MASS FORMULA AND OORT'S CONJECTURE FOR SUPERSINGULAR ABELIAN THREEFOLDS

VALENTIJN KAREMAKER, FUETARO YOBUKO, AND CHIA-FU YU

ABSTRACT. Using the theory of polarised flag type quotients, we determine mass formulae for all principally polarised supersingular abelian threefolds defined over an algebraically closed field k of characteristic p. We combine these results with computations of the automorphism groups to study Oort's conjecture; we prove that every generic three-dimensional principally polarised supersingular abelian variety over k of characteristic $\neq 2$ has automorphism group $\{\pm 1\}$.

1. INTRODUCTION

Throughout the paper, let p be a prime number, and let k be an algebraically closed field of characteristic p. An abelian variety X over k is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves; it is called *superspecial* if it is isomorphic to a product of supersingular elliptic curves. To each polarised supersingular abelian variety $x = (X_0, \lambda_0)$ of p-power polarisation degree, we associate a set Λ_x of isomorphism classes of p-power degree polarised abelian varieties (X, λ) over k, consisting of those whose associated quasi-polarised p-divisible groups satisfy $(X, \lambda)[p^\infty] \simeq (X_0, \lambda_0)[p^\infty]$. It is known that Λ_x is a finite set, and the *mass* of Λ_x is defined to be the weighted sum

$$\mathrm{Mass}(\Lambda_x) := \sum_{(X,\lambda)\in\Lambda_x} \frac{1}{|\mathrm{Aut}(X,\lambda)|}. \tag{1}$$

If $x = (X_0, \lambda_0)$ is a g-dimensional principally polarised superspecial abelian variety, then Λ_x coincides with the set $\Lambda_{g,1}$ of isomorphism classes of *all* principally polarised superspecial abelian varieties, called the *principal genus*. The classical mass formula (see Hashimoto-Ibukiyama [5, Proposition 9] and Ekedahl [2, p. 159]) states that

$$\mathrm{Mass}(\Lambda_g) = \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{i=1}^{g} \zeta(1-2i) \right\} \cdot \prod_{i=1}^{g} \left\{ (p^i + (-1)^i \right\}, \tag{2}$$

where $\zeta(s)$ denotes the Riemann zeta function.

More generally, for any integer c with $0 \le c \le \lfloor g/2 \rfloor$, let Λ_{g,p^c} denote the finite set of isomorphism classes of g-dimensional polarised superspecial abelian varieties (X, λ) such that $\ker(\lambda) \simeq \alpha_p^{2c}$, where α_p is kernel of the Frobenius morphism on the additive group $\mathbb{G}_a$. Then one also has $\Lambda_{g,p^c} = \Lambda_x$ for any member x in Λ_{g,p^c}. The case $c = \lfloor g/2 \rfloor$ is called the *non-principal genus*. As shown by Li-Oort [12], both the principal and non-principal genera describe the irreducible components of the Siegel supersingular locus $\mathscr{S}_{g,1} \subseteq \mathscr{A}_g \otimes \overline{\mathbb{F}}_p$, where $\mathscr{A}_g$ is the moduli space of g-dimensional principally polarised abelian varieties. Similarly, the sets Λ_{g,p^c} describe the supersingular Ekedahl-Oort (EO) strata in $\mathscr{A}_g \otimes \overline{\mathbb{F}}_p$, cf. [3]. The explicit determination of the class number $|\Lambda_{g,p^c}|$, i.e., the class number problem, is a very difficult task for large g, and is still open for $g = 3$ and $c = 1$. Nevertheless, an explicit calculation of the mass $\mathrm{Mass}(\Lambda_{g,p^c})$ is more accessible and provides a good estimate for the class number. This

Date: February 26, 2020.

mass was calculated explicitly by the third author [21, Theorem 1.4] when $g = 2c$ and extended to arbitrary g and c by Harashita [3, Proposition 3.5.2].

In [7], Ibukiyama resumes his earlier unpublished results of non-equivalent principal polarisations of a supersingular abelian surface X_0. He explicitly computes the number of polarisations and the mass of the principally polarised surfaces, and shows the agreement with $|\Lambda_x|$ and $\mathrm{Mass}(\Lambda_x)$, respectively, for a member $x = (X_0, \lambda_0)$ in $S_{2,1}$. As a surprising arithmetic application, Ibukiyama proved Oort's conjecture that the automorphism group of any generic member is C_2 for $g = 2$ and $p \geq 3$, and he gave a counterexample for $g = 2$ and $p = 2$.

Inspired by Ibukiyama's work, in this paper we explore the possibility of explicit determination of $\mathrm{Mass}(\Lambda_x)$ when $g = 3$, with similar arithmetic applications in mind. To describe our results, we need some notation; more details wil be given in Sections 2 and 3.

For any abelian variety X over k, the *a-number* of X is $a(X) := \dim_k \mathrm{Hom}(\alpha_p, X)$. For abelian threefolds X we have $a(X) \in \{1, 2, 3\}$; when computing the mass, we will separate into cases based on the a-number.

Further let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ with Frobenius endomorphism $\pi_E = -p$, and let $\overline{E} = E \otimes_{\mathbb{F}_{p^2}} k$. For each integer c with $0 \leq c \leq \lfloor g/2 \rfloor$, we denote by $P_{p^c}(\overline{E^3})$ the set of polarisations μ on $\overline{E^3}$ such that $\ker\mu \simeq \alpha_p^{2c}$; one has $P_{p^c}(\overline{E^3}) = P_{p^c}(E^3)$. As superspecial abelian threefolds are unique up to isomorphism, there is a natural bijection $P_{p^c}(\overline{E^3}) \simeq \Lambda_{g,p^c}$.

Let μ be a polarisation in $P_1(\overline{E}^3)$. As alluded to above, Li and Oort [12] show there is a one-to-one natural correspondence between the set $P_1(\overline{E^3})$ and the set $\Sigma(\mathscr{S}_{3,1})$ of (geometrically) irreducible components of $\mathscr{S}_{3,1}$. More precisely, they consider the moduli space $\mathscr{P}_\mu$ (resp. $\mathscr{P}'_\mu$) over $\mathbb{F}_{p^2}$ of three-dimensional (resp. rigid) polarised flag type quotients with respect to μ. This space is an irreducible scheme which comes with a proper projection morphism $\mathrm{pr}_0 : \mathscr{P}_\mu \to \mathscr{S}_{3,1}$, such that for each principally polarised supersingular abelian threefold (X, λ) there exists a $\mu \in P_1(\overline{E}^3)$ and a $y \in \mathscr{P}_\mu$ such that $\mathrm{pr}_0(y) = [(X, \lambda)] \in \mathscr{S}_{3,1}$.

Let $C \subseteq \mathbb{P}^2$ be the Fermat curve of degree $p+1$ defined by the equation $X_1^{p+1} + X_2^{p+1} + X_3^{p+1} = 0$. There exists a structure morphism $\pi : \mathscr{P}_\mu \simeq \mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1)) \to C$ that has a section $s : C \xrightarrow{\sim} T \subseteq \mathscr{P}_\mu$, giving $\mathscr{P}_\mu$ the structure of a $\mathbb{P}^1$-bundle over C, cf. [12, Section 9.4] and Definition 3.10. In particular, for each choice of μ and (X, λ), corresponding to a $y \in \mathscr{P}_\mu$, there exists a unique pair (t, u) where $t = (t_1 : t_2 : t_3) \in C(k)$ and $u = (u_1 : u_2) \in \pi^{-1}(t) \simeq \mathbb{P}^1_t(k)$ that characterises it. Moreover, we have (cf. Proposition 3.11):

(1) If $y \in T$ then $a(X) = 3$;
(2) For any $t \in C(k)$, we have $t \in C(\mathbb{F}_{p^2})$ if and only if for any $y \in \pi^{-1}(t)$ the corresponding threefold X has $a(X) \geq 2$.
(3) We have $a(X) = 1$ if and only if $y \notin T$ and $\pi(y) \notin C(\mathbb{F}_{p^2})$.

We are now ready to state our first two main results, computing the mass for any principally polarised supersingular abelian threefold.

Theorem A. *(Theorem 4.3) Let $x = (X, \lambda) \in \mathscr{S}_{3,1}(k)$ with $a(X) \geq 2$, let $\mu \in P_1(E^3)$, and let $y \in \mathscr{P}'_\mu(k)$ be such that* $\mathrm{pr}_0(y) = [(X, \lambda)]$. *Write $y = (t, u)$ where $t = \pi(y) \in C(\mathbb{F}_{p^2})$ and $u \in \pi^{-1}(t) \simeq \mathbb{P}^1_t(k)$. Then*

$$\mathrm{Mass}(\Lambda_x) = \frac{L_p}{2^{10} \cdot 3^4 \cdot 5 \cdot 7},$$

where

$$L_p = \begin{cases} (p-1)(p^2+1)(p^3-1) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ (p-1)(p^3+1)(p^3-1)(p^4-p^2) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ 2^{-e(p)}(p-1)(p^3+1)(p^3-1)p^2(p^4-1) & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}); \end{cases}$$

where $e(p) = 0$ *if* $p = 2$ *and* $e(p) = 1$ *if* $p > 2$.

Theorem B. *(Theorem 5.21) Let* $x = (X, \lambda) \in \mathscr{S}_{3,1}$ *such that* $a(X) = 1$. *For* $\mu \in P^1(E^3)$, *consider the associated element* $y \in \mathscr{P}_\mu$ *which is characterised by the pair* (t, u) *with* $t \in C(k) \setminus C(\mathbb{F}_{p^2})$ *and* $u \in \mathbb{P}^1_t(k)$. *Let* D_t *be as in Definition 5.16, and let* $d(t)$ *be as in Definition 5.12. Then*

$$\mathrm{Mass}(\Lambda_x) = \frac{p^3 L_p}{2^{10} \cdot 3^4 \cdot 5 \cdot 7},$$

where

$$L_p = \begin{cases} 2^{-e(p)} p^{2d(t)}(p^2-1)(p^4-1)(p^6-1) & \text{if } u \notin D_t; \\ p^{2d(t)}(p-1)(p^4-1)(p^6-1) & \text{if } t \notin C(\mathbb{F}_{p^6}) \text{ and } u \in D_t; \\ p^6(p^2-1)(p^3-1)(p^4-1) & \text{if } t \in C(\mathbb{F}_{p^6}) \text{ and } u \in D_t. \end{cases}$$

Our computations of the automorphism groups can be summarised as follows.

Theorem C. *Let* $x = (X, \lambda) \in \mathscr{S}_{3,1}(k)$ *and* $\mu \in P_1(E^3)$. *Consider the associated element* $y \in \mathscr{P}_\mu$ *which is characterised by the pair* (t, u) *with* $t \in C(k)$ *and* $u \in \mathbb{P}^1_t(k)$. *Let* D_t *be as in Definition 5.16 and let* $d(t)$ *be as in Definition 5.12.*

(1) *(Theorem 7.3.) Suppose that* $a(X) = 1$, *so that* $t \in C(k) \setminus C(\mathbb{F}_{p^2})$. *Assume that* $(t, u) \notin D$, *that is,* $u \notin D_t$.
  (a) *If* $p = 2$, *then* $\mathrm{Aut}(X, \lambda) \simeq C_2^3$.
  (b) *If* $p \geq 5$, *or* $p = 3$ *and* $d(t) = 6$, *then* $\mathrm{Aut}(X, \lambda) \simeq C_2$.
(2) *(Theorem 7.8.) Suppose that* $a(X) = 1$ *and that* $(t, u) \in D$ *with* $t \notin C(\mathbb{F}_{p^6})$.
  (a) *If* $p = 2$, *then* $\mathrm{Aut}(X, \lambda) \simeq C_2^3 \times C_3$.
  (b) *If* $p = 3$ *and* $d(t) = 6$, *then* $\mathrm{Aut}(X, \lambda) \in \{C_2, C_4\}$.
  (c) *For* $p \geq 5$, *we have the following cases:*
    (i) *If* $p \equiv -1 \pmod 4$, *then* $\mathrm{Aut}(X, \lambda) \in \{C_2, C_4\}$.
    (ii) *If* $p \equiv -1 \pmod 3$, *then* $\mathrm{Aut}(X, \lambda) \in \{C_2, C_6\}$.
    (iii) *If* $p \equiv 1 \pmod{12}$, *then* $\mathrm{Aut}(X, \lambda) \simeq C_2$.
(3) *(Proposition 7.11.) Let* $\Lambda_{3,1}(C_2) := \{(X, \lambda) \in \Lambda_{3,1} : \mathrm{Aut}(X, \lambda) \simeq C_2\}$ *be the set of superspecial principally polarised abelian threefolds satisfying Oort's conjecture. Then*

$$\frac{|\Lambda_{3,1}(C_2)|}{|\Lambda_{3,1}|} \to 1 \quad \text{as } p \to \infty.$$

In particular, Part (1) of Theorem C shows that Oort's conjecture is true precisely for $p \neq 2$. That is, every generic principally polarised supersingular abelian threefold over k of characteristic $\neq 2$ has automorphism group C_2.

