1 | 3 |

as in (1.9) obtained from a standard divisor $L$ on $A = E \times E$ which gives $W$ by the method indicated in (2.2). We use the notations in (4.1). The group $\Gamma(\mathscr{B})$ induces the group of automorphisms of the family (7.1) (cf. Section 4). We set

$$G: = R\Gamma(\mathscr{B}). \tag{7.2}$$

Then, by Proposition 4.1, we have $G \subset \mathrm{Aut}\,(\mathbf{P}^1)$, and the morphism

$$S = \mathbf{P}^1 \xrightarrow{\tilde{\psi}} \mathbf{P}^1/G = \tilde{W} \xrightarrow{\Psi} W \subset \mathscr{A}_{2,1}, \tag{7.3}$$

where $\tilde{\psi}$ is the natural projection, $\Psi$ is the normalization and $\Psi \circ \tilde{\psi}$ is the morphism $\psi = \psi_1$ described in Section 2. Sometimes, we write $\mathrm{Gal}\,(S \to W)$ instead of $G$.

In this section, we study the following questions:
(1) Which groups $G$ can occur?
(2) Which ramification groups I of $G$ occur?
Note that if $p \geqslant 3$, then by Corollary 4.4, for every component $W$ of $V$ the related group $G$ is a subgroup of $PSp(4, \mathbb{Z}/2) \simeq S_6$:

$$G \subset S_6 \tag{7.4}$$

Lemma 7.1. *Let $k$ be a field of characteristic $p \geqslant 0$, and let $S$ be an algebraic curve over $k$. For a non-singular point $P$ of $S$, let $I$ be a finite subgroup* Aut $(S)$ *of automorphisms of $S$ which fixes the point $P$. If $p = 0$, then $I$ is a cyclic group. If $p > 0$, then there exists a normal subgroup $I_0$ of $I$ such that $|I_0|$ is a power of $p$, and such that $I/I_0$ is a cyclic group of order prime to $p$.*

*Proof.* Let $T^*$ be the co-tangent space of $S$ at $P$. Since $\sigma(P) = P$ for every $\sigma$ of $I$, we obtain a representation of $I$ on the one-dimensional vector space $T^*$. Therefore, we have a homomorphism

$$\mu: I \to k^*.$$

We set $I_0 = \mathrm{Ker}\,\mu$. Since $\mu(I) \simeq I/I_0$ is a subgroup of $k^*$, we see that $I/I_0$ is a cyclic group. Moreover, if $p > 0$, then the order of $I/I_0$ is prime to $p$. When $p = 0$ (resp. $p > 0$), let $\sigma$ be any element of order $n$ of $I_0$ with $(n, p) = 1$. Let $t$ be a regular system of parameters at $P$. We set

$$s = t + \sigma^* t + \cdots + (\sigma^*)^{n-1} t.$$

Since $s = nt$ in $T^*$, we see that $s$ is a regular system of parameters at $P$. Since $s$ is invariant under $\sigma$, the action of $\sigma$ on the local ring of $P$ is trivial. Hence, $\sigma$ is the identity of $I_0$. Hence, $I_0 = \{1\}$ if $p = 0$ (resp. the order of $I_0$ is a power of $p$ if $p > 0$). Q.E.D.

We denote by $V_4$ (resp. $S_n$, resp. $A_n$, resp. $D_{2e}$) Klein's four group (resp. the symmetric group of degree $n$, resp. the alternating group of degree $n$, resp. the dihedral group of order $2e$). We have $V_4 \simeq D_4$ and $S_3 \simeq D_6$.

LEMMA 7.2. *Assume $p \geqslant 7$. Then, the order of the group $G$ as in* (7.2) *is prime to $p$, and the group $G$ is isomorphic to one of the following groups*:

$$\mathbb{Z}/\mathrm{d}\,(1 \leqslant \mathrm{d} \leqslant 6),\ D_{2e}(2 \leqslant e \leqslant 6),\ A_4,\ S_4,\ A_5.$$

*Moreover, the ramification group $I$ of $G$ at a point of $S$ is a cyclic group.*

*Proof.* Since $p \geqslant 7$ and $G \subset S_6$ by (7.4), $p$ does not divide the order of $G$. Hence, there is no wild ramification in $\mathbf{P}^1 \to \mathbf{P}^1/G$, and we can prove the former part in usual way (cf. Pinkham [17, p. 3–p. 5]). The latter part of this lemma follows from Lemma 7.1. Q.E.D.

For our family $q: \mathscr{X} \to S \simeq \mathbf{P}^1$, we have the diagram (1.9) in Section 1. Let $I$ be the stabilizer of $G$ at a point $x$ of $S$. The group $I$ is called a ramification group of $G$ at a branch point $\hat{\psi}(x)$ of $S/G = \tilde{W}$. In this case, we say that the ramification group $I$ occurs at the curve $D_x$. If $I \simeq \mathbb{Z}/n$ $(2 \leqslant n \leqslant 6)$, then the ramification is called a $\mathbb{Z}/n$-ramification. The ramification group $I$ induces a subgroup of the reduced group of automorphisms of $(\mathscr{X}_x, D_x)$. By the definition of $R\Gamma(\mathscr{B})$ with $\mathscr{B} = \mathscr{B}(\mathscr{X}, D)$, the group $I$ also induces a subgroup of $RA(D_x)$:

$$I \hookrightarrow RA(D_x). \tag{7.5}$$

Assume that $\mathscr{X}_x$ is isomorphic to $E \times E$. Then, by (1.9) and (3.11), we have the following diagram:

$$\begin{array}{ccccc} \tilde{A} & \xrightarrow{\tilde{\pi}} & A & \xrightarrow{\pi} & A' \simeq \mathscr{X}_x \\ \| & & \| & & \| \\ E \times E & & E \times E & & E \times E \\ & & \cup & & \cup \\ & & (\pi^{-1})(D_x) & & D_x \end{array} \tag{7.6}$$

with $A = (pr_2)^{-1}(x)$, where $\pi$ and $\tilde{\pi}$ are purely inseparable morphisms of degree $p$, and $\pi \circ \tilde{\pi}$ is the Frobenius morphism. We set $(\pi \circ \tilde{\pi})^{-1}(D_x) = p\tilde{D}_x$. Then, $\tilde{D}_x$ is a (not necessarily irreducible) curve of genus two such that

$$\tilde{D}_x \simeq (D_x)^{(1/p)}. \tag{7.7}$$

The divisor $\pi^{-1}(D_x)$ satisfies Condition (1.10). Since $\pi \circ \tilde{\pi}$ is the Frobenius morphism, the group $I$ also induces a subgroup of $RA(\tilde{D}_x)$:

$$I \hookrightarrow RA(\tilde{D}_x). \tag{7.8}$$

The group $RA(\tilde{D}_x) \simeq RA_v(\tilde{A}, \tilde{D}_x)$ acts on $p + 1$ very good directions of $(\tilde{A}, \tilde{D}_x)$ (cf. Section 3). Therefore, the group $I$ also acts on these very good directions through $RA(\tilde{D}_x)$. Let $a$ be the direction of the natural immersion of Ker $\tilde{\pi} \simeq \alpha_p$ into $\tilde{A} = E \times E$. Then, by our construction, $a$ is a very good direction of $(\tilde{A}, \tilde{D}_x)$ and the action of $I$ on $p + 1$ very good directions of $(\tilde{A}, \tilde{D}_x)$ preserves the direction $a$.

LEMMA 7.3. *Under the notations as above,*

$$I \simeq RA_v(\tilde{A}, \tilde{D}_x, a).$$

*Proof.* The group $RA_v(\tilde{A}, \tilde{D}_x, a)$ is isomorphic to $RA_v(A, \pi^{-1}(D_x))$, which is a subgroup of $R\Gamma(\mathscr{B})$. The group $\Gamma(\mathscr{B})$ induces the group of automorphisms of the family $q$: $\mathscr{X} \to S$ with relative polarization $D$ (cf. Section 4). Therefore, by our construction, we see $I \simeq RA_v(A, \pi^{-1}(D_x))$, hence, $I \simeq RA_v(\tilde{A}, \tilde{D}_x, a)$. Q.E.D.

From here on, we assume $p \geqslant 7$. In this case, the group $I$ is a cyclic group by Lemma 7.2. Let $\sigma$ be a generator of $I$. Then, by (7.8) $\sigma$ acts on the set $\mathbf{P}^1$ of directions of $\tilde{A} = E \times E$ (cf. Section 3). Since the order of $I$ is prime to $p$ in this case, $\sigma$ has two fixed points on $\mathbf{P}^1$. The automorphism $\sigma$ also acts on the set of $p + 1$ very good directions of $(\tilde{A}, \tilde{D}_x)$. The direction $a$ as above is fixed by $\sigma$. From these considerations, we can easily prove the following lemma.

LEMMA 7.4. *Assume $p \geqslant 7$. Under the same notations as above, assume $A' = \mathscr{X}_x \simeq E \times E$. Then, the ramification group $I = \langle\sigma\rangle$ acts on $p + 1$ very good directions of $(\tilde{A}, \tilde{D}_x)$. The automorphism $\sigma$ has at least one fixed* *point and has at most two fixed points on these $p + 1$ very good directions. Moreover, the group $I$ acts freely on the very good directions except the fixed points of $\sigma$.*

We list in Table 2 the ramifications in each group in Lemma 7.2 (for instance, see Pinkham [17, p. 4]).