The organisation of the paper is as follows. Sections 2 and 3 contain preliminaries, respectively on mass formulae and the structure of the supersingular locus $\mathscr{S}_{3,1}$. In particular, the strategy we will follow in later sections to obtain mass formulae is outlined at the end of Section 2. Sections 4 and 5 determine the mass formulae for supersingular abelian threefolds X, respectively with $a(X) = 2$ (cf. Theorem A) and $a(X) = 1$ (cf. Theorem B). Section 6 is an independent section which considers in more detail a set-theoretic intersection arising in Section 5. The automorphism groups, as well as the implications for Oort's conjecture, are studied in Section 7 (cf. Theorem C).

ACKNOWLEDGEMENTS

Parts of this work were carried out when the first author visited the Academia Sinica, and when the first and third authors visited RIMS and Kyoto University. They would like to thank these institutes for their hospitality and excellent working conditions. A part of this paper is contained in the second author's master's thesis written at Tohoku University; he thanks his advisor Nobuo Tsuzuki for enlightening comments, advice and encouragement. The authors are grateful to Ming-Lun Hsieh and Akio Tamagawa for useful discussions, and for proving Propositions 6.2 and 6.3, respectively. They would like to thank Tomoyoshi Ibukiyama and Jiangwei Xue for useful discussions. The second author is supported by JSPS grants 15J05073 and 19K14501. The third author is partially supported by MoST grant 107-2115-M-001-001-MY2.

2. MASS FORMULAE FOR SUPERSINGULAR ABELIAN VARIETIES

2.1. **Set-up and notation.**

Throughout the paper, let p be a prime number, let g be a positive integer, and let k be an algebraically closed field of characteristic p. The ground field for objects studied is k, unless stated otherwise.

For a finite set S, write $|S|$ for the cardinality of S. Let α_p be the unique α-group of order p over $\mathbb{F}_p$; it is defined to be the kernel of the Frobenius morphism on the additive group $\mathbb{G}_a$ over $\mathbb{F}_p$. For a matrix $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(k)$ and integer r, write $A^{(p^r)} := (a_{ij}^{p^r})$ for the image of A under the rth Frobenius map. Denote by $\widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ the profinite completion of $\mathbb{Z}$ and by $\mathbb{A}_f = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ the finite adele ring of $\mathbb{Q}$.

Definition 2.1. For any integer $d \geq 1$, let $\mathscr{A}_{g,d}$ denote the (coarse) moduli space over $\overline{\mathbb{F}}_p$ of g-dimensional polarised abelian varieties (X,λ) with polarisation degree $\deg\lambda = d^2$. For any $m \geq 1$, let S_{g,p^m} be the supersingular locus of $\mathscr{A}_{g,p^m}$, which consists of all polarised supersingular abelian varieties in $\mathscr{A}_{g,p^m}$. Then $\mathscr{S}_{g,1}$ is the moduli space of g-dimensional principally polarised supersingular abelian varieties. Denote $\mathscr{S}_{g,p^*} = \cup_{m\geq 1}\mathscr{S}_{g,p^m}$.

Definition 2.2. (1) If S is a finite set of objects with finite automorphism groups in a specified category, then we define the *mass* of S to be the weighted sum

$$\mathrm{Mass}(S) := \sum_{s\in S} \frac{1}{|\mathrm{Aut}(s)|}.$$

(2) For any $x = (X_0, \lambda_0) \in \mathscr{S}_{g,p^*}(k)$, we define

$$\Lambda_x = \{(X,\lambda) \in \mathscr{S}_{g,p^*}(k) : (X,\lambda)[p^\infty] \simeq (X_0,\lambda_0)[p^\infty]\}, \tag{3}$$

where $(X,\lambda)[p^\infty]$ denotes the polarised p-divisible group associated to (X,λ). Then Λ_x is a finite set; see [20, Theorem 2.1]. The *mass* of Λ_x is defined as

$$\mathrm{Mass}(\Lambda_x) = \sum_{(X,\lambda)\in\Lambda_x} \frac{1}{|\mathrm{Aut}(X,\lambda)|}.$$

2.2. **Superspecial mass formulae.**

Recall that a superspecial abelian variety over k is an abelian variety isomorphic to a product of supersingular elliptic curves.

Definition 2.3. Let $0 \le c \le \lfloor g/2 \rfloor$ be an integer. We define Λ_{g,p^c} to be the set of isomorphism classes of g-dimensional superspecial polarised abelian varieties (X, λ) whose polarisation λ satisfies $\ker(\lambda) \simeq \alpha_p^{2c}$. Its mass is

$$\mathrm{Mass}(\Lambda_{g,p^c}) = \sum_{(X,\lambda)\in\Lambda_{g,p^c}} \frac{1}{|\mathrm{Aut}(X,\lambda)|}.$$

If $x = (X, \lambda)$ is any member in Λ_{g,p^c}, then we have $\Lambda_x = \Lambda_{g,p^c}$ (cf. Definition 2.2). In particular, $\mathrm{Mass}(\Lambda_{g,p^c})$ is a special case of $\mathrm{Mass}(\Lambda_x)$. Note that the p-divisible group of a superspecial abelian variety of given dimension is unique up to isomorphism. Furthermore, the polarised p-divisible group associated to any member in Λ_{g,p^c} is unique up to isomorphism, cf. [12, Proposition 6.1].

Theorem 2.4. (1) *For any $g \ge 1$, we have*

$$\mathrm{Mass}(\Lambda_{g,1}) = \frac{(-1)^{g(g+1)/2}}{2^g} \prod_{i=1}^{g} \zeta(1-2i) \cdot \prod_{i=1}^{g} (p^i + (-1)^i).$$

(2) *For any $g \ge 1$ and $0 \le c \le \lfloor g/2 \rfloor$, we have*

$$\mathrm{Mass}(\Lambda_{g,p^c}) = \frac{(-1)^{g(g+1)/2}}{2^g} \prod_{i=1}^{g} \zeta(1-2i) \cdot \prod_{i=1}^{g-2c} (p^i + (-1)^i) \cdot \prod_{i=1}^{c} (p^{4i-2} - 1) \cdot \frac{\prod_{i=1}^{g} (p^{2i}-1)}{\prod_{i=1}^{2c}(p^{2i}-1) \prod_{i=1}^{g-2c}(p^{2i}-1)}.$$

Proof. (1) See [2, p. 159] and [5, Proposition 9]. (2) This follows from [3, Proposition 3.5.2] by the functional equation for $\zeta(s)$. See also [21] for a geometric proof in the case where $g = 2c$. □

Using the fact that $\zeta(-1) = -1/12, \zeta(-3) = 1/120$ and $\zeta(-5) = -1/(42 \cdot 6)$, we obtain the following corollary.

Corollary 2.5. *Let $g = 3$.*

(1) *If $c = 0$, then $\Lambda_{g,p^c} = \Lambda_{3,1}$ consists of all principally polarised superspecial abelian threefolds, and*

$$\mathrm{Mass}(\Lambda_{3,1}) = \frac{(p-1)(p^2+1)(p^3-1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}. \tag{4}$$

(2) *If $c = 1$, then $\Lambda_{g,p^c} = \Lambda_{3,p}$ consists of all polarised superspecial abelian threefolds whose polarisation λ has $\ker(\lambda) \simeq \alpha_p \times \alpha_p$, and*

$$\mathrm{Mass}(\Lambda_{3,p}) = \frac{(p-1)(p^3+1)(p^3-1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}. \tag{5}$$

2.3. **From superspecial to supersingular mass formulae.**

For a (not necessary principally) polarised supersingular abelian variety $x = (X_0, \lambda_0)$ over k, let G_x be the automorphism group scheme over $\mathbb{Z}$ associated to x ; for any commutative ring R, the group of its R-valued points is defined by

$$G_x(R) = \{g \in (\mathrm{End}(X_0) \otimes_{\mathbb{Z}} R)^\times : g^T \lambda_0 g = \lambda_0\}. \tag{6}$$

Definition 2.6. For a connected reductive group G over $\mathbb{Q}$ with finite arithmetic subgroups and an open compact subgroup $U \subseteq G(\mathbb{A}_f)$, we define its (arithmetic) mass $\mathrm{Mass}(G, U)$ by

$$\mathrm{Mass}(G,U) = \sum_{i=1}^{h} \frac{1}{|\Gamma_i|}, \quad \Gamma_i := G(\mathbb{Q}) \cap c_i U c_i^{-1},$$

where $\{c_1, \cdots, c_h\}$ is a set of representatives for the double coset space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U$.

Proposition 2.7. *For any object $x = (X_0, \lambda_0) \in S_{g,p^*}(k)$, there is a natural bijection of pointed sets*

$$\Lambda_x \simeq G_x(\mathbb{Q})\backslash G_x(\mathbb{A}_f)/G_x(\widehat{\mathbb{Z}}).$$

Moreover, if (X, λ) is a member of Λ_x which corresponds to the class $[c]$ under the bijection, then $\mathrm{Aut}(X, \lambda) \simeq G_x(\mathbb{Q}) \cap cG_x(\widehat{\mathbb{Z}})c^{-1}$. In particular, we have

$$\mathrm{Mass}(\Lambda_x) = \mathrm{Mass}(G_x, G_x(\widehat{\mathbb{Z}})),$$

cf. Definition 2.2.

Proof. See [23, Theorems 2.2 and 4.6]. Also see [25, Proposition 2.1] for a proof sketch. □

Definition 2.8. Let U_1, U_2 be two open compact subgroups of $G_x(\mathbb{A}_f)$. Then we define

$$\mu(U_1/U_2) = \frac{[U_1 : U_1 \cap U_2]}{[U_2 : U_1 \cap U_2]}.$$

Interpreting the mass from Definition 2.6 as the volume of a fundamental domain, with notation as above, we have the following lemma.

Lemma 2.9. *Let U_1, U_2 be two open compact subgroups of $G_x(\mathbb{A}_f)$. Then their (arithmetic) masses compare as*

$$\mathrm{Mass}(G_x, U_2) = \mu(U_1/U_2)\mathrm{Mass}(G_x, U_1).$$

Lemma 2.10. *Let X be a supersingular abelian variety over k. Then there exists a pair (Y, φ), where Y is a superspecial abelian variety and $\varphi : Y \to X$ is an isogeny such that for any pair (Y', φ') as above there exists a unique isogeny $\rho : Y' \to Y$ such that $\varphi' = \varphi \circ \rho$.*

Dually, there exists a pair (Z, γ), where Z is a superspecial abelian variety and $\gamma : X \to Z$ such that for any pair (Z', γ') as above there exists a unique isogeny $\rho : Z \to Z'$ such that $\gamma' = \rho \circ \gamma$.

Proof. See [12, Lemma 1.8]; also see [22, Corollary 4.3] for an independent proof. The proof of [12, Lemma 1.8] contains a gap; see Remark 3.13 for a counterexample to the argument. □

Definition 2.11. Let X be a supersingular abelian variety over k. We call the pair $(Y, \varphi : Y \to X)$ or the pair $(Z, \gamma : X \to Z)$ as in Lemma 2.10 *the minimal isogeny* of X.

Proposition 2.12. *Let $x = (X, \lambda) \in \mathscr{S}_{g,p^*}(k)$ and let $\varphi : \widetilde{X} \to X$ be the minimal isogeny of X. Put $\widetilde{x} = (\widetilde{X}, \widetilde{\lambda})$, where $\widetilde{\lambda} := \varphi^*\lambda$. Let $(M, \langle\, , \rangle), (\widetilde{M}, \langle\, , \rangle)$ denote the quasi-polarised (contravariant) Dieudonné module of $X, \widetilde{X}$, respectively. Then φ induces an injective map $\varphi^* : \mathrm{End}(X[p^\infty]) \hookrightarrow \mathrm{End}(\widetilde{X}[p^\infty])$, or equivalently $\varphi^* : \mathrm{End}(M) \hookrightarrow \mathrm{End}(\widetilde{M})$, and we have*

$$\begin{aligned} \mathrm{Mass}(\Lambda_x) &= [\mathrm{Aut}((\widetilde{X}, \widetilde{\lambda})[p^\infty]) : \mathrm{Aut}((X, \lambda)[p^\infty])] \cdot \mathrm{Mass}(\Lambda_{\widetilde{x}}) \\ &= [\mathrm{Aut}(\widetilde{M}, \langle\, , \rangle) : \mathrm{Aut}(M, \langle\, , \rangle)] \cdot \mathrm{Mass}(\Lambda_{\widetilde{x}}). \end{aligned} \tag{7}$$

Here the injective map φ^* yields the inclusion map $\mathrm{Aut}(M, \langle\, , \rangle) \subseteq \mathrm{Aut}(\widetilde{M}, \langle\, , \rangle)$.