*Notation 7.5.* Let $G$ be a group as in (7.2). We write

*Table 2.* $p \geqslant 7$

| Group G | Order | Ramification index |
|---|---|---|
| $\mathbb{Z}/n$ $(2 \leqslant n \leqslant 6)$ | $n$ | $(n, n)$ |
| $D_{2e}$ $(2 \leqslant n \leqslant 6)$ | $2e$ | $(2, 2, e)$ |
| $A_4$ | 12 | (2, 3, 3) |
| $S_4$ | 24 | (2, 3, 4) |
| $A_5$ | 60 | (2, 3, 5) |

$$(G;\, e_1', e_2', \text{- - -}\,;\, e_1'', e_2'', \text{- - -}\,)$$

if $e_1'$, $e_2'$, - - - are the orders of the ramification groups at the points of $\tilde{W}$ over which the principal polarizations of type $E' \cup E''$ lie, and $e_1''$, $e_2''$, - - - are the orders of ramification groups at the points of $\tilde{W}$ over which the principal polarizations given by irreducible curves of genus two lie.

Let $C$ be a non-singular irreducible curve of genus two. By Igusa [7], $RA(C)$ is isomorphic to one of the following groups:

$$(0)\{0\},\ (1)\ \mathbb{Z}/2,\ (2)\ S_3,\ (3)\ V_4,\ (4)\ D_{12},\ (5)\ S_4,\ (6)\ \mathbb{Z}/5.$$

In [IKO], Katsura and Oort [8], we said that an irreducible curve $C$ of genus two is in Class (i) $(0 \leqslant i \leqslant 6)$ if $RA(C)$ *contains* the group in (i). In this paper, we use the following definition.

*Definition 7.6.* We say that an irreducible curve $C$ of genus two is of type (i) $(0 \leqslant i \leqslant 6)$ if $RA(C)$ *is isomorphic to* the group in (i).

We note that curves $C$ and $C^{(1/p)}$ are in the same class and of the same type, that is, $RA(C)$ is isomorphic to $RA(C^{(1/p)})$.

*Definition 7.7.* Let $\sigma$ be an element of $S_6$. An element $\tau$ of $S_6$ is said to be of type $\sigma$ if it is conjugate with $\sigma$ in $S_6$.

LEMMA 7.8. *A* $\mathbb{Z}/6$-ramification *appears if and only if* $p \equiv 5 \pmod{12}$, *and in this case it appears once, and we have*

$$(D_{12};\ 2,\ 6;\ 2).$$

*For a generator* $\sigma$ *of the ramification group* $\mathbb{Z}/6$, $\sigma$ *is of type* $(1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6)$.

*Proof.* If $C$ is an irreducible curve of type (i) $(0 \leqslant i \leqslant 6)$ with $i \neq 4$, then $RA(C)$ does not contain a cyclic group of order six. The curve of type (4) is supersingular if and only if $p \equiv 5 \pmod 6$ (cf. [IKO, Proposition 1.11]):

$$p + 1 \equiv 0 \pmod 6. \tag{7.9}$$

The group $RA(C) \simeq D_{12}$ operates on $p + 1$ very good directions of $(J(C), C)$. By (7.9), the group of order six cannot operate on $p + 1$ points with fixed points as in Lemma 7.4. Thus, $\mathbb{Z}/6$-ramifications never appear at any irreducible curve of genus two.

If $C$ is a reducible curve, by Table 1 in Section 6 we see that a $\mathbb{Z}/6$-ramification occurs if and only if $p \equiv 5 \pmod{12}$. In case $p \equiv 5 \pmod{12}$ it appears exactly one. If $G \simeq \mathbb{Z}/6$, then $G$ has two fixed points on $S = \mathbf{P}^1$. Therefore, a $\mathbb{Z}/6$-ramification appears twice on $\tilde{W}$. A contradiction. Therefore, by Lemma 7.2 we have $G \simeq D_{12}$. The group $G$ acts on $5p - 5$ points on $S$ over which the polarizations are reducible. Since $5p - 5 \equiv 8 \pmod{12}$, we have among these $5p - 5$ points two points whose stabilizers are isomorphic to $\mathbb{Z}/6$. The two points transform into each other by $G$. Hence, a $\mathbb{Z}/2$-ramification and a $\mathbb{Z}/6$-ramification appears at some reducible curves and another $\mathbb{Z}/2$-ramification appears once at one curve of type (i) $(1 \leqslant i \leqslant 5)$. The final statement follows from (7.4). Q.E.D.

LEMMA 7.9. *A* $\mathbb{Z}/5$-ramification *appears if and only if* $p \equiv 2$ or $3 \pmod 5$. *In these cases, it appears once, and it appears at the curve of type* (6). *For a generator* $\sigma$ *of the ramification group* $\mathbb{Z}/5$, $\sigma$ *is of type* $(1\ \ 2\ \ 3\ \ 4\ \ 5)$. *The group* $G$ *is*

$$\text{either}\quad G \simeq A_5 \ \text{or}\ G \simeq D_{10}.$$

*If* $G \simeq A_5$ *and*

$$p \equiv \begin{cases} 1 \pmod{12}, \text{ then } (A_5;\ -;\ 2,\ 3,\ 5), \\ 5 \pmod{12}, \text{ then } (A_5;\ 3;\ 2,\ 5), \\ 7 \pmod{12}, \text{ then } (A_5;\ 2;\ 3,\ 5), \\ 11 \pmod{12}, \text{ then } (A_5;\ 2,\ 3;\ 5); \end{cases}$$

*if* $G \simeq D_{10}$, *then*

either $(D_{10}; 2, 2; 5)$ or $(D_{10}; -; 2, 2, 5)$.

*Proof.* Since the order of Aut $(E' \times E'', E' + E'')$ is not divisible by five, a $\mathbb{Z}/5$-ramification cannot appear at any reducible curve. A $\mathbb{Z}/5$-ramification may appear at the curve of type (6). By [IKO, Proposition 1.13], in case $p \geqslant 7$ the curve $C$ of type (6) is supersingular if and only if $p \not\equiv 1 \pmod 5$. If $p \equiv 4 \pmod 5$, the Jacobian variety $J(C)$ is isomorphic to $E \times E$. $RA(C) \simeq \mathbb{Z}/5$ operates at $p + 1$ very good directions of $(J(C), C)$. Since $p + 1 \equiv 0 \pmod 5$, such an action does not exist by Lemma 7.4. Hence, a $\mathbb{Z}/5$-ramification does not appear if $p \equiv 4 \pmod 5$. If $p \equiv 2$ or $3 \pmod 5$, $J(C)$ is supersingular and is not isomorphic to a product of two supersingular elliptic curves. By Theorem 1.2, there exists a unique $\alpha_p$-covering

$$\pi' : E \times E \to J(C).$$

By Lemma 1.5, the action of $\mathbb{Z}/5$ on $(J(C), C)$ lifts to the action on $(E \times E, (\pi')^{-1}(C))$. We may assume that $C$ is symmetric in $J(C)$. Then, $(\pi')^{-1}(C)$ satisfies Condition (2.10). Using this divisor, we can construct a family as in Section 1 in which a $\mathbb{Z}/5$-ramification appears. Conversely, if there exists a family as in Section 1 in which a $\mathbb{Z}/5$-ramification appears, then on $E \times \mathrm{E}$ we can find an effective divisor $L$ which satisfies Condition (1.10) and which is fixed by a group of order five. Since the order of Aut $(E' \times E'', E' + E'')$ is not divisible by five, we see that $L$ is given by an irreducible curve. This means that $L$ is up to isomorphism of $E \times E$ given by $(\pi')^{-1}(C)$ as above with the unique curve of type (6). Hence, the family in which a $\mathbb{Z}/5$-ramification appears uniquely exists if $p \equiv 2$ or $3 \pmod 5$, and a $\mathbb{Z}/5$-ramification appears once. For a generator $\sigma$ of the ramification group $\mathbb{Z}/5$, $\sigma$ is of the type $(1\ 2\ 3\ 4\ 5)$ by (7.4). Suppose $G \simeq \mathbb{Z}/5$. Then, $G$ has two fixed points on $S \simeq \mathbf{P}^1$, and a $\mathbb{Z}/5$-ramification appears twice on $\tilde{W}$. A contradiction. Therefore, we have $G \supsetneqq \mathbb{Z}/5$. By Lemma 7.2, we conclude that $G \simeq A_5$ or $G \simeq D_{10}$. If $p \equiv 1, 5, 7, 11 \pmod{12}$ respectively, then $5p - 5 \equiv 0, 20, 30, 50 \pmod{60}$ respectively. If $G \simeq A_5$, a group of order sixty acts on $5p - 5$ points on $\mathbf{P}^1$ over which reducible polarizations lie. This gives as in the proof of Lemma 7.8 the ramification behavior indicated. If $G \simeq D_{10}$, we have $p^2 + 1 \equiv 0 \pmod{10}$ and $5p - 5 \equiv 0 \pmod{10}$, and the possibilities for the ramification behavior follow. Q.E.D.

*Definition 7.10.* We denote by $E' \cup E''$ a curve composed of two elliptic curves $E'$ and $E''$ whose zero points are identified with transversal crossing. We call six points of exact order two on $E'$ and $E''$ Weierstrass points of $E' \cup E''$.

LEMMA 7.11. *A* $\mathbb{Z}/4$-ramification *does not appear if* $p \equiv \pm 1 \pmod 8$. *If* $p \equiv 3 \pmod 8$, *it appears exactly once. In this case, it appears at a reducible curve* $E' \cup E'$ *and a generator of the ramification group* $\mathbb{Z}/4$ *is of type* $(1\ 2\ 3\ 4)(5\ 6)$. *If* $p \equiv 5 \pmod 8$, *it appears exactly once. In this case, it appears at the curve of type* (5), *and a generator of the ramification group* $\mathbb{Z}/4$ *is of the type* $(1\ 2\ 3\ 4)$. *In these cases, we have either* $G \simeq S_4$ *or* $G \simeq D_8$.