Proof. This may be regarded as a refinement of [20, Theorem 2.7]. Through the isogeny φ, we may view $G_{\widetilde{x}}(\widehat{\mathbb{Z}})$ and $\varphi^* G_x(\widehat{\mathbb{Z}})$ as open compact subgroups of the same group $G_{\widetilde{x}}(\mathbb{A}_f)$. Using Proposition 2.7 and Lemma 2.9, we see that

$$\begin{aligned}\mathrm{Mass}(\Lambda_x) &= \mu(G_{\widetilde{x}}(\widehat{\mathbb{Z}})/\varphi^* G_x(\widehat{\mathbb{Z}}))\mathrm{Mass}(\Lambda_{\widetilde{x}}) \\ &= \frac{[G_{\widetilde{x}}(\widehat{\mathbb{Z}}) : G_{\widetilde{x}}(\widehat{\mathbb{Z}}) \cap \varphi^* G_x(\widehat{\mathbb{Z}})]}{[\varphi^* G_x(\widehat{\mathbb{Z}}) : G_{\widetilde{x}}(\widehat{\mathbb{Z}}) \cap \varphi^* G_x(\widehat{\mathbb{Z}})]}\mathrm{Mass}(\Lambda_{\widetilde{x}}).\end{aligned}$$

Note that $G_{\widetilde{x}}(\widehat{\mathbb{Z}})$ and $\varphi^* G_x(\widehat{\mathbb{Z}})$ differ only at p. By [22, Proposition 4.8], every endomorphism of $X[p^\infty]$ lifts uniquely to an endomorphism of $\widetilde{X}[p^\infty]$. This shows the injectivity of the map $\varphi^* : \mathrm{End}(X[p^\infty]) \to \mathrm{End}(\widetilde{X}[p^\infty])$. Therefore, we have the inclusion $G_x(\mathbb{Z}_p) = \mathrm{Aut}((X,\lambda)[p^\infty]) \hookrightarrow G_{\widetilde{x}}(\mathbb{Z}_p) = \mathrm{Aut}((\widetilde{X},\widetilde{\lambda})[p^\infty])$ via φ^* and find the first part of Equation (7).

By Dieudonné module theory, for any polarised supersingular abelian variety (X,λ) with quasi-polarised Dieudonné module $(M, \langle\, ,\rangle)$, we may identify $\mathrm{Aut}((X,\lambda)[p^\infty])$ with $\mathrm{Aut}(M, \langle\, ,\rangle)$. This yields Equation (7). □

To summarise, the results of this section provide the following strategy for obtaining a mass formula for any principally polarised supersingular abelian variety:

(a) For any supersingular abelian variety $x = (X,\lambda)$, construct the minimal isogeny $\varphi : (\widetilde{X},\widetilde{\lambda}) \to (X,\lambda)$ from a suitable superspecial abelian variety $\widetilde{x} = (\widetilde{X},\widetilde{\lambda})$.
(b) Use Theorem 2.4 (or Corollary 2.5 if $g = 3$) to compute $\mathrm{Mass}(\Lambda_{\widetilde{x}})$.
(c) Compute the local index $[\mathrm{Aut}(\widetilde{M}, \langle,\rangle) : \mathrm{Aut}((M, \langle,\rangle)]$, cf. (7).
(d) Compute $\mathrm{Mass}(\Lambda_x)$, i.e., compare $\mathrm{Mass}(\Lambda_{\widetilde{x}})$ and $\mathrm{Mass}(\Lambda_x)$ by applying Proposition 2.12.

We will carry out these steps, in particular Step (c), in the next sections in the case where $g = 3$. In the next section, we start by studying in detail the moduli space $\mathscr{S}_{3,1}$ of supersingular principally polarised abelian threefolds and the minimal isogenies (cf. Definition 2.11) between threefolds.

3. Structure of the supersingular locus $\mathscr{S}_{3,1}$

In this section we describe the supersingular locus $\mathscr{S}_{3,1}$. The structure will be used to determine the minimal isogenies, cf. Proposition 3.12. Finer structures will be introduced in order to compute the local index in Step (c) in the previous section.

3.1. **The moduli space $\mathscr{S}_{3,1}$.**

To describe the moduli space $\mathscr{S}_{3,1}$ of supersingular principally polarised abelian threefolds, we will use the framework of polarised flag type quotients (for $g = 3$) as developed by Li and Oort [12], which we will briefly describe below.

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve whose Frobenius endomorphism is $\pi_E = -p$ and denote $\overline{E} = E \otimes_{\mathbb{F}_{p^2}} k$. Let $P(\overline{E^3}) = P_1(\overline{E^3})$ (resp. $P(E^3) = P_1(E^3)$) be the set of isomorphism classes of principal polarisations on $\overline{E^3}$ (resp. E^3). Since every polarisation on $\overline{E^3}$ is defined over $\mathbb{F}_{p^2}$, we may identify $P(\overline{E^3})$ with $P(E^3)$. Recall that an α-group of rank r over an $\mathbb{F}_p$-scheme S is a finite flat group scheme over S which is Zariski-locally isomorphic to α_p^r. For a scheme X over S, put $X^{(p)} := X \times_{S,F_S} S$. where $F_S : S \to S$ denotes the absolute Frobenius morphism on S.

Definition 3.1. (cf. [12, Section 3])

(1) For any $\mu \in P(E^3)$, a *three-dimensional polarised flag type quotient (PFTQ)* with respect to μ is a chain of polarised abelian threefolds over a base $\mathbb{F}_{p^2}$-scheme S

$$(Y_\bullet, \rho_\bullet) : (Y_2, \lambda_2) \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_0, \lambda_0),$$

such that:

(i) $(Y_2, \lambda_2) = (E^3, p\mu) \times_{\operatorname{Spec} \mathbb{F}_{p^2}} S$;

(ii) $\ker(\rho_i)$ is an α-group of rank i for $1 \leq i \leq 2$;

(iii) $\ker(\lambda_i) \subseteq \ker(\mathsf{V}^j \circ \mathsf{F}^{i-j})$ for $0 \leq i \leq 2$ and $0 \leq j \leq \lfloor i/2 \rfloor$, where $\mathsf{F} = F_{Y_i/S} : Y_i \to Y_i^{(p)}$ and and $\mathsf{V} = V_{Y_i/S} : Y_i^{(p)} \to Y_i$ are the relative Frobenius and Verschiebung morphisms, respectively.

In particular, λ_0 is a principal polarisation on Y_0. An isomorphism of three-dimensional polarised flag type quotients is a chain of isomorphisms $(\alpha_i)_{0 \leq i \leq 2}$ of polarised abelian varieties such that $\alpha_2 = \mathrm{id}_{Y_2}$.

(2) A three-dimensional polarised flag type quotient $(Y_\bullet, \rho_\bullet)$ is said to be *rigid* if

$$\ker(Y_2 \to Y_i) = \ker(Y_2 \to Y_0) \cap Y_2[\mathsf{F}^{2-i}] = \ker(\mathsf{F}^{2-i} : Y_2 \to Y_2^{(p^{2-i})}), \quad \text{for } 1 \leq i \leq 2,$$

or equivalently if $\ker(\rho_2) = \ker(Y_2 \to Y_0) \cap Y_2[\mathsf{F}]$.

(3) Let $\mathscr{P}_\mu$ (resp. $\mathscr{P}'_\mu$) denote the moduli space over $\mathbb{F}_{p^2}$ of three-dimensional (resp. rigid) polarised flag type quotients with respect to μ.

Clearly, each member Y_i of $(Y_\bullet, \rho_\bullet)$ is a supersingular abelian threefold. According to [12, Section 9.4], $\mathscr{P}_\mu$ is a two-dimensional geometrically irreducible scheme over $\mathbb{F}_{p^2}$. The projection to the last member gives a proper $\overline{\mathbb{F}}_p$-morphism

$$\begin{aligned} \mathrm{pr}_0 : \mathscr{P}_\mu &\to \mathscr{S}_{3,1}, \\ (Y_2 \to Y_1 \to Y_0) &\mapsto (Y_0, \lambda_0). \end{aligned}$$

Moreover, for each principally polarised supersingular abelian threefold (X, λ) there exist a $\mu \in P(E^3)$ and a polarised flag type quotient $y \in \mathscr{P}_\mu$ such that $\mathrm{pr}_0(y) = [(X, \lambda)] \in \mathscr{S}_{3,1}$. Put differently, it holds that the morphism

$$\coprod_{\mu \in P(E^3)} \mathscr{P}_\mu \to \mathscr{S}_{3,1} \tag{8}$$

is surjective and generically finite.

Roughly speaking, Equation (8) says that each $\mathscr{P}_\mu$ approximates an irreducible component of the supersingular locus $\mathscr{S}_{3,1}$. More precisely, one can show the following structure results; for more details, we refer to [12, Sections 9.3-9.4].

Let $C \subseteq \mathbb{P}^2$ be the Fermat curve defined by the equation $X_1^{p+1} + X_2^{p+1} + X_3^{p+1} = 0$.

Proposition 3.2. *The Fermat curve C can be interpreted as the classifying space of isogenies $(Y_2, \lambda_2) \to (Y_1, \lambda_1)$ whose kernel is locally isomorphic to α_p^2. Moreover, there is an isomorphism $\mathscr{P}_\mu \simeq \mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1))$ for which the structure morphism $\pi : \mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1)) \to C$ corresponds to the forgetful map $((Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (Y_0, \lambda_0)) \mapsto ((Y_2, \lambda_2) \to (Y_1, \lambda_1))$.*

Proof. Let M_2 be the polarised contravariant Dieudonné module of Y_2. Choosing an isogeny ρ_2 from $\overline{E^3}$ such that $\ker(\rho_2) \simeq \alpha_p^2$ is equivalent to choosing a surjection of Dieudonné modules $M_2 \to k^2$. Since Frobenius F and Verschiebung V act as zero on k^2, this is further equivalent to choosing a one-dimensional subspace of the three-dimensional (since $a(Y_2) = 3$) k-vector space $M_2/(\mathsf{F}, \mathsf{V})M_2$ which corresponds to a point $(t_1 : t_2 : t_3) \in \mathbb{P}^2 = \mathbb{P}((M_2/(\mathsf{F}, \mathsf{V})M_2)^*)$.

The polarisation $\lambda_2 = p\mu$ descends to a polarisation λ_1 on Y_1 through such ρ_2, and the condition $\ker(\lambda_1) \subseteq Y_1[\mathsf{F}]$ is equivalent to the condition

$$t_1^{p+1} + t_2^{p+1} + t_3^{p+1} = 0,$$

which describes the Fermat curve C of degree $p+1$ in $\mathbb{P}^2$. For precise computations, we refer to [11].

Let M_1 be the polarised Dieudonné module of Y_1: the polarisation λ_1 induces a quasi-polarisation $D(\lambda_1)\colon M_1^\vee \to M_1$, and we regard $M_1^\vee$ as an submodule of M_1 under this injection. Choosing a second isogeny $(Y_1, \lambda_1) \to (Y_0, \lambda_0)$ is equivalent to choosing a one-dimensional subspace of the two-dimensional vector space $M_1/M_1^\vee$. Thus each fibre of the structure morphism $\pi\colon \mathscr{P}_\mu \to C$ is isomorphic to $\mathbb{P}((M_1/M_1^\vee)^*) \simeq \mathbb{P}^1$ and this fibration corresponds to a rank two vector bundle on C. The canonical one-dimensional space $(\mathsf{F}, \mathsf{V})M_2/M_1^\vee \subseteq M_1/M_1^\vee$ defines a section s of $\pi\colon \mathscr{P}_\mu \to C$ and corresponds to a surjection $\mathscr{P} \to \mathscr{O}(-1)$. By the duality of polarisations, we see that $\mathscr{P}$ is an extension of $\mathscr{O}(-1)$ by $\mathscr{O}(1)$ and this extension splits. □

Since the Fermat curve C is a smooth plane curve of degree $p+1$, its genus is equal to $p(p-1)/2$. Let $U_3(\mathbb{F}_p) \subseteq \mathrm{GL}_3(\mathbb{F}_{p^2})$ denote the unitary subgroup consisting of matrices A such that $A^T A^{(p)} = \mathbb{I}_3$. We see that for each $A \in U_3(\mathbb{F}_p)$ and $t \in C$, the matrix multiplication $A \cdot t^T$ lies in C. This gives a left action of $U_3(\mathbb{F}_p)$ on the curve C. It is known that $|U_3(\mathbb{F}_p)| = p^3(p+1)(p^2-1)(p^3+1)$.