*If* $G \simeq S_4$ *and*

$$p \equiv \begin{cases} 5 \pmod{24}, \text{ then } (S_4;\ 2,\ 3;\ 4), \\ 11 \pmod{24}, \text{ then } (S_4;\ 2,\ 3,\ 4;\ -), \\ 13 \pmod{24}, \text{ then } (S_4;\ 2;\ 3,\ 4), \\ 19 \pmod{24}, \text{ then } (S_4;\ 2,\ 4;\ 3); \end{cases}$$

*if* $G \simeq D_8$ *and*

$$p \equiv \begin{cases} 3 \pmod 8, \text{ then } (D_8;\ 2,\ 2,\ 4;\ -) \text{ or } (D_8;\ 4;\ 2,\ 2), \\ 5 \pmod 8, \text{ then } (D_8;\ 2;\ 2,\ 4). \end{cases}$$

*Proof.* In the case of an irreducible curve, a $\mathbb{Z}/4$-ramification can only appear at the curve $C$ of type (5). By [IKO, Proposition 1.12], this curve is supersingular if and only if $p \equiv 5$ or $7 \pmod 8$. In the case of a reducible curve, a $\mathbb{Z}/4$-ramification can appear if and only if $p \equiv 3 \pmod 8$ by Table 1 in Section 6, and it appears exactly once. If $p \equiv 7 \pmod 8$, $RA(C) \simeq S_4$ acts on $p + 1$ very good directions of $(J(C), C)$. Since $p + 1 \equiv 8$ or $0 \pmod{24}$, a $\mathbb{Z}/4$-ramification does not appear by Lemma 7.4 in this case. If $p \equiv 5 \pmod 8$, $RA(C) \simeq S_4$ acts on $p + 1$ very good directions of $(J(C), C)$. Since $p + 1 \equiv 6$ or $14 \pmod{24}$, each cyclic subgroup of order four has two fixed directions on these $p + 1$ very good directions by Lemma 7.4. In $RA(C)$ we have three cyclic subgroups of order four. Therefore, these fixed directions transform into each other by $RA(C)$. Therefore, a $\mathbb{Z}/4$-ramification appears exactly once and $\mathbb{Z}/4 \subsetneqq G$ as in the proof of Lemma 7.9. Hence, we conclude $G \simeq S_4$ or $D_4$ by Lemma 7.2. Considering the action of the ramification group $\mathbb{Z}/4$ on six Weierstrass points of $C$, we see that a generator of the ramification group $\mathbb{Z}/4$ is of type $(1\ 2\ 3\ 4)$ (cf. Igusa [7]). If $p \equiv 3 \pmod 8$, a $\mathbb{Z}/4$-ramification appears exactly once at the reducible curve $E_i \cup E_i$ (cf. (6.5)). Thus, we have $\mathbb{Z}/4 \subsetneqq G$. The group

$$\tilde{I} \subset \operatorname{Aut}(E_i \times E_i, E_i \times \{0\} + \{0\} \times E_i, a)$$

with a suitable very good direction $a$ which gives the ramification group $\mathbb{Z}/4$ is generated by

$$\begin{pmatrix} 0 & \sigma \\ 1 & 0 \end{pmatrix} : E_i \times E_i \to E_i \times E_i,$$

where $\sigma$ is a complex multiplication by $\sqrt{-1}$ on $E_i$. Considering the action $\left(\begin{smallmatrix} 0 & \sigma \\ 1 & 0 \end{smallmatrix}\right)$ on Weierstrass points of $E_i \times \{0\} \cup \{0\} \times E_i$, we see that a generator of the ramification group $\mathbb{Z}/4$ is of type $(1\ 2\ 3\ 4)(5\ 6)$. Ramification behavior of the groups, if they appear, is computed as in Lemmas 7.8 and 7.9. Q.E.D.

*Notation 7.12.*

$$[a_1, a_5, a_7, a_{11}, a_{13}, a_{17}, a_{19}, a_{23}; 24] := a_i \quad \text{if } p \equiv i \pmod{24}.$$

*Notation 7.13.* We denote by $n_2$ (resp. $n_3$) the number of isomorphism classes of irreducible supersingular curves $C$ of genus two with $RA(C) \simeq S_3$ (resp. $RA(C) \simeq V_4$).

The numbers $n_2$ and $n_3$ are explicitly calculated in [IKO, Theorem 3.3]:

$$n_2 = [([p/3] + 1)/2] - [0, 2, 1, 1, 1, 1, 0, 2; 24],$$

$$n_3 = [([p/4] + 1)/2] - [0, 2, 1, 1, 1, 1, 0, 2; 24],$$

where $[r]$ means the integral part of a rational number $r$.

LEMMA 7.14. *The following is the complete list of all* $\mathbb{Z}/3$-ramifications *which can appear*:

if $p \equiv 5 \pmod{12}$, then $(p - 5)/12$ times at $E_\omega \cup E_\omega$,
if $p \equiv 11 \pmod{12}$, then $(p + 1)/12$ times at $E_\omega \cup E_\omega$,
if $p \equiv 1 \pmod 3$, then $n_2$ times at the curves of type (2),
if $p \equiv 7$ or $13 \pmod{24}$, then once also at the curve of type (5).

*Proof.* For reducible curves, we can read off all ramification groups from Table 1 in Section 6. Since the orders of $RA(C)$ of curves $C$ of type (0), (1), (3) or (6) are not divisible by three, these curves are excluded. As we saw in Lemma 7.8, a $\mathbb{Z}/6$-ramification appears at the curve of type (4) if and only if $p \equiv 5 \pmod{12}$ and a $\mathbb{Z}/3$-ramification does not appear at this curve. The curve $C$ of type (5) is supersingular if and only if $p \equiv 5$ or $7 \pmod 8$. The group $RA(C) \simeq S_4$ acts on $p+1$ very good directions of $(J(C), C)$. If $p \equiv 5$ or $23 \pmod{24}$, then elements of order three act on these very good directions without fixed points by Lemma 7.4. If $p \equiv 7$ or $13 \pmod{24}$, then elements of order three act on these very good directions with fixed points. By this fact, we see that a $\mathbb{Z}/3$-ramification appears exactly once at the curve of type (5) if $p \equiv 7$ or $13 \pmod{24}$. In a similar way, we see that a $\mathbb{Z}/3$-ramification appears exactly once at each curve of type (2) if $p \equiv 1 \pmod 3$, and a $\mathbb{Z}/3$-ramification does not appear at any curve of type (2) if $p \equiv 2 \pmod 3$. Q.E.D.

*Definition* 7.15. Let $C$ be a non-singular complete curve of genus two or a curve as in Definition 7.10. Let $\sigma$ be an element of Aut $(C)$. Suppose that the order of $\sigma$ is two. We say that $\sigma$ is long if the action of $\sigma$ on Weierstrass points of $C$ is a permutation of type $(1\ 2)(3\ 4)(5\ 6)$; we say that $\sigma$ is short if the action on Weierstrass points of $C$ is of type $(1\ 2)(3\,4)$.

LEMMA 7.16. *A* $\mathbb{Z}/2$-ramification *does not appear at* $C = E_\omega \cup E_\omega$. *All* $\mathbb{Z}/2$-ramifications *at* $C = E_i \cup E_i$ *with* $p \equiv 3 \pmod 4$ *are short. All* $\mathbb{Z}/2$-ramifications *at* $C = E' \cup E'$ *with* $j(E') \neq 0,\ 1728$, *and with* $p \equiv 1 \pmod 4$ *are long.*

*Proof.* The first statement follows from Table 1 in Section 6. If $p \equiv 1 \pmod 4$, for every $E'$ with $j(E') \neq 0,\ 1728$ there exists exactly one point on $\tilde{W}$ with ramification group $\mathbb{Z}/2$ (cf. Table 1 in Section 6). It is given by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : E' \cup E' \to E' \cup E',$$

where 1 (resp. $-1$) is the identity (resp. the inversion) of $E'$. On the Weierstrass points of $C = E' \cup E'$, this gives a permutation which is long. If $p \equiv 3 \pmod 4$, every ramification group $\mathbb{Z}/2$ for a reducible curve is given by $C = E_i \cup E_i$ with

$$\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} : E_i \cup E_i \to E_i \cup E_i$$

with $\sqrt{-1}$ of Aut $(E_i)$, the complex multiplication of $\sqrt{-1}$ on $E_i$ as before. The action of this automorphism on the Weierstrass points of $C = E_i \cup E_i$ is short. Q.E.D.

*Remark 7.17.* Both matrices in the proof of the previous lemma are of order four.

PROPOSITION 7.18. *Let $C$ be an irreducible curve of genus two. Let $\sigma$ be an element of order two of $RA(C)$, and let $\tilde{\sigma}$ be an element of* Aut $(C)$ *which gives $\sigma$ in $RA(C)$.*

(*i*) *If $\sigma$ is short, then the order of $\tilde{\sigma}$ is equal to four.*
(*ii*) *If $\sigma$ is long, then the order of $\tilde{\sigma}$ is equal to two.*
(*iii*) *If $C$ is supersingular and a ramification group $\mathbb{Z}/2$ is given by $\sigma$, then $\sigma$ is short.*

*Proof.* (i) In this case, we can assume that $\sigma$ fixes the points 0 and $\infty$ of $\mathbf{P}^1$ with respect to a suitable coordinate $X$ of $\mathbf{A}^1$ in $\mathbf{P}^1$. Then, the curve $C$ is given in the form

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

with $a, b \in k^*$; $a \neq 0, 1$; $b \neq 0, 1$; $a \neq b$, and the automorphism $\tilde{\sigma}$ is given by

$$\tilde{\sigma}\colon X \mapsto -X,\ Y \mapsto \sqrt{-1}\,Y.$$

Hence, we have ord $\tilde{\sigma} = 4$.

(ii) In this case, $C$ is given in the form

$$Y^2 = (X^2 - a)(X^2 - b)(x^2 - c)$$

and $\tilde{\sigma}$ is given in the form

$$\tilde{\sigma}\colon X \mapsto -X,\ Y \mapsto Y.$$

Hence, we have ord $\tilde{\sigma} = 2$.

(iii) Let $\sigma \in RA(C)$ be an element of order two. Since $\sigma$ has exactly two fixed points on $\mathbf{P}^1 \simeq C/\langle\iota\rangle$, $\sigma$ cannot be of type (1 2). Suppose $\sigma$ is long. Then, by (ii) there exists an element $\tilde{\sigma}$ of order two of Aut $(C)$ such that $\tilde{\sigma}$ gives $\sigma$ in $RA(C)$. As in Igusa [7, p. 648] and [IKO, the proof of Proposition 1.3], we have a separable morphism of degree four

$$\pi_1 \colon J(C) \to E_\sigma \times E_\tau, \tag{7.10}$$

where $E_\sigma = C/\langle\tilde{\sigma}\rangle$, $E_\tau = C/\langle\iota \circ \tilde{\sigma}\rangle$ and they are elliptic curves. Ker $\pi_1$ is contained in the group of elements of order two of $J(C)$. Therefore, there exists an isogeny $\pi_2$: $E_\sigma \times E_\tau \to J(C)$ such that $\pi_1 \circ \pi_2 = [2]_{E_\sigma \times E_\tau}$. The automorphism $\tilde{\sigma}$ acts on $J(C)$ and induces the action on $E_\sigma \times E_\tau$ in (7.10). The action of $\tilde{\sigma}$ on $E_\sigma \times E_\tau$ is given by

$$\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : E_\sigma \times E_\tau \to E_\sigma \times E_\tau,$$

where 1 (resp. $-1$) is the identity of $E_\sigma$ (the inversion of $E_\tau$). We have the commutative diagram:

$$\begin{tikzcd}
E_\sigma \times E_\tau \arrow[r, "\sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}"] \arrow[d, "\pi_2"'] & E_\sigma \times E_\tau \arrow[d, "\pi_2"] \\
J(C) \arrow[r, "\sigma'"] \arrow[d, "\pi_1"'] & J(C) \arrow[d, "\pi_1"] \\
E_\sigma \times E_\tau \arrow[r, "\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}"'] & E_\sigma \times E_\tau,
\end{tikzcd} \tag{7.11}$$

where $\sigma'$ is an isomorphism induced by $\sigma_2$. The isomorphism $\sigma'$ is different from $\tilde{\sigma}$ by a translation by an element of order two. Since $(\sigma')^*(C)$ is algebraically equivalent to $C$, $\sigma_2^* \circ \pi_2^*(C)$ is algebraically equivalent to $\pi_2^*(C)$. Therefore, we have the following commutative diagram:

$$\begin{tikzcd}
E_\sigma \times E_\tau \arrow[r, "\sigma_2"] \arrow[d, "\varphi_{E_\sigma + E_\tau}"'] & E_\sigma \times E_\tau \arrow[d, "\varphi_{E_\sigma + E_\tau}"] \\
E_\sigma^t \times E_\tau^t & E_\sigma^t \times E_\tau^t \arrow[l, "\sigma_2^t"'] \\
E_\sigma \times E_\tau \arrow[r, "\sigma_2"] \arrow[u, "\varphi_{\pi_2^*(C)}"] & E_\sigma \times E_\tau . \arrow[u, "\varphi_{\pi_2^*(C)}"']
\end{tikzcd}$$

Since $\varphi_{E_\sigma + E_\tau}$ is an isomorphism, we have

$$\varphi^{-1}_{E_\sigma + E_\tau} \circ \varphi_{\pi^*(C)} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where $\alpha \in \operatorname{End}(E_\sigma)$, $\delta \in \operatorname{End}(E_\tau)$, $\beta \in \operatorname{Hom}(E_\tau, E_\sigma)$ and $\gamma \in \operatorname{Hom}(E_\sigma, E_\tau)$. Therefore, we have

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Hence, we have $\beta = 0$ and $\gamma = 0$. Since $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \delta \end{smallmatrix}\right)$ is given by a polarization, we see that $\alpha$ and $\delta$ are integers (cf. Mumford [12, p. 190, (3)]). It is easy to see that

$$\varphi^{-1}_{E_\sigma + E_\tau} \circ \varphi_{E_\sigma} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\varphi^{-1}_{E_\sigma + E_\tau} \circ \varphi_{E_\tau} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Therefore, we have

$$\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} = \varphi^{-1}_{E_\sigma + E_\tau} \circ \varphi_{\delta E_\sigma + \alpha E_\tau}.$$

Hence, we have

$$\pi_2^*(C) \equiv \delta E_\sigma + \alpha E_\tau.$$

We denote by $pr_\tau$ the projection from $E_\sigma \times E_\tau$ to the second factor $E_\tau$, and by $o_\tau$ the origin of $E_\tau$. We have the equality of intersection numbers

$$(C \cdot \pi_1^*(E_\sigma)) = (C \cdot \pi_1^* \circ pr_\tau^*(o_\tau)) = \deg pr_\tau \circ \pi_1|_C = 2.$$

We have also

$$(\pi_1 \circ \pi_2)^*(E_\sigma) = [2]^*_{E_\sigma + E_\tau}(E_\sigma) \equiv 4E_\sigma.$$

Therefore, we have

$$\begin{aligned} 4(E_\sigma \cdot \pi_2^*(C)) &= ((\pi_1 \circ \pi_2)^*(E_\sigma) \cdot \pi_2^*(C)) \\ &= \deg \pi_2 \cdot (\pi_1^*(E_\sigma) \cdot C) = 2^2 \cdot 2. \end{aligned}$$

Hence, we have $\alpha = (E_\sigma \cdot \pi_2^*(C)) = 2$. Similarly, we have $\delta = (E_\tau \cdot \pi_2^*(C)) = 2$, that is, we have

$$\pi_2^*(C) \equiv 2(E_\sigma + E_\tau). \tag{7.12}$$

The tangent space at the origin of $E_\sigma \times E_\tau$ is isomorphic to the tangent space at the origin of $J(C)$ by the homomorphism $(\pi_2)_*$ induced by $\pi_2$. By (7.12), we see that $a \in k^*$ is a very good direction of $(E_\sigma \times E_\tau, E_\sigma + E_\tau)$ if and only if $(\pi_2)_*(a)$ is a very good direction of $(J(C), C)$. Let $(\pi_2)_*(a)$ be a very good direction of $(J(C), C)$ which is fixed by the action of $\tilde{\sigma}$. Then, by the definition of the action of $\sigma$ and the diagram (7.11), $a$ is a very good direction of $(E_\sigma \times E_\tau, E_\sigma + E_\tau)$ fixed by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Hence, we have $(1, a) = (1, 0)$ or $(0, 1)$. This contradicts the result in Moret-Bailly [11, p. 139]. Hence, $\sigma$ is short. Q.E.D.

COROLLARY 7.19. (*i*) *Curves of type* (1) *do not give any* $\mathbb{Z}/2$-ramification.
(*ii*) *Curves of type* (2) *do not give any* $\mathbb{Z}/2$-ramification.
(*iii*) *Curves of type* (3) *do not give any* $\mathbb{Z}/2$-ramification *if* $p \equiv 3 \pmod 4$. *Each curve of type* (3) *gives exactly once a* $\mathbb{Z}/2$-ramification *if* $p \equiv 1 \pmod 4$.

*Proof.* For curves of type (1) or (2) every 2-torsion element in $RA(C)$ is long. Therefore, (i) and (ii) follow from Proposition 7.18. For a curve $C$ of type (3), $RA(C) = V_4$ has two long and one short 2-torsion elements. This group acts on $p + 1$ very good directions of $(J(C), C)$. If $p \equiv 3 \pmod 4$, by Lemmas 7.2 and 7.4 the subgroups of $RA(C)$ of order two give in all no or four fixed directions on these very good directions. By Proposition 7.18, we conclude that $RA(C)$ gives no fixed directions. If $p \equiv 1 \pmod 4$, the subgroups of $RA(C)$ of order two gives in all two or six fixed directions. Therefore, by Proposition 7.18, it gives exactly two fixed directions.Since the order of $RA(C)$ is four, the two fixed directions transform into each other by $RA(C)$. Hence, a $\mathbb{Z}/2$-ramification appears exactly once for each curve $C$ in this case. Q.E.D.

COROLLARY 7.20. *If* $p \equiv 5 \pmod{12}$, *the normalization of the component of* $V$ *corresponding to the group* $D_{12}$ *has a* $\mathbb{Z}/2$-ramification *at a curve of type* $E' \cup E'$ *with* $j(E') \neq 0, 1728$.

*Proof.* Since we have an injection $D_{12} \to S_6$, $D_{12}$ acts on six points as permutation. Therefore, the order of the stabilizer of each point is equal to two. Therefore, the number of elements of order two of $D_{12}$ which is not long is at most three. We denote by $N$ the normal subgroup of order six of $D_{12}$. Then, we have an element of order two of $D_{12}\backslash N$ which is long. Hence, this proposition follows from Lemma 7.16 and Proposition 7.18 (iii). Q.E.D.

LEMMA 7.21. (*i*) *If* $D_{10} \to S_6$, *then all* 2-torsion *elements in* $D_{10}$ *are short.*
(*ii*) *If* $D_8 \hookrightarrow S_6$ *with* $\delta \mapsto (1\ 2\ 3\ 4)$, *then* $D_8\backslash\langle\delta\rangle$ *has short and long* 2-torsion *elements.*
(*iii*) *If* $D_8 \hookrightarrow S_6$ *with* $\delta \mapsto (1\ 2\ 3\ 4)(5\ 6)$, *then either all elements* $D_8\backslash\langle\delta\rangle$ *are short, or* $D_8$ *contains an element of type* $(2\ 4)$.

*Proof.* Considering the action of groups on six points, we get this lemma by straightforward calculation. Q.E.D.

We summarize in Table 3 the results on the numbers of branch points which can appear. We denote by $E_\omega$ (resp. $E_i$) the elliptic curve with $j(E_\omega) = 0$ (resp. $j(E_i) = 1728$) as in (6.5). In the following table, we denote by $E'$ supersingular elliptic curves with $j(E') \neq 0, 1728$.

For small prime numbers we list in Table 4 the total number of branch points for the groups determined by the irreducible components of $V$.