Lemma 3.3. *We have $|C(\mathbb{F}_{p^2})| = p^3+1$. Thus, it is $\mathbb{F}_{p^2}$-maximal and hence $\mathbb{F}_{p^4}$-minimal. Moreover, we have $C(\mathbb{F}_{p^2}) = C(\mathbb{F}_{p^4})$. Furthermore, we have*

$$|C(\mathbb{F}_{p^{2i}})| = \begin{cases} p^{2i} + p^{i+2} - p^{i+1} + 1 & \text{if } i \text{ is odd;} \\ p^{2i} - p^{i+2} + p^{i+1} + 1 & \text{if } i \text{ is even.} \end{cases} \tag{9}$$

Proof. For each $t = (t_i) \in C(\mathbb{F}_{p^2})$, let $s_i = t_i^{p+1}$. Then $s_i \in \mathbb{F}_p$ and $s_1 + s_2 + s_3 = 0$. So there are $p+1$ points (s_i) in $\mathbb{P}^1(\mathbb{F}_p)$. For each point (s_i), there are $p+1$ (resp. $(p+1)^2$) points (t_i) over (s_i) if some of the s_i are zero (resp. otherwise); there are 3 points (s_i) with $s_i = 0$ for some i. Thus,

$$|C(\mathbb{F}_{p^2})| = (p+1-3)(p+1)^2 + 3(p+1) = p^3 + 1.$$

A curve is $\mathbb{F}_{p^{2k}}$-maximal (resp. minimal) if its Frobenius eigenvalues over $\mathbb{F}_{p^{2k}}$ all equal $-p^k$ (resp. p^k). One checks that this means C is $\mathbb{F}_{p^2}$-maximal. Hence, C is $\mathbb{F}_{p^4}$-minimal and satisfies $|C(\mathbb{F}_{p^4})| = p^3 + 1$. Since C is $\mathbb{F}_{p^{2i}}$-maximal (resp. $\mathbb{F}_{p^{2i}}$-minimal) if i is odd (resp. even), the formula (9) follows immediately. □

Lemma 3.4. *Let $t = (t_1 : t_2 : t_3) \in C(k)$. Then $t \in C(\mathbb{F}_{p^2})$ if and only if t_1, t_2, t_3 are linearly dependent over $\mathbb{F}_{p^2}$.*

Proof. See [15, Lemma 2.1]. Alternatively, we give the following independent proof:

The forward implication is immediate, so we will only show the reverse implication. Assume t_1, t_2, t_3 are linearly dependent over $\mathbb{F}_{p^2}$. Then there exist $a, b \in k$ such that $t_i = a t_i^{p^2} + b t_i^{p^4}$ for $i = 1, 2, 3$. Substituting this into the defining equation of C, we obtain

$$a^{p+1} \sum_{i=1}^{3} t_i^{p^2+p^3} + ab^p \sum_{i=1}^{3} t_i^{p^2+p^5} + a^p b \sum_{i=1}^{3} t_i^{p^3+p^4} + b^{p+1} \sum_{i=1}^{3} t_i^{p^4+p^5} = 0.$$

Again using the defining equation of C, we see that the first, third, and fourth terms vanish, so that also $ab^p \sum_{i=1}^3 t_i^{p^2+p^5} = ab^p (\sum_{i=1}^3 t_i^{p^3+1})^{p^2} = 0$. If $a = 0$ then the point $t = (t_1 : t_2 : t_3)$ is defined over $\mathbb{F}_{p^4}$ and hence, by Lemma 3.3, it is defined over $\mathbb{F}_{p^2}$. If $b = 0$, then t is defined over

$\mathbb{F}_{p^2}$ as well. So we may assume that $\sum_{i=1}^{3} t_i^{p^3+1} = 0$. Let $Z := V(X_1^{p^3+1} + X_2^{p^3+1} + X_3^{p^3+1})$ be the Fermat curve of degree p^3+1. Then $t \in C \cap Z$. The intersection number of C and Z is $(p+1)(p^3+1)$ and each point of $C(\mathbb{F}_{p^2})$ is in $C \cap Z$. Since $|C(\mathbb{F}_{p^2})| = p^3+1$ by Lemma 3.3, it is enough to show that for each point $s \in C(\mathbb{F}_{p^2})$, the local multiplicity of C and Z at s is $p+1$. Since the unitary group $U_3(\mathbb{F}_p)$ acts transitively on $C(\mathbb{F}_{p^2})$, we may assume that $s = (\zeta : 0 : 1)$ where $\zeta^{p+1} = -1$. With local coordinates $v = X_1 - \zeta$ and $w = X_2$, the respective equations for C and Z at y become $v^{p+1} + \zeta v^p + \zeta v + w^{p+1}$ and $v^{p^3+1} + \zeta v^{p^3} + \zeta^p v + w^{p^3+1}$. Now we may read off that the local multiplicity, i.e., the valuation of v at s, is $p+1$, as required. □

We will denote $C^0 := C \setminus C(\mathbb{F}_{p^2})$. Slightly abusively, we will tacitly switch between the notations (t_1, t_2, t_3) and $(t_1 : t_2 : t_3)$. For later use, we define the following:

Definition 3.5. For $t = (t_1, t_2, t_3) \in k^3$ (viewed as a column vector), let

$$\mathrm{End}(t) = \{A \in \mathrm{Mat}_3(\mathbb{F}_{p^2}) : A \cdot t \in k \cdot t\}.$$

Lemma 3.6. *For any $t \in C^0(k)$, the $\mathbb{F}_{p^2}$-algebra $\mathrm{End}(t)$ is isomorphic to either $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^6}$.*

Proof. For any $A \in \mathrm{End}(t)$, we have $A \cdot t = \alpha_A t$ for some $\alpha_A \in k$. The map

$$\begin{aligned} \mathrm{End}(t) &\to k \\ A &\mapsto \alpha_A \end{aligned}$$

is an $\mathbb{F}_{p^2}$-algebra homomorphism. It is injective, i.e., $A \cdot t = 0$ with $t = (t_1 : t_2 : t_3)$ implies that $A = 0$, since the t_i are linearly independent over $\mathbb{F}_{p^2}$ by Lemma 3.4. Hence, $\mathrm{End}(t)$ is a finite field extension of $\mathbb{F}_{p^2}$. Since $\mathrm{End}(t) \subseteq M_3(\mathbb{F}_{p^2}) = \mathrm{End}((\mathbb{F}_{p^2})^3)$, we may regard $(\mathbb{F}_{p^2})^3$ as a vector space over $\mathrm{End}(t)$. It follows that $[\mathrm{End}(t) : \mathbb{F}_{p^2}] \mid 3$, as required. □

Lemma 3.7. *We have*

$$CM := \{t \in C^0(k) : \mathrm{End}(t) \simeq \mathbb{F}_{p^6}\} = C^0(\mathbb{F}_{p^6}). \tag{10}$$

Proof. The containment $\{t \in C^0(k) : \mathrm{End}(t) \simeq \mathbb{F}_{p^6}\} \subseteq C^0(\mathbb{F}_{p^6})$ is immediate, because t is an eigenvector of a matrix in $\mathrm{Mat}_3(\mathbb{F}_{p^2})$ and can be solved over the ground field $\mathbb{F}_{p^6}$. We will now prove the reverse containment.

For each $t \in C^0(\mathbb{F}_{p^6})$, we construct for each element $\alpha \in \mathbb{F}_{p^6}$ a matrix $A \in \mathrm{Mat}_3(\mathbb{F}_{p^6})$ as follows

$$A = A_\alpha := (t, t^{(p^2)}, t^{(p^4)}) \cdot \mathrm{diag}(\alpha, \alpha^{p^2}, \alpha^{p^4}) \cdot (t, t^{(p^2)}, t^{(p^4)})^{-1}.$$

Since the t_i are linearly independent over $\mathbb{F}_{p^2}$ by Lemma 3.4, the matrix $(t, t^{(p^2)}, t^{(p^4)})$ is invertible. We check that

$$\begin{aligned} A^{(p^2)} &= (t^{(p^2)}, t^{(p^4)}, t) \cdot \mathrm{diag}(\alpha^{p^2}, \alpha^{p^4}, \alpha) \cdot (t^{(p^2)}, t^{(p^4)}, t)^{-1} \\ &= (t, t^{(p^2)}, t^{(p^4)}) \cdot \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \mathrm{diag}(\alpha^{p^2}, \alpha^{p^4}, \alpha) \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot (t, t^{(p^2)}, t^{(p^4)})^{-1} \\ &= A, \end{aligned}$$

and hence $A \in \mathrm{Mat}_3(\mathbb{F}_{p^2})$. We also have that $A_\alpha \cdot t = \alpha t$. Thus, the map $\alpha \in \mathbb{F}_{p^6} \mapsto A_\alpha$ gives an isomorphism $\mathbb{F}_{p^6} \simeq \mathrm{End}(t)$, as required. □

Remark 3.8.

(1) We can also show that $U_3(\mathbb{F}_p)$ acts transitively on $C^0(\mathbb{F}_{p^6}) = CM$. The action on $C(\mathbb{F}_{p^2})$ is also transitive, with stabilisers of size $p^3(p+1)(p^2-1)$; this gives another proof of the result $|C(\mathbb{F}_{p^2})| = p^3+1$.

(2) The proof of Lemma 3.6 proves the following more general result. Let F be any field contained in a field K and $t_1, t_2, \dots, t_n$ be a set of F-linearly independent elements in K. Put $t = (t_1, \dots, t_n)^T$ and $\mathrm{End}(t) := \{A \in \mathrm{Mat}_n(F) : A \cdot t \subseteq K \cdot t\}$. Then $\mathrm{End}(t)$ is a finite field extension of F of degree dividing n.
(3) The proof of Lemma 3.7 proves the following result in linear algebra: Let $t_1, \dots, t_n$ be a set of $\mathbb{F}_q$-linearly independent elements in k. Suppose that $t = (t_i) \in \mathbb{F}_{q^n}^n$. Then t is an eigenvector of a matrix in $\mathrm{Mat}_n(\mathbb{F}_q)$.

Definition 3.9. For an abelian variety X over k, its a-number is defined as

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

So for an abelian threefold X over k, we have $a(X) \in \{1, 2, 3\}$. For a Dieudonné module M over k, the a-number of M is defined as $a(M) := \dim(M/(\mathsf{F}, \mathsf{V})M)$. If M is the Dieudonné module of X, then $a(M) = a(X)$. When $x \in \mathscr{P}_\mu \simeq \mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1))$ corresponds to a polarised flag type quotient $((Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (Y_0, \lambda_0))$, we say that its a-number is $a(x) = a(Y_0)$.

Definition 3.10. The morphism $\pi : \mathscr{P}_\mu \to C$ admits a section s defined as follows. For a base scheme S, let $\rho_2 : (Y_2, p\mu) \to (Y_1, \lambda_1)$ be an object in $C(S)$. Put $(Y_2^{(p)}, \mu^{(p)}) := (Y, \mu) \times_{S, F_S} S$, where $F_S : S \to S$ is the absolute Frobenius map. The relative Frobenius morphism $\mathsf{F} : Y_2 \to Y_2^{(p)}$ gives rise to a morphism of polarised abelian schemes $\mathsf{F} : (Y_2, p\mu) \to (Y_2^{(p)}, \mu^{(p)})$. Since $\ker(\rho_2) \subseteq \ker(\mathsf{F})$, the morphism factors through an isogeny $\rho_1 : Y_1 \to Y_2^{(p)}$. As $\rho_2^* \rho_1^* \mu^{(p)} = \mathsf{F}^* \mu^{(p)} = p\mu = \rho_2^* \lambda_1$, we see that $\rho_1^* \mu^{(p)} = \lambda_1$ and thus obtain a polarised flag type quotient

$$(Y_2, p\mu) \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_2^{(p)}, \mu^{(p)}).$$

This defines the section s, whose image will be denoted by T.

Proposition 3.11. *Let the notation be as above.*
(1) *We have $\mathscr{P}'_\mu = \mathscr{P}_\mu - T$.*
(2) *If $x \in T$ then we have $a(x) = 3$.*
(3) *For any $t \in C(k)$, we have $t \in C(\mathbb{F}_{p^2})$ if and only if $a(x) \geq 2$ for any $x \in \pi^{-1}(t)$.*
(4) *For any $x \in \mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1))$, we have $a(x) = 1$ if and only if $x \notin T$ and $\pi(x) \notin C(\mathbb{F}_{p^2})$.*

Proof. See [12, Section 9.4]. □

3.2. **Minimal isogenies.**

Given a polarised flag type quotient $Y_2 = \overline{E}^3 \xrightarrow{\rho_2} Y_1 \xrightarrow{\rho_1} Y_0 = X$, the composite map $\rho_1 \circ \rho_2 : (Y_2, \lambda_2) \to (Y_0, \lambda_0) = (X, \lambda)$ is an isogeny from a superspecial abelian variety Y_2. Thus, this isogeny factors through the minimal isogeny of (X, λ):

$$(Y_2, \lambda_2) \xrightarrow{\rho_1 \circ \rho_2} (\widetilde{X}, \widetilde{\lambda}) \xrightarrow{\varphi} (X, \lambda).$$

Since every member $(X, \lambda) \in \mathscr{S}_{3,1}(k)$ can be constructed from a polarised flag type quotient $(Y_\bullet, \rho_\bullet)$, we can construct the minimal isogeny of (X, λ) from $(Y_\bullet, \rho_\bullet)$.

To describe the minimal isogenies for supersingular abelian threefolds in more detail, in the following proposition we separate into three cases, based on the a-number of the threefold.