## §8. Examples

Let $k$ be an algebraically closed field of characteristic $p \geqslant 2$. Every irreducible component $W$ of the supersingular locus $V$ of $\mathscr{A}_{2,1}$ is given in the form

$$\psi\colon S = \mathbf{P}^1 \to \mathbf{P}^1/G = \tilde{W} \to W \subset \mathscr{A}_{2,1} \tag{8.1}$$

as in (2.2), where $G$ is the group as in (7.2), and where $\tilde{W}$ is the normalization of $W$ (for the case $p = 2$, see Remarks 1.5 and 4.6). For a point $x$ of $S$, we denote by $G_x$ the stabilizer of $G$ at $x$ as before. For a point $y$ of $\tilde{W}$ we also

*Table 3.* $p \geqslant 7$

<table>
<tr><td colspan="3">Ramification group \ $p$ mod 24</td><td>1</td><td>5</td><td>7</td><td>11</td><td>13</td><td>17</td><td>19</td><td>23</td></tr>
<tr><td>$\mathbb{Z}/6$</td><td colspan="2">at $E_\omega \cup E_\omega$</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">$\mathbb{Z}/4$</td><td colspan="2">type (1 2 3 4)(5 6) at $E_\iota \cup E_\iota$</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td colspan="2">type (1 2 3 4) at $C$ of type (5)</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td rowspan="3">$\mathbb{Z}/3$</td><td colspan="2">at $E_\omega \cup E_\omega$</td><td>0</td><td>$(p-5)/12$</td><td>0</td><td>$(p+1)/12$</td><td>0</td><td>$(p-5)/12$</td><td>0</td><td>$(p+1)/12$</td></tr>
<tr><td colspan="2">at $C$ of type (5)</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td colspan="2">at $C$ of type (2)</td><td>$n_2$</td><td>0</td><td>$n_2$</td><td>0</td><td>$n_2$</td><td>0</td><td>$n_2$</td><td>0</td></tr>
<tr><td rowspan="4">$\mathbb{Z}/2$</td><td>long</td><td>at $E' \cup E'$</td><td>$(p-1)/12$</td><td>$(p-5)/12$</td><td>0</td><td>0</td><td>$(p-1)/12$</td><td>$(p-5)/12$</td><td>0</td><td>0</td></tr>
<tr><td rowspan="3">short</td><td>at $E_\iota \cup E_\iota$</td><td>0</td><td>0</td><td>$(p+1)/8$</td><td>$(p-3)/8$</td><td>0</td><td>0</td><td>$(p-3)/8$</td><td>$(p+1)/8$</td></tr>
<tr><td>at $C$ of type (4)</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>at $C$ of type (3)</td><td>$n_3$</td><td>$n_3$</td><td>0</td><td>0</td><td>$n_3$</td><td>$n_3$</td><td>0</td><td>0</td></tr>
<tr><td>$\mathbb{Z}/5$</td><td colspan="2">at $C$ of type (6)</td><td colspan="8">0 if $p \equiv 1$ or 4 (mod 5)<br>1 if $p \equiv 2$ or 3 (mod 5)</td></tr>
</table>

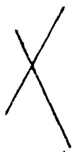
*Table 4.* $p \geqslant 7$

| Ramification group | | $p$ | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathbb{Z}/6$ | $E_\omega \cup E_\omega$ | | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| $\mathbb{Z}/5$ | type (6) | | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| $\mathbb{Z}/4$ | $E_\iota \cup E_\iota$ | | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| | type (5) | | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| $\mathbb{Z}/3$ | $E_\omega \cup E_\omega$ | | 0 | 1 | 0 | 1 | 0 | 2 | 2 | 0 | 0 | 3 | 0 | 4 | 4 | 5 | 1 |
| | type (5) | | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| | type (2) | | 0 | 0 | 1 | 0 | 3 | 0 | 0 | 4 | 5 | 0 | 7 | 0 | 0 | 0 | 9 |
| $\mathbb{Z}/2$ | long | $E' \cup E'$ | 0 | 0 | 1 | 1 | 0 | 0 | 2 | 0 | 3 | 3 | 0 | 0 | 4 | 0 | 5 |
| | short | $E_\iota \cup E_\iota$ | 1 | 1 | 0 | 0 | 2 | 3 | 0 | 4 | 0 | 0 | 5 | 6 | 0 | 7 | 0 |
| | | type (4) | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| | | type (3) | 0 | 0 | 1 | 1 | 0 | 0 | 2 | 0 | 4 | 4 | 0 | 0 | 5 | 0 | 7 |
| total | | | 3 | 3 | 6 | 6 | 6 | 6 | 9 | 9 | 15 | 12 | 14 | 11 | 17 | 13 | 23 |
| $H_2(1, p)$ | | | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 5 | 4 | 5 | 4 | 6 | 5 | 8 |

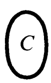
denote by $G_y$ the corresponding inertia group. We denote by $\delta_y$ the degree of local difference at $y$ of $\tilde{W}$. For a point $x$ of $S$, we denote $\delta_{\psi(x)}$ by $\delta_x$. We have

$$\begin{aligned} &\delta_x \geqslant |G_x| - 1 \text{ for } x \text{ of } \tilde{W} \text{ (resp. of } S), \\ &\text{and the equality holds if } |G_x| \text{ is prime to } p. \end{aligned} \tag{8.2}$$

In this section, for small characteristics $p$ we determine which groups $G$ appear, and in which way the ramifications, the groups and the curves are related. In the picture below, we use the following symbols:

(*a*):  $E_1$ $E_2$ principally polarized abelian surface $E_1 \times E_2$ with polarization $E_1 + E_2$, where $E_1$ and $E_2$ are supersingular elliptic curves,

(b):  $C$ principally polarized abelian surface $(J(C), C)$ with a non-singular curve $C$ of genus two such that $J(C)$ is isomorphic to a product of two supersingular elliptic curves,

(c):  principally polarized abelian surface $(J(C), C)$ with a non-singular curve $C$ of genus two such that $J(C)$ is supersingular and is not isomorphic to a product of two elliptic curves.

In a family $q$: $\mathscr{X} \to \mathbf{P}^1$ with relative polarization $D$ as in (1.9) we have $p^2 + 1$ fibres of type (*a*) or (*b*), and we have $5p - 5$ fibres of type (*a*) as we have seen in (1.13).

(1) $p = 2$

In this case, the supersingular locus was already studied by Igusa [7, pp. 615–616], and it turned out to be irreducible. In Moret-Bailly [10], we find a more refined description. There exists exactly one family $q$: $\mathscr{X} \to S$ of principally polarized abelian surfaces as in Moret-Bailly [10]. Exactly five fibres of $q$: $\mathscr{X} \to S$ are principally polarized abelian surfaces of degenerate type. Let $x_1, \text{---}, x_5$ be the corresponding points. In case $p = 2$, there is only one isomorphism class of supersingular elliptic curves defined by

$$E \colon Y^2 + Y = X^3.$$

There is only one standard divisor as in Section 3, which corresponds to the family $q$: $\mathscr{X} \to S$. Let $\mathscr{G}$ be the group of automorphisms of the family $q$: $\mathscr{X} \to S$ preserving the relative polarization. By the uniqueness of the standard divisor, $\mathscr{G}$ acts transitively on the set $\{x_1, \text{- - -}, x_5\}$, and by Table 1 in Section 6 we see that the order of the stabilizer at $x_1$ is equal to $192 \times 2 = 384$. Therefore, we have

$$|\mathscr{G}|/384 = 5, \quad \text{hence } |\mathscr{G}| = 1920.$$

If a curve of genus two in characteristic two is supersingular, its normal form is $Y^2 + Y = X^5 + \alpha X^3$ (cf. Igusa [7, p. 615]), hence by Igusa [7, p. 645] we see that a general fibre of $q: \mathscr{X} \to S$ has a group of automorphisms of order $2^4 \times 2$ as principally polarized abelian surface. Thus, $G = \text{Gal}\,(\mathbf{P}^1 \to \tilde{V})$ has order

$$|G| = 1920/(2^4 \times 2) = 60.$$

This group $G$ acts transitively on the set $\{x_1, \text{- - -}, x_5\}$ and the inertia group $G$ has order $384/(2^4 \times 2) = 12$. There is exactly one (isomorphism class of an) irreducible curve $C$ which has more automorphisms than a general supersingular curve:

$$C\colon Y^2 + Y = X^5.$$

In Igusa [7, p. 645], we have $|RC(C)| = 16 \times 5$. Let $\{y_1, \text{- - -}, y_n\}$ be the points of $S$ over which there is such a fibre. Then the inertia group at such a point has order $160/(2^4 \times 2) = 5$, hence at such points the covering is tamely ramified, and the local difference at such points equals $\delta_y = 4$. The covering $\tilde{\psi}: S = \mathbf{P}^1 \to \tilde{V}$ ramifies exactly at the points corresponding to the following principally abelian surfaces:

(a) $(E \times E, E \times \{0\} + \{0\} \times E)$ with
 $|G_x| = 12$, $x = \tilde{\psi}(x_i)$ $(1 \leqq i \leqq 5)$ and local different $\delta_x$;
 note that $\delta_x \geqq 12$,

(b) $(J(C), C)$ with
 $|G_y| = 4$, $y = \tilde{\psi}(y_j)$ $(i \leqq j \leqq n)$ and $\delta_y = 4$.

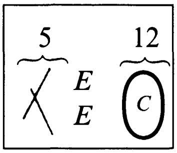
The Zeuthen–Hurwitz–Hasse formula reads in this case:

$$-2 = 60 \times (-2) + (60/12)\delta_x + n \times \delta_y.$$

Note that $n$ is a multiple of 12. We see that this is only possible with $n = 12$ and $\delta_x = 14$. Thus there is one orbit of points corresponding to $C$.