Proposition 3.12. *Let (X, λ) be a supersingular principally polarised abelian threefold over k. Suppose that (X, λ) lies in the image of $\mathscr{P}'_\mu$ under the map $\mathscr{P}'_\mu \to \mathscr{S}_{3,1}$ for some $\mu \in P(E^3)$, so that there is a unique PFTQ over (X, λ).*
(1) *If $a(X) = 1$, then the associated polarised flag type quotient $(Y_2, \lambda_2) \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_0, \lambda_0) = (X, \lambda)$ gives the minimal isogeny $\varphi := \rho_1 \circ \rho_2$ of degree p^3.*

(2) *If $a(X) = 2$, then in the associated polarised flag type quotient $Y_2 = \overline{E}^3 \to Y_1 \to Y_0 = X$ we have $a(Y_1) = 3$, so Y_1 is superspecial. Thus, the minimal isogeny is $\rho_1 : (Y_1, \lambda_1) \to (X, \lambda)$ of degree p, where $\rho_1^* \lambda = \lambda_1$ satisfies $\ker(\lambda_1) \simeq \alpha_p \times \alpha_p$.*

(3) *If $a(X) = 3$, then X is superspecial. Thus, X is k-isomorphic to $\overline{E}^3$ and the minimal isogeny is the identity map.*

Proof. (1) Let M_2, M_1, M_0 denote the Dieudonné modules of $Y_2, Y_1, Y_0 = X$, respectively. Then $a(M_2) = 3$. Suppose that $a(M_0) = 1$. By Proposition 3.11, this corresponds to a point $t = (t_1 : t_2 : t_3) \notin C(\mathbb{F}_{p^2})$. We claim that $a(M_1) = 2$, which implies the statement. The Dieudonné modules satisfy the following inclusions:

$$\begin{array}{ccccccccc}
M_2 & \supseteq & M_1 & \supseteq & M_0 & & & & \\
& \rotatebox[origin=c]{-45}{$\supsetneq$} & \rotatebox[origin=c]{90}{$\subseteq$} & & \rotatebox[origin=c]{90}{$\subseteq$} & \rotatebox[origin=c]{-45}{$\supsetneq$} & & & \\
& & (\mathsf{F},\mathsf{V})M_2 & \supset & (\mathsf{F},\mathsf{V})M_1 & = & (\mathsf{F},\mathsf{V})M_0 & & \\
& & & \rotatebox[origin=c]{-45}{$\supsetneq$} & \rotatebox[origin=c]{90}{$\subseteq$} & \rotatebox[origin=c]{-45}{$\supsetneq$} & \rotatebox[origin=c]{90}{$\subseteq$} & \rotatebox[origin=c]{-45}{$\supsetneq$} & \\
& & & & (\mathsf{F},\mathsf{V})^2M_2 & = & (\mathsf{F},\mathsf{V})^2M_1 & = & (\mathsf{F},\mathsf{V})^2M_0.
\end{array}$$

All inclusions follow from the construction of flag type quotients. For the equalities, we note the following: Since M_2 is superspecial of genus three, we have $(\mathsf{F},\mathsf{V})M_2 = \mathsf{F}M_2, (\mathsf{F},\mathsf{V})^2 M_2 = pM_2$, and

$$\dim(M_2/\mathsf{F}M_2) = \dim(\mathsf{F}M_2/pM_2) = 3.$$

It follows from the definition of flag type quotients that $\dim(M_1/\mathsf{F}M_2) = 1$, so $M_1/\mathsf{F}M_2$ is generated by one element, namely the image of t (abusively again denoted t). So $(\mathsf{F},\mathsf{V})M_1/pM_2$ is two-dimensional and generated by the two elements $\mathsf{F}t$ and $\mathsf{V}t$, which are k-linearly independent since $t \notin C(\mathbb{F}_{p^2})$, by Lemma 3.4. Using this, we see that

$$\dim(\mathsf{F}M_2/(\mathsf{F},\mathsf{V})M_1) = \dim(\mathsf{F}M_2/pM_2) - \dim((\mathsf{F},\mathsf{V})M_1/pM_2) = 1$$

and $a(M_1) = \dim(M_1/(\mathsf{F},\mathsf{V})M_1) = 2$, as claimed. It follows from $\dim(M_1/M_0) = 1$ and $a(M_1) = 2$ that $\dim(M_0/(\mathsf{F},\mathsf{V})M_1) = 1$. As we have assumed that $a(M_0) = \dim(M_0/(\mathsf{F},\mathsf{V})M_0) = 1$, the latter implies the equality $(\mathsf{F},\mathsf{V})M_1 = (\mathsf{F},\mathsf{V})M_0$. Since $\dim(M_0/(\mathsf{F},\mathsf{V})M_1) = 1$ and $\dim(M_0/pM_2) = 2$, one has $\dim(\mathsf{F},\mathsf{V})M_1/pM_2) = 2$. Since t_1, t_2, t_3 are $\mathbb{F}_{p^2}$-linearly independent by Lemma 3.4, the vectors $\mathsf{F}^2 t, pt$ and $\mathsf{V}^2 t$ in $\mathsf{F}M_2/p\mathsf{F}M_3$ span a 3-dimensional subspace and hence $\dim((\mathsf{F},\mathsf{V})^2 M_1/p\mathsf{F}M_2) = 3$. This shows the equality $pM_2 = (\mathsf{F},\mathsf{V})^2 M_1 = (\mathsf{F},\mathsf{V})^2 M_0$.

Now put $\Phi := 1 + \mathsf{F}\mathsf{V}^{-1}$. We have shown that $\mathsf{V}\Phi M_0 = (\mathsf{F},\mathsf{V})M_1$ is not superspecial and that $\Phi^2 M_0 = pM_2$ is superspecial. Therefore, M_2 is the smallest superspecial Dieudonné module containing M_0. This proves that $\rho_1 \circ \rho_2 : Y_2 \to X$ is the minimal isogeny.

(2) When $a(M_0) = 2$, this corresponds to a point $t = (t_1 : t_2 : t_3) \in C(\mathbb{F}_{p^2})$. Using the notation from the previous item, we still have that $(\mathsf{F},\mathsf{V})M_1/pM_2$ is generated by $\mathsf{F}t$ and $\mathsf{V}t$, but since the t_i are $\mathbb{F}_{p^2}$-linearly dependent, we have $\dim((\mathsf{F},\mathsf{V})M_1/pM_2) = 1$, so $a(M_1) = 3$. Since $\ker(\lambda) \subseteq Y_1[F] \simeq \alpha_p^3$, we have $\ker(\lambda) \simeq \alpha_p^2$, as claimed.

(3) The fact that $a(X) = 3$ if and only if X is superspecial is due to Oort, [14, Theorem 2]. □

Remark 3.13. The proof of [12, Lemma 1.8] uses the claim: If X is a g-dimensional supersingular abelian variety with $a(X) < g$, and $X' := X/A(X)$, where $A(X)$ is the maximal α-subgroup of X, then $a(X') > a(X)$.

Now take Y_1 the abelian threefold as in Proposition 3.12(1). We have computed $a(Y_1) = 2$ and $a(Y_1/A(Y_1)) = a((\mathsf{F},\mathsf{V})M_1) = 2$. This gives a counterexample to the claim.

4. THE CASE $a(X) \geq 2$

Let $x = (X, \lambda) \in \mathscr{S}_{3,1}(k)$ with $a(X) = 2$ and let $y \in \mathscr{P}_\mu \simeq \mathbb{P}^1_C(\mathscr{O}(-1) \oplus \mathscr{O}(1))$ be the point corresponding to the PFTQ over it:

$$(Y_2, \lambda_2) \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_0, \lambda_0) = (X, \lambda).$$

By Propositions 3.11 and 3.12, (Y_1, λ_1) corresponds to a point $t = (t_1, t_2, t_3) \in C(\mathbb{F}_{p^2})$ and $u \in \mathbb{P}^1_t(k) := \pi^{-1}(t)$. Moreover, $\rho_1 : (Y_1, \lambda_1) \to (X, \lambda)$ is the minimal isogeny. Put $x_1 = (Y_1, \lambda_1)$. Then $\Lambda_{x_1} = \Lambda_{3,p}$ and by Corollary 2.5 and Proposition 2.12 we have

$$\mathrm{Mass}(\Lambda_x) = \frac{(p-1)(p^3+1)(p^3-1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7} \cdot [\mathrm{Aut}(M_1, \langle\,\rangle) : \mathrm{Aut}(M, \langle\,,\rangle)], \tag{11}$$

where $(M, \langle\,,\rangle) \subseteq (M_1, \langle\,,\rangle)$ are the quasi-polarised Dieudonné modules associated to $(Y_1, \lambda_1) \to (X, \lambda)$.

Let $M_1^\vee$ denote the dual lattice of M_1 with respect to $\langle\,,\rangle$. Then one has $M_1^\vee \subseteq M \subseteq M_1$ and $M/M_1^\vee \in \mathbb{P}(M_1/M_1^\vee) = \mathbb{P}^1_t(k)$ is a one-dimensional k-subspace in $M_1/M_1^\vee$. Since the morphism ρ_2 is defined over $\mathbb{F}_{p^2}$, the threefold Y_1 is endowed with the $\mathbb{F}_{p^2}$-structure Y_1' with Frobenius $\pi_{Y_1'} = -p$. The induced $\mathbb{F}_{p^2}$-structure on $\mathbb{P}^1_t$ is defined by the $\mathbb{F}_{p^2}$-vector space $V_0 := M_1^\diamond/M_1^{t,\diamond}$, where $M_1^\diamond := \{m \in M_1 : \mathsf{F}m + \mathsf{V}m = 0\}$ is the skeleton of M_1, cf. [12, Section 5.7].

Since $\ker(\lambda_1) \simeq \alpha_p \times \alpha_p$, the quasi-polarised superspecial Dieudonné module $(M_1, \langle\,,\rangle)$ decomposes into a product of a two-dimensional indecomposable superspecial Dieudonné module and a one-dimensional such module. By [12, Proposition 6.1], there is a W-basis $e_1, e_2, e_3, f_1, f_2, f_3$ for M_1 such that $\mathsf{F}e_i = -\mathsf{V}e_i = f_i$, $\mathsf{F}f_i = -\mathsf{V}f_i = -pe_i$. for $i = 1, 2, 3$,

$$\langle e_1, e_2 \rangle = p^{-1}, \quad \langle f_1, f_2 \rangle = 1, \quad \langle e_3, f_3 \rangle = 1,$$

and other pairings are zero. Then $M_1^\vee$ is spanned by $pe_1, p_2, e_3, f_1, f_2, f_3$ and $M_1/M_1^\vee = \mathrm{Span}_k\{e_1, e_2\}$. Let $u = (u_1 : u_2) \in \mathbb{P}^1_t(k)$ be the projective coordinates of the point corresponding to $M/M_1^\vee$. That is, $M/M_1^\vee$ is the one-dimensional subspace spanned by $u = u_1\bar{e}_1 + u_2\bar{e}_2$, where $\bar{e}_i$ denotes the image of e_i in $M_1/M_1^\vee$.

If $u \in \mathbb{P}^1_t(\mathbb{F}_{p^2})$, then $a(M) = 3$ and $\mathrm{Mass}(\Lambda_x)$ is already computed in Corollary 2.5. Suppose then that $u \notin \mathbb{P}^1_t(\mathbb{F}_{p^2})$. In this case, M_1 (resp. $M_1^\vee$) is the smallest (resp. maximal) superspecial Dieudonné module containing (resp. contained in) M. Thus,

$$\mathrm{End}(M) = \{g \in \mathrm{End}(M_1) : g(M_1^\vee) \subseteq M_1^\vee,\ g(M) \subseteq M\}.$$

Consider the reduction map

$$m : \mathrm{End}(M_1) = \mathrm{End}(M_1^\diamond) \twoheadrightarrow \mathrm{End}(M_1^\diamond/M_1^{t,\diamond}) = \mathrm{End}_{\mathbb{F}_{p^2}}(V_0) = \mathrm{Mat}_2(\mathbb{F}_{p^2}).$$

It is clear that $\mathrm{End}(M)$ contains $\ker(m)$ and that m induces a surjective map

$$m : \mathrm{End}(M) \twoheadrightarrow m(\mathrm{End}(M)) = \{g \in \mathrm{Mat}_2(\mathbb{F}_{p^2}) : g \cdot u \subseteq k \cdot u\}.$$

Write $\mathrm{End}(u) := \{g \in \mathrm{Mat}_2(\mathbb{F}_{p^2}) : g \cdot u \subseteq k \cdot u\}$.

Lemma 4.1.

(1) *If* $u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) - \mathbb{P}^1_t(\mathbb{F}_{p^2})$, *then* $\mathrm{End}(u) \subseteq \mathrm{Mat}_2(\mathbb{F}_{p^2})$ *is an* $\mathbb{F}_{p^2}$*-subalgebra which is isomorphic to* $\mathbb{F}_{p^4}$.

(2) *If* $u \in \mathbb{P}^1_t(k) - \mathbb{P}^1_t(\mathbb{F}_{p^4})$, *then* $\mathrm{End}(u) = \mathbb{F}_{p^2}$.

Proof. This is a simpler version of Lemmas 3.6 and 3.7 so we omit the proof; cf. also [25, Section 3]. □

Put $\langle\, ,\rangle_1 := p\langle\, ,\rangle$. Then $\langle\, ,\rangle_1$ induces a non-degenerate alternating pairing, again denoted $\langle\, ,\rangle_1 : V_0 \times V_0 \to \mathbb{F}_{p^2}$. The reduction map m then gives rise to the following map

$$m : \mathrm{Aut}(M_1, \langle\, ,\rangle) = \mathrm{Aut}(M_1, \langle\, ,\rangle_1) \to \mathrm{Aut}(V_0, \langle\, ,\rangle_1) \simeq \mathrm{SL}_2(\mathbb{F}_{p^2}). \tag{12}$$

Lemma 4.2. *The map $m : \mathrm{Aut}(M_1, \langle\, ,\rangle) \to \mathrm{Aut}(V_0, \langle\, ,\rangle_1)$ is surjective.*

Proof. Since Y_1 is supersingular, we have that $\mathrm{End}(Y_1) \otimes \mathbb{Z}_p \simeq \mathrm{End}(M_1)$ and that $G_{x_1}(\mathbb{Z}_p) \simeq \mathrm{Aut}(M_1, \langle\, ,\rangle)$; recall the notation from (6). The group scheme $G_{x_1} \otimes \mathbb{Z}_p$ is a parahoric group scheme and in particular is smooth over $\mathbb{Z}_p$. Thus, the map $G_{x_1}(\mathbb{Z}_p) \to G_{x_1}(\mathbb{F}_p)$ is surjective. Now $\mathrm{Aut}(V_0, \langle\, ,\rangle_1) = \mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p} \mathrm{SL}_2$ viewed as an algebraic group over $\mathbb{F}_p$ is a reductive quotient of the special fibre $G_{x_1} \otimes \mathbb{F}_p$. Therefore, the map $G_{x_1}(\mathbb{F}_p) \to \mathrm{Aut}(V_0, \langle\, ,\rangle_1) = \mathrm{SL}_2(\mathbb{F}_{p^2})$ is also surjective. This proves the lemma. □

We now prove the main result of this section.

Theorem 4.3. *Let $x = (X, \lambda) \in \mathscr{S}_{3,1}(k)$ with $a(X) \geq 2$ and let $y \in \mathscr{P}'_\mu(k)$ be a lift of x for some $\mu \in P(E^3)$. Write $y = (t, u)$ where $t = \pi(y) \in C(\mathbb{F}_{p^2})$ and $u \in \pi^{-1}(t) = \mathbb{P}^1_t(k)$. Then*

$$\mathrm{Mass}(\Lambda_x) = \frac{L_p}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}, \tag{13}$$

where

$$L_p = \begin{cases} (p-1)(p^2+1)(p^3-1) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ (p-1)(p^3+1)(p^3-1)(p^4-p^2) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ 2^{-e(p)}(p-1)(p^3+1)(p^3-1)p^2(p^4-1) & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}); \end{cases} \tag{14}$$

where $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$.

Proof. By Lemma 4.2,

$$[\mathrm{Aut}(M_1, \langle\, ,\rangle) : \mathrm{Aut}(M, \langle\, ,\rangle)] = [\mathrm{SL}_2(\mathbb{F}_{p^2}) : \mathrm{SL}_2(\mathbb{F}_{p^2}) \cap \mathrm{End}(u)^\times].$$

By Lemma 4.1,

$$\mathrm{SL}_2(\mathbb{F}_{p^2}) \cap \mathrm{End}(u)^\times = \begin{cases} \mathbb{F}^1_{p^4} & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ \{\pm 1\} & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}). \end{cases}$$

It follows that

$$[\mathrm{Aut}(M_1, \langle\rangle) : \mathrm{Aut}(M, \langle\, ,\rangle)] = \begin{cases} p^2(p^2-1) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ |\,\mathrm{PSL}_2(\mathbb{F}_{p^2})| & \text{if } u \notin \mathbb{P}^1_t(\mathbb{F}_{p^4}), \end{cases}$$

so the theorem follows from (11). □

5. The case $a(X) = 1$

Suppose that (X, λ) is a supersingular principally polarised abelian threefold over k with $a(X) = 1$. By Proposition 3.12(1), there is a minimal isogeny $\varphi : (Y_2, \mu) \to (X, \lambda)$, where $Y_2 = \overline{E}^3$, and where $\varphi^*\lambda = p\mu$ for $\mu \in P(E^3)$ a principal polarisation. In this section we will compute the local index

$$[\mathrm{Aut}((Y_2, \mu)[p^\infty]) : \mathrm{Aut}((X, \lambda)[p^\infty])]. \tag{15}$$

Let M and M_2 be the Dieudonné modules of X and Y_2, respectively. Together with the induced (quasi-)polarisations, we have $(M, \langle,\rangle)$ and $(M_2, \langle,\rangle_2)$, where $\langle,\rangle_2 = p\langle,\rangle$ is again a principal polarisation. (Note that $(M_2, \langle,\rangle_2)$ is the quasi-polarised Dieudonné module associated to (Y_2, μ), and not to $(Y_2, p\mu)$.) The proof of Proposition 3.12(1) shows that every automorphism of M can be lifted to an automorphism of M_2, i.e., that $\mathrm{Aut}((M,\langle,\rangle)) \subseteq \mathrm{Aut}((M_2,\langle,\rangle_2))$. Then equivalently to (15), cf. Proposition 2.12, we will compute

$$[\mathrm{Aut}((M_2,\langle,\rangle_2)) : \mathrm{Aut}((M,\langle,\rangle))]. \tag{16}$$

5.1. Determining $\mathrm{Aut}((M_2,\langle,\rangle_2))$.

Let $W = W(k)$ denote the ring of Witt vectors over k. Choose a W-basis $e_1, e_2, e_3, f_1, f_2, f_3$ for M_2 such that

$$\mathsf{F}e_i = -\mathsf{V}e_i = f_i, \quad \mathsf{F}f_i = -\mathsf{V}f_i = -pe_i, \quad \langle e_i, f_j\rangle_2 = \delta_{ij}, \quad \langle e_i, e_j\rangle_2 = \langle f_i, f_j\rangle_2 = 0, \tag{17}$$

for all $i, j \in \{1,2,3\}$.

Let D_p be the division quaternion algebra over $\mathbb{Q}_p$ and let $\mathscr{O}_{D_p}$ denote its maximal order. We also write $D_p = \mathbb{Q}_{p^2}[\Pi]$ and $\mathscr{O}_{D_p} = \mathbb{Z}_{p^2}[\Pi]$, where $\mathbb{Z}_{p^2} = W(\mathbb{F}_{p^2})$ and $\mathbb{Q}_{p^2} = \mathrm{Frac}W(\mathbb{F}_{p^2})$, and where $\Pi^2 = -p$ and $\Pi a = \overline{a}\Pi$ for any $a \in \mathbb{Q}_{p^2}$. Here $a \mapsto \overline{a}$ denotes the non-trivial automorphism of $\mathbb{Q}_{p^2}/\mathbb{Q}_p$. If we let $*$ denote the canonical involution of D_p, then $a^* = \overline{a}$ for any $a \in \mathbb{Q}_{p^2}$, and $\Pi^* = -\Pi$.

Lemma 5.1. *We have* $\mathrm{End}(M_2) \simeq \mathrm{Mat}_3(\mathscr{O}_{D_p})$ *and hence* $\mathrm{Aut}(M_2) \simeq \mathrm{GL}_3(\mathscr{O}_{D_p})$ *(not taking the polarisation into account).*

Proof. We have $\mathrm{End}(M_2) = \mathrm{End}_{\mathscr{O}_{D_p}}(M_2^\diamondsuit)$, where $M_2^\diamondsuit := \{m \in M_2 : \mathsf{F}m + \mathsf{V}m = 0\}$ denotes the skeleton of M_2; this is an $\mathscr{O}_{D_p}$-module where Π acts by F and Π^* acts by V. Now the result follows by using the basis e_1, e_2, e_3 for $\mathrm{Mat}_3(\mathscr{O}_{D_p})^{\mathrm{op}}$ (the opposite algebra); we choose a convention where the matrices act on the left. We fix the isomorphism $\mathrm{Mat}_3(\mathscr{O}_{D_p})^{\mathrm{op}} \simeq \mathrm{Mat}_3(\mathscr{O}_D)$ by sending A to A^*. □

We fix the identification $\mathrm{End}(M_2) = \mathrm{Mat}_3(\mathscr{O}_D)$ by the isomorphism chosen in Lemma 5.1 with respect to the basis in (17).

Lemma 5.2. *We have* $\mathrm{Aut}(M_2,\langle,\rangle_2) \simeq \{A \in \mathrm{GL}_3(\mathscr{O}_{D_p}) : A^*A \simeq \mathbb{I}_3\}$.

Proof. It suffices to check that $\langle A\cdot e_i, e_j\rangle_2 = \langle e_i, A^*\cdot e_j\rangle_2$ for any $A \in \mathrm{Mat}_3(\mathscr{O}_{D_p})$ and any $i, j \in \{1,2,3\}$. Write $A = (a_{ij})$ and $A^* = (a'_{ij})$ with $a_{ij} = c_{ij} + d_{ij}\Pi$ for $c_{ij}, d_{ij} \in \mathbb{Z}_{p^2}$, and with $a'_{ij} = a^*_{ji}$. Then

$$\langle A\cdot e_i, e_j\rangle_2 = \langle \sum_k a_{ik}e_k, e_j\rangle_2 = \langle d_{ij}f_j, e_j\rangle_2 = -d_{ij}$$

coincides with

$$\langle e_i, A^*\cdot e_j\rangle_2 = \langle e_i, \sum_k a'_{jk}e_k\rangle_2 = \langle e_i, a'_{ji}e_i\rangle_2 = \langle e_i, \overline{c}_{ij}e_i - d_{ij}f_i\rangle_2 = -d_{ij},$$

as required. □

5.2. Endomorphisms and automorphisms modulo pM_2.

The proof of Proposition 3.12(1) contains the important observation that $pM_2 \subseteq M$. This allows us to consider the endomorphisms and automorphisms of both M_2 and M modulo p (i.e., reducing modulo pM_2) and modulo Π. We first define these objects.

Definition 5.3. Let m_p denote the reduction-modulo-p map and m_Π the reduction-modulo-Π map. By Lemma 5.1, for M_2 we have

$$\mathrm{End}(M_2) \simeq \mathrm{Mat}_3(\mathscr{O}_{D_p}) \xrightarrow{m_p} \mathrm{Mat}_3(\mathbb{F}_{p^2}[\Pi]) \xrightarrow{m_\Pi} \mathrm{Mat}_3(\mathbb{F}_{p^2}). \tag{18}$$

On the level of automorphisms (respecting the polarisation) we get

$$\mathrm{Aut}(M_2,\langle,\rangle_2) \xrightarrow{m_p} G_{(M_2,\langle,\rangle_2)} \xrightarrow{m_\Pi} \overline{G}_{(M_2,\langle,\rangle_2)}, \tag{19}$$

where

$$(20) \qquad G_{(M_2,\langle,\rangle_2)} := \{A + B\Pi \in \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi]) : A\overline{A}^T = \mathbb{I}_3, B^T\overline{A} = \overline{A}^T B\},$$

(here, B^T denotes the transpose of the matrix B), and where

$$(21) \qquad \overline{G}_{(M_2,\langle,\rangle_2)} := \{A \in \mathrm{GL}_3(\mathbb{F}_{p^2}) : A^*A = \mathbb{I}_3\}.$$

Definition 5.4. For M we have $\mathrm{End}(M) = \{g \in \mathrm{End}(M_2) : g(M) \subseteq M\}$ and $\mathrm{Aut}(M) = \{g \in \mathrm{Aut}(M_2) : g(M) = M\}$, and

$$(22) \qquad \mathrm{Aut}(M, \langle,\rangle) = \{g \in \mathrm{Aut}(M_2, \langle,\rangle_2) : g(M) = M\}.$$

Under the same maps m_p and m_Π, we find

$$(23) \qquad E_M := m_p(\mathrm{End}(M)) = \{A \in \mathrm{Mat}_3(\mathbb{F}_{p^2}[\Pi]) : A \cdot M/pM_2 \subseteq M/pM_2\}$$

and $\overline{E}_M := m_\Pi(E_M) \subseteq \mathrm{Mat}_3(\mathbb{F}_{p^2})$. These fit in the diagram

$$(24) \qquad \begin{array}{ccc} \mathrm{End}(M) & \longrightarrow & \mathrm{End}(M_2) = \mathrm{Mat}_3(\mathscr{O}_{D_p}) \\ \downarrow{\scriptstyle m_p} & & \downarrow{\scriptstyle m_p} \\ E_M & \longrightarrow & \mathrm{Mat}_3(\mathbb{F}_{p^2}[\Pi])) \\ \downarrow{\scriptstyle m_\Pi} & & \downarrow{\scriptstyle m_\Pi} \\ \overline{E}_M & \longrightarrow & \mathrm{Mat}_3(\mathbb{F}_{p^2}) \end{array}$$

in which all horizontal maps are inclusion maps and the left vertical maps are the surjective reduction maps.

On the level of automorphisms, we let

$$(25) \qquad G_M := m_p(\mathrm{Aut}(M)) = \{A \in \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi]) : A \cdot M/pM_2 \subseteq M/pM_2\}$$

and $\overline{G}_M := m_\Pi(G_M)$. For the polarised versions, since $\varphi^*\lambda = p\mu$, we obtain

$$(26) \qquad G_{(M,\langle,\rangle)} := \{g \in G_{(M_2,\langle,\rangle_2)} : g(M/pM_2) \subseteq M/pM_2\}$$

and

$$(27) \qquad \overline{G}_{(M,\langle,\rangle)} := \{g \in \overline{G}_{(M_2,\langle,\rangle_2)} : g(M/pM_2) \subseteq M/pM_2\}.$$

Denote the group of three-by-three symmetric matrices over $\mathbb{F}_{p^2}$ by $S_3(\mathbb{F}_{p^2})$; this group has cardinality p^{12} (since it a six-dimensional $\mathbb{F}_{p^2}$-vector space). Also recall that the group $U_3(\mathbb{F}_p)$ of three-by-three unitary matrices with entries in $\mathbb{F}_{p^2}$ has cardinality $p^3(p+1)(p^2-1)(p^3+1)$.

Lemma 5.5. *In Equation* (20) *we have* $A \in U_3(\mathbb{F}_p)$ *and* $B^T\overline{A} \in S_3(\mathbb{F}_{p^2})$. *Hence,*

$$(28) \qquad |G_{(M_2,\langle,\rangle_2)}| = |U_3(\mathbb{F}_p)| \cdot |S_3(\mathbb{F}_{p^2})| = p^{15}(p+1)(p^2-1)(p^3+1).$$

Remark 5.6. Now we note, cf. (16), that

$$(29) \qquad [\mathrm{Aut}((M_2, \langle,\rangle_2)) : \mathrm{Aut}((M, \langle,\rangle))] = [G_{(M_2,\langle,\rangle_2)} : G_{(M,\langle,\rangle)}].$$

In light of Lemma 5.5, it now suffices to compute $[G_{(M_2,\langle,\rangle_2)} : G_{(M,\langle,\rangle)}]$. This will take up the remainder of this section.