Summarizing, we have:

$\mathscr{X}$




$$\downarrow q$$

$$S \quad \underset{x_i \qquad y_j}{\rule{6em}{0.4pt}} \xrightarrow{\tilde{\psi}} \tilde{V} \longrightarrow V \subset \mathscr{A}_{2,1}$$

$$|G_x| = 12,\ \delta_x = 14; \quad |G_y| = 5,\ \delta_y = 4; \quad \deg \tilde{\psi} = 60.$$

THEOREM 8.1. *Assume $p = 2$. Under the notations as above,*

$$G \simeq A_5.$$

*Proof.* The group $G$ acts on the set $\{x_1, \text{- - -}, x_5\}$ as permutation. Since any element of $G$ which is not the identity has at most two fixed points on $\mathbf{P}^1$, the action of $G$ on $\{x_1, \text{- - -}, x_5\}$ is faithful. Since $|G| = 60$, we conclude $G \simeq A_5$. Q.E.D.

*Remark 8.2.* We give here another proof of Theorem 8.1 and a remark on the defining field of some special points on $S$. Let $\sigma$ be an element of $\mathscr{G}_{x_1}$ with $\operatorname{ord} \sigma = 3$. Then, $\sigma$ permutes $\{x_2, \text{- - -}, x_5\}$. It has a fixed point in $\{x_2, \text{- - -}, x_5\}$, say $\sigma(x_2) = x_2$. We choose an isomorphism

$$\theta \colon S \xrightarrow{\sim} \mathbf{P}^1$$

such that $\theta(\{x_3, x_4, x_5\}) = \mathbf{P}^1(\mathbf{F}_2)$. Then, we have $\sigma \in PGL(2, \mathbf{F}_2)$. Therefore, we have $x_1, x_2 \in \mathbf{P}^1(\mathbf{F}_4)$, and

$$\theta(\{x_1, \text{- - -}, x_5)\} = \mathbf{P}^1(\mathbf{F}_4).$$

Thus, we have an injective homomorphism

$$G \hookrightarrow PGL(2, \mathbf{F}_4).$$

Since $|G| = 60 = |PGL(2, \mathbf{F}_4)|$, we have

$$G \simeq PGL(2, \mathbf{F}_4) \simeq A_5.$$

Note that under $\theta$ the points $y_j$ $(1 \leqslant j \leqslant 12)$ are mapped onto $\mathbf{P}^1(\mathbf{F}_{16})\backslash\mathbf{P}^1(\mathbf{F}_4)$.

Now, assume $p \geqslant 3$. The number of irreducible components of $V_2 \subset \mathscr{A}_{2,1,2}$ equals $(p^2 - 1)/4$ (cf. Corollary 5.2). For every irreducible component $W$ of $V$ in $\mathscr{A}_{2,1}$, and an irreducible component $W_2$ of $V_2$ in $\mathscr{A}_{2,1,2}$ over $W$, we have a family $q\colon \mathscr{X} \to S \simeq \mathbf{P}^1$ and a group $G$ as in (7.2) such that $S$ is isomorphic to the normalization $\tilde{W}_2$ of $W_2$ (cf. Corollary 4.5). We have the morphism

$$\psi\colon S \to S/G \simeq \tilde{W} \to W \subset \mathscr{A}_{2,1}.$$

We fix a prime number $p$. We use the notations in Section 5. We set

$$G_\lambda\colon = R\Gamma(\mathscr{B}_\lambda) \quad (\lambda = 1, \text{- - -}, H' = H_2(1, p))$$

(cf. Theorem 5.7). Since $S \simeq \tilde{W}_2$, we have

$$\sum_{\lambda=1}^{H'} 720/|G_\lambda| = (p^2 - 1)/4 \tag{8.3}$$

(cf. Theorem 5.1 and Corollary 5.2).

(2) $p = 3$

There exists up to isomorphism exactly one supersingular elliptic curve $E$ defined by

$$E\colon Y^2 = X^3 - X.$$

We have only one standard divisor (cf. Section 3 and Table 1 in Section 6). Therefore, we have $H' = 1$ (see also Remark 5.9). Thus, by (8.3) we have

$$|G| = 4 \cdot 720/(p^2 - 1) = 360.$$

The family $q\colon \mathscr{X} \to S$ with relative polarization $D$ has $5p - 5 = 10$ fibres of principally polarized abelian surfaces of degenerate type, say at $x_1$, - - - , $x_{10}$ of $S$. By Table 1 in Section 6, we see

$$|G_{x_i}| = 72/2 = 36,$$

hence, $G$ operates transitively on $\{x_1, \cdots, x_{10}\}$. The branch locus of $\tilde{\psi}$: $S = \mathbf{P}^1 \to \tilde{W}$ is at the points corresponding to
(a) $(E \times E, E \times \{0\} + \{0\} \times E)$
(b) $(J(C), C)$, $C$: $Y^2 = X^5 - 1$ (the curve of type (6)).
The Jacobian variety $J(C)$ is not isomorphic to a product of two supersingular elliptic curves (cf. [IKO, Proposition 1.13]). Let $y_j \in S$ $(1 \leqslant j \leqslant n(360/5)$ with an integer $n)$ be the points of $S$ corresponding to the curve of type (6). Then, since $RA(C) \simeq \mathbb{Z}/5$, we see that

$$G_{y_j} \simeq \mathbb{Z}/5 \quad (1 \leqslant j \leqslant n(360/5))$$

by a similar method as in the proof of Lemma 7.9. By the Zeuthen–Hurwitz–Hasse formula, we have

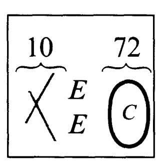
$$-2 = 360 \times (-2) + \sum_{i=1}^{10} \delta_{x_i} + \sum_{j=1}^{72n} \delta_{y_j}$$

with $\delta_{y_j} = 4$ and $\delta_{x_i} = m$, where $m$ and $n$ are some integers. Thus, we have

$$-2 = 360 \times (-2) + 10m + 4 \times 72n.$$

This is possible if and only if $n = 1$ and $m = 43$. We set $x = \tilde{\psi}(x_i)$ $(1 \leqslant i \leqslant 10)$ and $y = \tilde{\psi}(y_j)$ $(1 \leqslant j \leqslant 72)$. Then, we have the following picture of $q$: $\mathscr{X} \to S$ with relative polarization $D$.

$\mathscr{X}$




$\downarrow q$

$S$ $\underset{x_i \qquad y_j}{\overline{\qquad\qquad}} \xrightarrow{\tilde{\psi}} \tilde{V} \longrightarrow V \subset \mathscr{A}_{2,1}$

$|G_x| = 36,\ \delta_x = 43;\quad |G_y| = 5,\ \delta_y = 4;\quad \deg \tilde{\psi} = 360.$

THEOREM 8.3. *Assume $p = 3$. Under the notations as above,*

$$G \simeq A_6.$$

*Proof.* By Corollary 4.4, we have an injective homomorphism $G \hookrightarrow S_6$. Since $|G| = 360$, we conclude $G \simeq A_6$. Q.E.D.

(3) $p = 5$

There exists up to isomorphism exactly one supersingular elliptic curve $E$ defined by

$$E:\ Y^2 = X^3 - 1.$$

There exists up to isomorphism exactly one irreducible supersingular curve $C$ of genus two defined by

$$C:\ Y^2 = X^5 - X$$

such that the Jacobian variety $J(C)$ is isomorphic to $E \times E$. We have $RA(C) \simeq PGL(2, \mathbf{F}_5)$ (cf. Igusa [7, p. 645]), thus $|RA(C)| = 120$. We have only one standard divisor (cf. Section 3 and Table 1 in Section 6). Therefore, we have $H' = 1$ (see also Remark 5.9), and by (8.3) we have

$$|G| = 4 \cdot 720/(p^2 - 1) = 120.$$

We have $5p - 5 = 20$ points $x_1, \cdots, x_{20}$ of $S$ corresponding to

(a) $(E \times E, E \times \{10\} + \{0\} \times E)$.

By Table 1 in Section 6 we have

$$|G_{x_i}| = 12/2 = 6.$$

Therefore, $G$ operates transitively on the set $\{x_1, \cdots, x_{20}\}$. Since $J(C) \simeq E \times E$, the number of points of $S$ corresponding to

(b) $(J(C), C)$

is equal to $(p^2 + 1) - (5p - 5) = 6$. We denote by $y_1, \cdots, y_6$ the points of $S$ which correspond to $(J(C), C)$. Let $t$ be the number of orbits of the action of $G$ on $\{y_1, \cdots, y_6\}$, and let $n_i$ $(1 \leqslant i \leqslant t)$ be the cardinality of these orbits. By the Zeuthen–Hurwitz–Hasse formula we have

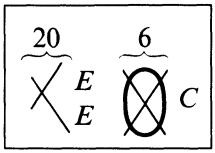
$$-2 = 120 \times (-2) + \sum_{i=1}^{20} \delta_{x_i} + \sum_{j=1}^{6} \delta_{y_j}$$

with $\delta_{x_i} = 5$ $(1 \leqslant i \leqslant 20)$. Thus, we have $\Sigma_{j=1}^{6} \delta_{y_j} = 138$. If $y_j$ is a point in an orbit whose cardinality is $n_i$, then we have

$$\delta_{y_j} \geqslant (120/n_i) - 1$$

by (8.2). Since $n_1 + n_2 + \cdots + n_t = 6$, we see that if $t \geqslant 2$, then $\Sigma_{j=1}^{6} \delta_{y_j} > 6 \cdot 23 = 138$. Thus, we have $t = 1$. Hence, $G$ acts transitively on $\{y_1, \cdots, y_6\}$ and we have $|G_{y_j}| = 20$ $(1 \leqslant j \leqslant 6)$. Moreover, we have $\delta_{y_j} = 138/6 = 23$. We set $x = \tilde{\psi}(x_i)$ $(1 \leqslant i \leqslant 20)$ and $y = \tilde{\psi}(y_j)$ $(1 \leqslant j \leqslant 6)$. Then, we have the following picture of $q\colon \mathscr{X} \to S$ with relative polarization $D$.