We start by studying the unpolarised automorphisms G_{M_2}. Thus, let $g = (a_{ij}+b_{ij}\Pi)_{1\le i,j\le 3} \in \mathrm{GL}_3(\mathbb{F}_{p^2}(\Pi))$ be an (unpolarised) automorphism of M_2/pM_2. If we take $\bar{e}_1, \bar{e}_2, \bar{e}_3, \bar{f}_1, \bar{f}_2, \bar{f}_3$

(i.e., the reductions of $e_1, \dots, f_3$ in the previous subsection) as a basis of M_2/pM_2 in this order, g can be expressed by a matrix of the form

$$g = \begin{pmatrix} A & 0 \\ B & A^{(p)} \end{pmatrix}, \tag{30}$$

where $A = (a_{ij})_{1\le i,j\le 3}$,$B = (b_{ij})_{1\le i,j\le 3}$, and $A^{(p)} = (a_{ij}^p)_{1\le i,j\le 3}$.

Recall from Proposition 3.12(1) that the polarised flag type quotient $Y_2 \to Y_1 \to X$ corresponds to a point $t = (t_1 : t_2 : t_3) \in C^0(k)$ such that $M_1/\mathsf{F}M_2$ is generated by $t_1\bar{e}_1+t_2\bar{e}_2+t_3\bar{e}_3$, where M_1 is the Dieudonné module of Y_1. We choose a new basis for M_2/pM_2 as follows:

$$\bar{E}_1 := \sum_{i=1,2,3} t_i\bar{e}_i,\ \bar{E}_2 := \sum_{i=1,2,3} t_i^p\bar{e}_i,\ \bar{E}_3 := \sum_{i=1,2,3} t_i^{p^{-1}}\bar{e}_i,$$
$$\bar{F}_1 := \sum_{i=1,2,3} t_i\bar{f}_i,\ \bar{F}_2 := \sum_{i=1,2,3} t_i^p\bar{f}_i,\ \bar{F}_3 := \sum_{i=1,2,3} t_i^{p^{-1}}\bar{f}_i.$$

(This is a basis by Lemma 3.4.) Using this basis, g is expressed as

$$g = \begin{pmatrix} \mathbb{T}^{-1}A\mathbb{T} & 0 \\ \mathbb{T}^{-1}B\mathbb{T} & \mathbb{T}^{-1}A^{(p)}\mathbb{T} \end{pmatrix}, \tag{31}$$

where

$$\mathbb{T} := \begin{pmatrix} t_1 & t_1^p & t_1^{p^{-1}} \\ t_2 & t_2^p & t_2^{p^{-1}} \\ t_3 & t_3^p & t_3^{p^{-1}} \end{pmatrix}. \tag{32}$$

Now we determine the group $G_M \subseteq \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi])$ of elements preserving M/pM_2. Any such element will also preserve M_1/pM_2. We prove the following proposition.

Proposition 5.7. *Let $g \in \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi])$ be an automorphism of M_2/pM_2, expressed as in* (30)*. Then $g \in G_M$ (i.e., g preserves M/pM_2) if and only if the following hold:*

(a) *We have $A \cdot t = \alpha t$ for some $\alpha \in k$, i.e., $A \in \mathrm{End}(t)$.*
(b) *The $(1,1)$-component of the matrix $\mathbb{T}^{-1}B\mathbb{T}$ is $u_2u_1^{-1}(\alpha - \alpha^{p^3})$.*

Proof. For an $A \in \mathrm{End}(t)$ (see Definition 3.5) with eigenvalue α, it holds by definition that

$$\mathbb{T}^{-1}A\mathbb{T} = \begin{pmatrix} \alpha & * & * \\ & * & * \\ & * & * \end{pmatrix}, \mathbb{T}^{-1}A^{(p)}\mathbb{T} = \begin{pmatrix} * & & \\ * & \alpha^p & \\ * & & \alpha^{p^{-1}} \end{pmatrix}. \tag{33}$$

As $\det(A) = \alpha^{1+p^2+p^{-2}}$ and $\det(A^{(p)}) = \det(A)^p$, we see that

$$\mathbb{T}^{-1}A^{(p)}\mathbb{T} = \begin{pmatrix} \alpha^{p^3} & & \\ * & \alpha^p & \\ * & & \alpha^{p^{-1}} \end{pmatrix}. \tag{34}$$

By Proposition 3.12(1), the quotient M_1/pM_2 is a two dimensional k-vector space generated by $\bar{E}_1$ and $\bar{F}_1$. As $M_1^\vee = (\mathsf{F},\mathsf{V})M_1 = pM_2$, we find that $M/pM_2 \subseteq M_1/pM_2$ is a one-dimensional k-vector space. Take $u_1, u_2 \in k$ so that M/pM_2 is generated by the image of $u_1\bar{E}_1 + u_2\bar{F}_1$. As $M \neq pM_2$, we see that $u_1 \neq 0$.

We see that if $g \in \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi])$ preserves $M_1/(\mathsf{F},\mathsf{V})M_2$, then it induces an automorphism of $M_1/(\mathsf{F},\mathsf{V})M_1 = M_1/pM_2$ which is expressed as $\left(\begin{smallmatrix} \alpha & \\ * & \alpha^{p^3} \end{smallmatrix}\right)$ by (31), (33), and (34). Moreover, g also preserves $M/(\mathsf{F},\mathsf{V})M_1 = M/pM_2$ if and only if the column vector $\left(\begin{smallmatrix} \alpha & \\ * & \alpha^{p^3} \end{smallmatrix}\right)\left(\begin{smallmatrix} u_1 \\ u_2 \end{smallmatrix}\right)$ is in the subspace spanned by $\left(\begin{smallmatrix} u_1 \\ u_2 \end{smallmatrix}\right)$. This is equivalent to the entry $*$ being equal to $u_2u_1^{-1}(\alpha - \alpha^{p^3})$. □

Remark 5.8. (1) It follows from the construction of polarised flag type quotients that for (X, λ) with $a(X) = 1$ and a choice $\mu \in P(E^3)$ together with an indentification $(\widetilde{X}, \widetilde{\lambda}) = (\overline{E}^3, p\mu)$, there exists a unique pair (t, u) where $t = (t_1 : t_2 : t_3) \in C^0(k)$ and $u = (u_1 : u_2) \in \mathbb{P}^1(k)$ as in the proof of Proposition 5.7. For the rest of the section, we will work with these (t, u).

(2) The coordinates (t, u) in (1) also give rise to a trivialisation $C^0 \times \mathbb{P} \simeq \mathscr{P}_{C^0}$, where $\mathscr{P}_{C^0} := \mathscr{P}_\mu \times_C C^0$, as follows. By Proposition 3.2, points in $\mathscr{P}_{C^0}$ correspond to pairs $(\overline{M}_1, \overline{M})$: here $\overline{M}_1 \subseteq \overline{M}_2$ is a four-dimensional subspace generated by the subspace $\mathsf{V}\overline{M}_2$ and $\overline{E}_1 = t_1\bar{e}_1 + t_2\bar{e}_2 + t_3\bar{e}_3$ with $(t_1 : t_2 : t_3) \in C^0$, and $\overline{M} \subseteq \overline{M}_2$ is a three-dimensional subspace with $\overline{M}_1^\perp \subseteq \overline{M} \subseteq \overline{M}_1$, where $\overline{M}_1^\perp$ is the orthogonal complement of $\overline{M}_1$ with respect to $\langle\, , \rangle_2$. The two-dimensional vector spaces $\overline{M}_1/\overline{M}_1^\perp$ for $t \in C^0$ form a rank two vector bundle $\mathscr{V} = \mathscr{O}(1) \oplus \mathscr{O}(-1)|_{C^0}$ over C^0. As shown in the proof of Proposition 5.7, the images of $\overline{E}_1$ and $\overline{F}_1$ in $\overline{M}_1/\overline{M}_1^\perp$ (again denoted by $\overline{E}_1$ and $\overline{F}_1$ for simplicity) form a basis, and give rise to two global sections $\widetilde{E}_1$ and $\widetilde{F}_1$ of $\mathscr{V}$ respectively (note that both $\overline{E}_1$ and $\overline{F}_1$ are vector-valued functions in t_1, t_2, and t_3). Then the desired trivialisation $C^0 \times \mathbb{P} \xrightarrow{\sim} \mathscr{P}_{C^0} \simeq \mathbb{P}(\mathscr{V})$ is given by $(t, (u_1 : u_2)) \mapsto [u_1\widetilde{E}_1(t) + u_2\widetilde{F}_1(t)]$. Since M_2 is the Dieudonné module of $\overline{E}^3$, the vector space $\overline{M}_2$ has an $\mathbb{F}_{p^2}$-structure, so we see that this trivialisation is defined over $\mathbb{F}_{p^2}$.

Now let $t \in C^0(k)$ and $u = (0 : 1)$. The corresponding subspace $\overline{M}$ is generated by $\overline{F}_1$ and $\overline{M}_1^\perp = (\mathsf{F}, \mathsf{V})\overline{M}_1$. Therefore, we have $\overline{M} = \mathsf{V}\overline{M}_2$, which corresponds a point in T. It follows that under the above trivialisation, $T \simeq C^0 \times \{\infty\}$.

The following lemma follows from Lemma 3.6, Lemma 3.7, and Proposition 5.7. It describes the *polarised* elements $g \in G_{(M_2, \langle , \rangle_2)}$ that preserve M_1/pM_2: for such g of the form (30), Proposition 5.7(1) implies that $A \in \mathrm{End}(t)$, while Definition 5.3(20) implies that A is unitary.

Lemma 5.9. *Let $t = (t_1 : t_2 : t_3) \in C^0(k)$.*

(1) *When $t \notin C(\mathbb{F}_{p^6})$, we have*

$$\mathrm{End}(t) \cap U_3(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^2} : \alpha^{p+1} = 1\}.$$

(2) *When $t \in C(\mathbb{F}_{p^6})$, we have*

$$\mathrm{End}(t) \cap U_3(\mathbb{F}_p) \simeq \{\alpha \in \mathbb{F}_{p^6} : \alpha^{p^3+1} = 1\}.$$

Proof. (1) This follows since a diagonal matrix $\alpha\mathbb{I}_3$ with $\alpha \in \mathbb{F}_{p^2}$ is unitary if and only if $\alpha^{p+1} = 1$.

(2) Take any $A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p)$. The eigenvalues of $A^{(p)T}$ are $\alpha^p, \alpha^{p^3}, \alpha^{p^5}$ where α is the eigenvalue of A. As A is unitary, α^{-1} is also an eigenvalue, so we have $\alpha^{-1} \in \{\alpha^p, \alpha^{p^3}, \alpha^{p^5}\}$. In each case, we have $\alpha^{p^3+1} = 1$.

For the converse, choose any $\alpha \in \mathbb{F}_{p^6}$ such that $\alpha^{p^3+1} = 1$. By the proof of Lemma 3.6, the corresponding $A \in \mathrm{End}(t)$ is given by

$$A = (t, t^{(p^2)}, t^{(p^4)})\mathrm{diag}(\alpha, \alpha^{p^2}, \alpha^{p^4})(t, t^{(p^2)}, t^{(p^4)})^{-1}.$$

We compute that

$$AA^{(p)T} = (t, t^{(p^2)}, t^{(p^4)}) \begin{pmatrix} & s^{-1} & \\ & & s^{-p^2} \\ s^{-p} & & \end{pmatrix} (t^{(p)}, t^{(p^3)}, t^{(p^5)})^T$$

where $s = t_1^{p^3+1} + t_2^{p^3+1} + t_3^{p^3+1}$. That is, $AA^{(p)T}$ is independent of α. By the case $\alpha = 1$, we have $AA^{(p)T} = 1$.

□

Suppose now that we have $g \in G_{(M_2,\langle,\rangle_2)}$ of the form (30) preserving M_1/pM_2, i.e., we have $A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p)$ by Lemma 5.9. We now determine the conditions on B so that g also preserves M/pM_2, i.e., so that $g \in G_{(M,\langle,\rangle)}$. By (20), B satisfies a symmetric condition.

Let $S_3(\mathbb{F}_{p^2})A$ (for $A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p)$ as above) be the $\mathbb{F}_{p^2}$-vector space consisting of matrices of the form SA for some $S \in S_3(\mathbb{F}_{p^2})$. Define a homomorphism of $\mathbb{F}_{p^2}$-vector spaces

$$\begin{aligned} \psi_{t,A} :& S_3(\mathbb{F}_{p^2})A \to k \\ & SA \mapsto \text{ the } (1,1)\text{-component of } \mathbb{T}^{-1}SA\mathbb{T}. \end{aligned} \tag{35}$$

Similarly define a homomorphism

$$\begin{aligned} \psi_t :& S_3(\mathbb{F}_{p^2}) \to k \\ & S \mapsto \text{ the } (1,1)\text{-component of } \mathbb{T}^{-1}S\mathbb{T}. \end{aligned} \tag{36}$$

Using these notations, we have the following proposition.