$\mathscr{X}$




$\downarrow q$

$S \qquad \underset{x_i \qquad y_j}{\rule{6cm}{0.4pt}} \xrightarrow{\tilde{\psi}} \tilde{V} \longrightarrow V \subset \mathscr{A}_{2,1}$

$$G_x \simeq \mathbb{Z}/6,\ \delta_x = 5; \quad |G_y| = 20,\ \delta_y = 23; \quad \deg \tilde{\psi} = 120.$$

Using Lemma 7.2 and $G_y \subset G \subset S_6$, we see $G_y \simeq \langle \sigma, \tau \rangle$ with suitable elements $\sigma$ and $\tau$ such that ord $\sigma = 4$, ord $\tau = 5$ and $\sigma\tau = \tau^2\sigma$.

THEOREM 8.4. *Assume $p = 5$. Under the notations as above,*

$$G \simeq PGL(2, \mathbf{F}_5) \simeq RA(C).$$

*Proof.* Let $\tau$ be an element of order five of $G_{y_6}$. Then, we have $\tau(y_6) = y_6$ and $\tau$ permutes $\{y_1, \cdots, y_5\}$. We may assume $\tau(y_1) = y_2$. We can choose an isomorphism

$$\theta\colon S \xrightarrow{\sim} \mathbf{P}^1$$

such that $\theta(y_6) = (1:0)$, $\theta(y_1) = (0:1)$ and $\theta(y_2) = (1:1)$. Then, by our choice of coordinates, we have

$$\theta \circ \tau \circ \theta^{-1}(x) = x + 1,$$

where $x$ is an inhomogeneous coordinate of $\mathbf{A}^1 = \mathbf{P}^1 \backslash \{(1:0)\}$. The set $\{y_1, \cdots, y_6\}$ is mapped by $\theta$ onto $\mathbf{P}^1(\mathbf{F}_5)$. Any element $g$ of $G$ induces a permutation of $\{y_1, \cdots, y_6\}$. Therefore, we have an injective homomorphism $g \hookrightarrow PGL(2, \mathbf{F}_5)$. Since $|G| = 120 = |PGL(2, \mathbf{F}_5)|$, we have $G \simeq PGL(2, \mathbf{F}_5)$. Q.E.D.

*Remark 8.5.* As in the proof of Theorem 8.4, any element of $G_{x_i}$ is defined over $\mathbf{F}_5$. Therefore, we see $\theta(x_i) \in \mathbf{P}^1(\mathbf{F}_{25})$. Hence, $\{x_1, \cdots, x_{20}\}$ is mapped onto $\mathbf{P}^1(\mathbf{F}_{25})\backslash\mathbf{P}^1(\mathbf{F}_5)$ by $\theta$.

*Remark 8.6.* In Section 5, we proved that $V$ is irreducible if and only if $p \leqslant 11$ (cf. Theorem 5.8). Here we present another proof in which we do not use any calculation of class numbers.

In case $2 \leqslant p \leqslant 5$, we have seen earlier in this section that $V$ is irreducible. Now we use the results in Section 7 for other prime numbers. In case $7 \leqslant p \leqslant 11$, we have

$$\sum_{\lambda=1}^{H'} 720/|G_\lambda| \leqslant 60$$

by (8.3). Therefore, we have $|G_\lambda| \geqslant 12$. By Lemma 7.2 and Pinkham [17, p. 4], $G_\lambda$ operates with at least three branch points. In Table 4 in Section 7, we have seen that for $p = 7$ or 11 the total number of branch points is equal to three. Thus, $V$ is irreducible in these cases. In case $p \geqslant 13$, we see by Table 3 in Section 7 that the total number of branch points is greater than or equal to six. Since for each family as in (7.1) we have at most three branch points by Table 2 in Section 7, we conclude that $V$ is reducible.

From now on, we assume $p \geqslant 7$. Under the notations in (8.1), we have seen in Lemma 7.2 which groups can appear. We have also seen

$$G \not\simeq \mathbf{Z}/6 \text{ (cf. Lemma 7.8) and } G \not\simeq \mathbf{Z}/5 \text{ (cf. Lemma 7.9).}$$

The supersingular locus $V_2$ in $\mathscr{A}_{2,1,2}$ has $(p^2 - 1)/4$ irreducible components (cf. Corollary 5.2). Let $\{W_\lambda\}_{\lambda=1,\cdots,H'}$ be the set of irreducible components of the supersingular locus $V$ in $\mathscr{A}_{2,1}$.

*Notation 8.7.* Suppose that $W_\lambda$ corresponds to $(G_\lambda;\, e'_{\lambda,1}, e'_{\lambda,2}, \cdots;\, e''_{\lambda,1}, e''_{\lambda,2}, \cdots)$ (cf. Notation 7.5) and that there exists $n_\lambda$ irreducible components of $V_2$ which are mapped by $\varphi$ to $W_\lambda$. Then, we write

$$\begin{aligned}(p^2 - 1)/4 &= n_1(G_1;\, e'_{1,1}, e'_{1,2}, \cdots;\, e''_{1,1}, e''_{1,2}, \cdots)\\ &\quad + \cdots + n_{H'}(G_{H'};\, e'_{H',1}, e'_{H',2} \cdots;\, e''_{H',1}, e''_{H',2}, \cdots).\end{aligned}$$

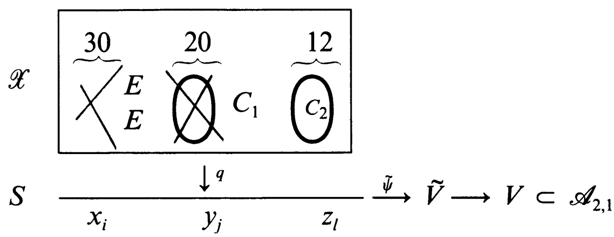
We have

$$(p^2 - 1)/4 = \sum_{\lambda=1}^{H'} n_\lambda \text{ and } n_\lambda|G_\lambda| = |S_6| = 720.$$

By Remark 5.9, Lemmas 7.2, 7.8, 7.9, 7.11, and Formulas (8.3) and (8.4), we have the following examples (4), (5), (6), (7), (8) and (9).

(4) $p = 7$

$$(p^2 - 1)/4 = 12 = 12(A_5; 2; 3, 5).$$




$$\deg \tilde{\psi} = 60.$$

$$E\colon Y^2 = X^3 - X,$$

$$C_1\colon Y^2 = X(X^2 - 1)(X^2 + 1),\ RA(C_1) \simeq S_4,$$

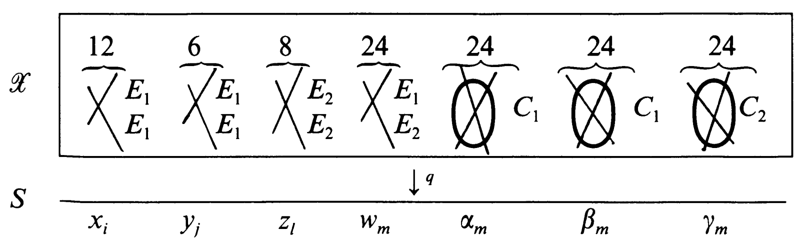
$$C_2\colon Y^2 = X^5 - 1,\ RA(C_2) \simeq \mathbb{Z}/5.$$

We set $\tilde{\psi}(x_i) = x\ (1 \leqslant i \leqslant 30)$, $\tilde{\psi}(y_j) = y\ (1 \leqslant j \leqslant 20)$, $\tilde{\psi}(z_l) = z\ (1 \leqslant l \leqslant 12)$.

$$G \simeq A_5;\ |G_x| = 2,\ |G_y| = 3,\ |G_z| = 5.$$

(5) $p = 11$

$$(p^2 - 1)/4 = 30 = 30(S_4; 2, 3, 4; -).$$




$$S \xrightarrow{\tilde{\psi}} \tilde{V} \longrightarrow V \subset \mathscr{A}_{2,1}$$

$\deg \tilde{\psi} = 24.$

$E_1\colon Y^2 = X^3 - X,$

$E_2\colon Y^2 = X^3 - 1,$

$C_1\colon Y^2 = (X^3 - 1)(X^3 - 3),\ RA(C_1) \simeq S_3,$

$C_2\colon Y^2 = X^6 - 1,\ RA(C_2) \simeq D_{12}.$

We set $\tilde{\psi}(x_i) = x$ $(1 \leqslant i \leqslant 12)$, $\tilde{\psi}(y_j) = y$ $(1 \leqslant j \leqslant 6)$, $\tilde{\psi}(z_l) = z$ $(1 \leqslant l \leqslant 8)$, $\tilde{\psi}(\alpha_m) = \alpha$, $\tilde{\psi}(\beta_m) = \beta$, $\tilde{\psi}(\gamma_m) = \gamma$ $(1 \leqslant m \leqslant 24)$.

$G \simeq S_4$; $|G_x| = 2$, $|G_y| = 4$, $|G_z| = 3$, $|G_w| = |G_\alpha| = |G_\beta| = |G_\gamma| = 1.$

We have $\hat{\psi}(\alpha) \neq \tilde{\psi}(\beta)$ and $\Psi \circ \tilde{\psi}(\alpha) = \Psi \circ \tilde{\psi}(\beta)$.

(6) $p = 13$

$(p^2 - 1)/4 = 42 = 12(A_5; -; 2, 3, 5) + 30(S_4; 2; 3, 4).$

(7) $p = 17$

$(p^2 - 1)/4 = 72 = 12(A_5; 3; 2, 5) + 60(D_{12}; 2, 6; 2).$

(8) $p = 19$

$(p^2 - 1)/4 = 90 = 30 + 60.$

By Lemma 7.8, $D_{12}$ does not appear. Hence, we have

$90 = 30(S_4; 2, 4; 3) + 60(A_4; 2; 3, 3).$

(9) $p = 23$

$(p^2 - 1)/4 = 132.$

We could not decide which of the two cases

$$\begin{aligned} 132 &= 12(A_4;\ 2,\ 3;\ 5) + 120(S_3;\ 2,\ 2,\ 3;\ -) \\ &= 72(D_{10};\ 2,\ 2;\ 5) + 60(A_4;\ 2,\ 3,\ 3;\ -) \end{aligned}$$

holds for this prime number.

(10) $p = 29$
Considering Lemma 7.8 and Table 4 in Section 7, we have two possibilities:

$$\begin{aligned} (p^2 - 1)/4 &= 210 \\ &= 60(D_{12};\ 2,\ 6;\ 2) + 30(S_4;\ 2,\ 3;\ 4) + 120(S_3;\ 3;\ 2,\ 2) \\ &= 60(D_{12};\ 2,\ 6;\ 2) + 90(D_8;\ 2;\ 2,\ 4) + 60(A_4;\ 3,\ 3;\ 2). \end{aligned}$$

LEMMA 8.8. *Assume $p = 29$. There exists up to isomorphism two supersingular curves of genus two with $RA(C) \simeq V_4$, and these two curves are conjugate with each other over the prime field $\mathbf{F}_{29}$.*

*Proof.* The zeros of the polynomial $h(X)$ which was introduced in [IKO, Definition 7.1] give all supersingular curves of type (3), (4) or (5) (cf. [IKO, Proposition 1.9]). In case $p = 29$, this polynomial is of degree seven. It is divisible by

$$(X + 1)(X - 9)(X - 13).$$

The curve with $\beta = -1$ is of type (5) and the curve with $\beta = 9$ or 13 is of type (4). A direct computation shows that for $p = 29$ we have

$$3h(X)/(X + 1)(X - 9)(X - 13) = X^4 - 3X^3 - X^2 - 3X + 1.$$

We can easily show that this polynomial is irreducible in $\mathbf{F}_{29}[X]$. Using zeros of this polynomial, we get two supersingular curves $C_1$, $C_2$ with $RA(C_1) = RA(C_2) \simeq V_2$ such that $C_1$ is not isomorphic to $C_2$ (cf. [IKO, Lemma 1.5]). Let $C_1$ (resp. $C_2$) be given by $\beta = \beta_1$ (resp. $\beta = \beta_2$) as in [IKO, Section 1.3]. Then $\beta_1$ is conjugate with $\beta_2$ over $\mathbf{F}_{29}$ as above. Thus, $C_1$ is conjugate with $C_2$ over $\mathbf{F}_{29}$. Q.E.D.

**Theorem 8.9.** *Assume $p = 29$. Then,*

$$210 = 60(D_{12}; 2, 6; 2) + 30(S_4; 2, 3; 4) + 120(S_3; 3; 2, 2).$$

*Proof.* Suppose

$$210 = 60(D_{12}; 2, 6; 2) + 90(D_8; 2; 2, 4) + 60(A_4; 3, 3; 2).$$

Under the notations in the proof of Lemma 8.8, curves $C_1$ and $C_2$ with $RA(C_i) \simeq V_4$ $(i = 1, 2)$ give $\mathbb{Z}/2$-ramifications. We denote by $\overline{\mathbb{F}}_{29}$ the algebraic closure of $\mathbb{F}_{29}$. The moduli space $\mathscr{A}_{2,1}$ is defined over $\mathbb{F}_{29}$ and the Galois group Gal $(\overline{\mathbb{F}}_{29}/\mathbb{F}_{29})$ operates. By Lemma 8.8, the point of $\mathscr{A}_{2,1}$ which corresponds to $(J(C_1), C_1)$ is transformed into the point which corresponds to $(J(C_2), C_2)$ by a suitable element of Gal $(\overline{\mathbb{F}}_{29}/\mathbb{F}_{29})$, which contradicts the fact that $C_1$ and $C_2$ belong to the different components with different groups. Q.E.D.

(11) $p = 31$
Considering Table 4 in Section 7, we conclude

$$\begin{aligned}(p^2 - 1)/4 &= 240 \\ &= 60(A_4; 2; 3, 3) + 60(A_4; 2; 3, 3) + 120(S_3; 2, 2; 3).\end{aligned}$$

*Remark 8.10.* We have no prime numbers for which we decided that one of the groups $D_{10}$, $D_8$, $V_4$ appears. In case $p \geqslant 7$ and the total number of branch points is not divisible by three (for example all prime numbers $p$ with $43 \leqslant p \leqslant 61$) it follows that from the groups $\mathbb{Z}/3$ and $\mathbb{Z}/2$ at least one of them appears.

*Remark 8.11.* The group $G = \{1\}$ appears for large $p$. If not, from (8.3) it would follow that

$$(p^2 - 1)/1440 \leqslant H' \leqslant (p^2 - 1)/48$$

by $2 \leqslant |G_\lambda| \leqslant 60$ for $\lambda = 1, 2, \cdots, H'$. The first inequality contradicts the asymptotic behavior of $H' = H_2(1, p)$ which has the leading term $(p^2 - 1)/2880$ (cf. Hashimoto and Ibukiyama [4, (II)]). Another way to show this fact, we calculate the total number of branch points. For example, in case $p \equiv 23 \pmod{24}$ and $|G_\lambda| \geqslant 2$ ($\lambda = 1, \cdots, H'$), then by Table 3 in Section 7 we have

$$(p + 1)/12 + (p + 1)/8 \geqslant 2H' \geqslant (p^2 - 1)/720,$$

a contradiction if $p \geqslant 167$.

*Remark 8.12.* We list in Table 5 some prime numbers where the group $G$ appears.

*Table 5.*

$p = 2 \quad G \simeq A_5$

$p = 3 \quad G \simeq A_6$

$p = 5 \quad G \simeq PGL(2, \mathbf{F}_5)$

$p \geqslant 7$

| Group $G$ | $720/\lvert G\rvert$ | appears at $p$ |
|---|---|---|
| $A_5$ | 12 | 7, 13, 17, --- |
| $S_4$ | 30 | 11, 13, 19, 29, --- |
| $D_{12}$ | 60 | iff $p \equiv 5 \pmod{12}$ |
| $A_4$ | 60 | 19, 31, --- |
| $D_{10}$ | 72 | ? > Ibukiyama: NO 20-IV-'85 |
| $D_8$ | 90 | ? |
| $S_3$ | 120 | 29, 31, --- |
| $V_4$ | 180 | ? |
| $\mathbb{Z}/3$ | 240 | at 43, 47, 53, 59, 61, --- |
| $\mathbb{Z}/2$ | 360 | |
| $\{1\}$ | 720 | 167 etc. |

*Remark 8.13.* Professor T. Ibukiyama communicated that he could decide the possibility of $G$ and could also compute, up to isomorphism, the number of families $\mathscr{X} \to S$ as above with group $G$ for each $p$.

## Acknowledgement

Toshiyuki Katsura was partially supported by Z.W.O. (Netherlands Organization for the Advancement of Pure Research), "Moduli", 10-80-004.

## References


1. M. Deuring: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg* 14 (1941) 197–272.
2. M. Eichler: Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.* 43 (1938) 102–109.
3. T. Ekedahl: *On supersingular curves and abelian varieties.* Prépublications Univ. de Paris-Sud, Orsay (1985).
4. K. Hashimoto and T. Ibukiyama: On the class numbers of positive definite binary quaternion hermitian forms (I). *J. Fac. Sci. Univ. Tokyo* sect. IA, 27 (1980), 549–601 (II) ibid. 28 (1981) 695–699.
5. T. Ibukiyama, T. Katsura and F. Oort: Supersingular curves of genus two and class numbers. *Comp. Math.* 57 (1986) 127–152.
6. J. Igusa: Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A.* 44 (1958) 312–314.
7. J. Igusa: Arithmetic variety of moduli for genus two. *Ann. of Math.* 72 (1960) 612–649.
8. T. Katsura and F. Oort: Supersingular abelian varieties of dimension two or three and class numbers. To appear in *Advanced Studies in Pure Math.*
9. N. Koblitz: $p$-adic variation of the zeta-function over families defined over finite fields. *Comp. Math.* 31 (1975) 119–218.
10. L. Moret-Bailly: Polarizations de degré 4 sur les surfaces abéliennes. *C.R. Acad. Sci. Paris* 289 (1979) 787–790.
11. L. Moret-Bailly: Familles de courbes et de variétés abéliennes sur $\mathbf{P}^1$. *Astérisque* 86 (1981) 109–140.
12. D. Mumford: *Abelian varieties.* Oxford Univ. Press (1970).
13. D. Mumford and J. Fogarty: *Geometric invariant theory* (second enlarged edition). Berlin–Heidelberg–New York: Springer-Verlag (1982).
14. M.N. Narasimhan and M.V. Nori: Polarizations on an abelian variety. *Geometry and analysis, Indian Acad. Sci. Bangalore* (1980) 125–128.
15. F. Oort: Subvarieties of moduli spaces. *Invent. Math.* 24 (1974) 95–119.
16. F. Oort: Which abelian surfaces are products of elliptic curves? *Math. Ann.* 214 (1975) 35–47.
17. H. Pinkham: Singularités de Klein, I. In Séminaire sur les singularités des surfaces. *Lecture Notes in Math.* 777, pp. 1–9. Berlin–Heidelberg–New York: Springer-Verlag (1980).
18. G. Shimura: Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan* 15 (1963) 33–65.
19. T. Shioda: Supersingular $K3$ surfaces. *Lecture Notes in Math.* 732, pp. 564–591. Berlin–Heidelberg–New York: Springer-Verlag (1979).
20. W.C. Waterhouse: Abelian varieties over finite fields. *Ann. Sci. Éc. Norm. Sup. 4^e série*, t.2 (1969) 521–560.
21. A. Weil: Zum Beweis des Torellischen Satzes. *Nachr. Acad. Wiss. Göttingen Math. Phys.* Kl (1957) 33–53.