Proposition 5.10. *The group $G_{(M,\langle,\rangle)}$ consists of the matrices of the form*

$$\begin{pmatrix} A & 0 \\ SA & A^{(p)} \end{pmatrix}$$

satisfying the following conditions:

(1) $A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p)$ *with eigenvalue* α*;*
(2) $S \in S_3(\mathbb{F}_{p^2})$ *is a symmetric matrix; and*
(3) $\psi_{t,A}(SA) = u_2 u_1^{-1}(\alpha - \alpha^{p^3})$.

The third condition is equivalent to

(3') $\psi_t(S) = u_2 u_1^{-1}(1 - \alpha^{p^3-1})$.

Proof. It follows from (26) and Proposition 5.7 that for $A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p)$ with eigenvalue α, the matrix $\begin{pmatrix} A & 0 \\ B & A^{(p)} \end{pmatrix}$ is an element of $G_{(M,\langle,\rangle_2)} \cap G_{(M,\langle,\rangle)}$ if and only if BA^{-1} is a symmetric matrix and the $(1,1)$-component of the matrix $\mathbb{T}^{-1}B\mathbb{T}$ is $u_2 u_1^{-1}(\alpha - \alpha^{p^3})$. The latter condition amounts to Condition (3) (and (3')) by noticing that since $\mathbb{T}^{-1}A\mathbb{T}$ is of the form

$$\begin{pmatrix} \alpha & * & * \\ & * & * \\ & * & * \end{pmatrix}$$

where α is the eigenvalue of A, we have a commutative diagram

$$\begin{array}{ccc} S_3(\mathbb{F}_{p^2}) & \xrightarrow{\psi_x} & k \\ \big\downarrow \cdot A & & \big\downarrow \cdot\alpha \\ S_3(\mathbb{F}_{p^2})A & \xrightarrow{\psi_{t,A}} & k \end{array}, \tag{37}$$

where the left vertical arrow is multiplying A from the right and the right vertical arrow is multiplying with α. □

The following corollary follows immediately from Proposition 5.10 and summarises the results in this subsection.

Corollary 5.11. *We have*

$$|G_{(M,\langle,\rangle)}| = |\{A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p) : u_2 u_1^{-1}(1 - \alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)\}| \cdot |\ker(\psi_t)|. \tag{38}$$

5.3. **Analysing $\mathrm{Im}(\psi_t)$ and $\ker(\psi_t)$.**

In the following subsection, we will make Corollary 5.11 more explicit by analysing the image and kernel of the homomorphism ψ_t.

Definition 5.12. In the notation as above, we set

$$d(t) := \dim_{\mathbb{F}_{p^2}}(\mathrm{Im}(\psi_t)). \tag{39}$$

As $\dim_{\mathbb{F}_{p^2}}(S_3(\mathbb{F}_{p^2})) = 6$, we see that $d(t) \leq 6$, and that

$$|\ker(\psi_t)| = p^{2(6-d(t))}. \tag{40}$$

We prove the following precise result about the values of $d(t)$.

Proposition 5.13. *We have $3 \leq d(t) \leq 6$. When $p = 2$, we have $d(t) = 3$. Let $v = (t_1^2, t_2^2, t_3^2, t_1t_2, t_1t_3, t_2t_3)$ and let*

$$\Delta = \left\{\det\left(v^T, (v^{(p^2)})^T, (v^{(p^4)})^T, \dots, (v^{(p^{10})})^T\right) = 0\right\}.$$

When $p \neq 2$, we have:

$$\begin{array}{llll} & d(t) = 3 & \textit{if and only if} & t \in C^0(\mathbb{F}_{p^6}); \\ & d(t) = 4 & \textit{if and only if} & t \in C^0(\mathbb{F}_{p^8}); \\ (41) & d(t) = 5 & \textit{if and only if} & t \in \Delta \cap C^0 \setminus \left(C^0(\mathbb{F}_{p^6}) \amalg C^0(\mathbb{F}_{p^8})\right); \\ & d(t) = 6 & \textit{if and only if} & t \notin \Delta \cap C^0. \end{array}$$

Proof. Since $t \in C^0(k)$, we see that $t_i \neq 0$, and without loss of generality we assume that $t_3 = 1$. For $1 \leq i, j \leq 3$, let I_{ij} be the three-by-three matrix whose (i,j)-component is one and where all other entries are zero. Then $I_{11}, I_{22}, I_{33}, I_{12} + I_{21}, I_{13} + I_{31}, I_{23} + I_{32}$ is a basis for $S_3(\mathbb{F}_{p^2})$ over $\mathbb{F}_{p^2}$. We set

$$\begin{aligned} &w_1 = \psi_t(I_{11}), w_2 = \psi_t(I_{22}), w_3 = \psi_t(I_{33}), \\ &w_4 = \psi_t(I_{12} + I_{21}), w_5 = \psi_t(I_{13} + I_{31}), w_6 = \psi_t(I_{23} + I_{32}). \end{aligned} \tag{42}$$

Lemma 5.14. *The w_i in (42) satisfy the following relations:*

$$\begin{aligned} &w_1 = t_1^2 w_3, \qquad w_2 = t_2^2 w_3, \\ &w_4 = 2t_1t_2w_3, \\ &w_5 = 2t_1w_3, \qquad w_6 = 2t_2w_3, \end{aligned}$$

and w_3 is not zero.

Proof of lemma. The inverse matrix of $\mathbb{T}$ is

$$\mathbb{T}^{-1} = \det(\mathbb{T})^{-1}\begin{pmatrix} t_2^p - t_2^{p^{-1}} & t_1^{p^{-1}} - t_1^p & t_1^p t_2^{p^{-1}} - t_1^{p^{-1}} t_2^p \\ t_2^{p^{-1}} - t_2 & t_1 - t_1^{p^{-1}} & t_1^{p^{-1}} t_2 - t_1 t_2^{p^{-1}} \\ t_2^p - t_2 & t_1 - t_1^p & t_1^p t_2 - t_1 t_2^p \end{pmatrix}.$$

Since for any matrices $M = (m_{ij})$, $N = (n_{ij})$ and $L = (l_{ij})$ the $(1,1)$-component of MNL is given by $\sum_{i,j} m_{1i}n_{ij}l_{j1}$, we have

$$\begin{aligned} w_1 &= \det(\mathbb{T})^{-1}(t_2^p - t_2^{p^{-1}})t_1; \\ w_2 &= \det(\mathbb{T})^{-1}(t_1^{p^{-1}} - t_1^p)t_2. \end{aligned}$$

Furthermore, w_3 is given by

$$\begin{aligned} w_3 &= \det(\mathbb{T})^{-1}(t_1^p t_2^{p^{-1}} - t_1^{p^{-1}} t_2^p) \\ &= \det(\mathbb{T})^{-1} t_1^{-1}(t_1^{p+1} t_2^{p^{-1}} - t_1^{p^{-1}+1} t_2^p) \\ &= \det(\mathbb{T})^{-1} t_1^{-1}(t_2^p - t_2^{p^{-1}}). \end{aligned}$$

For the last equality, we used equations $t_1^{p+1} + t_2^{p+1} + 1 = 0$ and $t_1^{p^{-1}+1} + t_2^{p^{-1}+1} + 1 = 0$. Similarly, we see that $w_3 = \det(\mathbb{T})^{-1} t_2^{-1}(t_1^{p^{-1}} - t_1^p)$. These computations imply the first two relations of the assertion, and since $t_1, t_2 \notin \mathbb{F}_{p^2}$, we see that w_3 is not zero. Furthermore, we compute that

$$\begin{aligned} w_4 &= \det(\mathbb{T})^{-1}((t_2^p - t_2^{p^{-1}})t_2 + (t_1^{p^{-1}} - t_1^p)t_1) \\ &= \det(\mathbb{T})^{-1}(t_2^{p+1} - t_2^{p^{-1}+1} + t_1^{p^{-1}+1} - t_1^{p+1}) \\ &= 2\det(\mathbb{T})^{-1} t_2(t_2^p - t_2^{p^{-1}}); \\ w_5 &= \det(\mathbb{T})^{-1}((t_2^p - t_2^{p^{-1}}) + (t_1^p t_2^{p^{-1}} - t_1^{p^{-1}} t_2^p)t_1) \\ &= \det(\mathbb{T})^{-1}(t_2^p - t_2^{p^{-1}} + t_1^{p+1} t_2^{p^{-1}} - t_1^{p^{-1}+1} t_2^p) \\ &= 2\det(\mathbb{T})^{-1}(t_2^p - t_2^{p^{-1}}). \end{aligned}$$

Similarly, we see that $w_6 = 2\det(\mathbb{T})^{-1}(t_1^{p^{-1}} - t_1^p)$, so we obtain the remaining relations. $\square$

When $p \neq 2$, we see from Lemma 5.14 that

$$d(t) = \dim_{\mathbb{F}_{p^2}}\langle w_1, w_2, w_3, w_4, w_5, w_6\rangle = \dim_{\mathbb{F}_{p^2}}\langle 1, t_1, t_2, t_1t_2, t_1^2, t_2^2\rangle.$$

In particular, this implies that

$$d(t) \geq \dim_{\mathbb{F}_{p^2}}\langle w_3, w_5, w_6\rangle = \dim_{\mathbb{F}_{p^2}}\langle 1, t_1, t_2\rangle = 3.$$

When $p = 2$, by Lemma 3.4 and Lemma 5.14, we see that $d(t) = 3$. So assume $p \neq 2$, and consider (41).

By construction (since $t_3 = 1$), we have $t \in \Delta$ if and only if $\dim_{\mathbb{F}_{p^2}}\langle 1, t_1, t_2, t_1t_2, t_1^2, t_2^2\rangle \leq 5$. Hence we see that $t \in \Delta \cap C^0$ if and only if $d(t) \leq 5$, which gives the required statement for $d(t) = 6$. Also note that if $d(t) \leq 5$ then there exists some conic $Q/\mathbb{F}_{p^2}$ with equation $a_1 + a_2t_1 + a_3t_2 + a_4t_1t_2 + a_5t_1^2 + a_6t_2^2 = 0$ such that $t \in C^0 \cap Q$. Similarly if $d(t) \leq 4$ then there exist two independent conics Q_1, Q_2 such that $t \in C^0 \cap Q_1 \cap Q_2$. In this case, Q_1 and Q_2 do not have a common component (even defined over $\overline{\mathbb{F}}_p$). Otherwise, the intersection $Q_1 \cap Q_2$ must be a line L defined over $\mathbb{F}_{p^2}$ (because we require $Q_1 \neq Q_2$) and $Q_1 = L \cup L_1$ for another line L_1 defined over $\mathbb{F}_{p^2}$. This implies that $t \in L$ or $t \in L_1$, a contradiction by Lemma 3.4. If $d(t) \leq 3$ there exist three independent conics Q_1, Q_2, Q_3 such that $t \in C^0 \cap Q_1 \cap Q_2 \cap Q_3$.

If $t \in C^0(\mathbb{F}_{p^{2a}})$ then $d(t) \leq a$, i.e., if $2 \leq \deg_{\mathbb{F}_{p^2}}(t) \leq a$ then $d(t) \leq a$, for any value of a. This shows in particular that if $t \in C^0(\mathbb{F}_{p^6})$, then $d(t) = 3$, cf. Lemma 3.4. Conversely, since $|Q_1 \cap Q_2| \leq 4$ by Bézout's theorem we see that if $d(t) \leq 4$ then $\deg_{\mathbb{F}_{p^2}}(t) \leq 4$. That is, then $t \in C^0(\mathbb{F}_{p^8}) \cup C^0(\mathbb{F}_{p^6})$; note that by Lemma 3.3 we have $C^0(\mathbb{F}_{p^4}) = \emptyset$. If $d(t) = 3$, then the $\mathbb{F}_{p^2}$-subspace $\langle 1, t_1, t_2, t_1^2, t_2^2, t_1t_2\rangle$ is equal to the $\mathbb{F}_{p^2}$-subspace U spanned by $1, t_1, t_2$. Since $t_1U \subset U$ and $t_2U \subset U$, the algebra $\mathbb{F}_{p^2}[t_1, t_2] = U$ has dimension three and $\deg_{\mathbb{F}_{p^2}}(t) = 3$. This implies that $d(t) = 3$ if and only if $t \in C^0(\mathbb{F}_{p^6})$ and hence $d(t) = 4$ if and only if $t \in C^0(\mathbb{F}_{p^8})$. The statement for $d(t) = 5$ now follows. $\square$

Remark 5.15. We provide another proof of the implication $d(t) = 3 \implies \deg_{\mathbb{F}_{p^2}}(t) = 3$, since this information may also be useful. Suppose $P_1, P_2, P_3, P_4 \in \mathbb{P}^2(K)$, where K is a field, are four distinct points not on the same line. Then the conics passing through them form a $\mathbb{P}^1$-family. To see this, suppose Q is represented by $F(t) = 0$, where $F(t) = a_1t_1^2 + a_2t_2^2 + a_3t_3^2 + a_4t_1t_2 + a_5t_1t_2 + a_6t_1t_3$. By assumption P_1, P_2, P_3 are not on the same line. Choose a coordinate for $\mathbb{P}^2$ over K such that $P_1 = (1 : 0 : 0), P_2 = (0 : 1 : 0)$ and $P_3 = (0 : 0 : 1)$. Then $a_1 = a_2 = a_3 = 0$. The point $P_4 = (\alpha_1 : \alpha_2 : \alpha_3)$ satisfies $(\alpha_1\alpha_2, \alpha_1\alpha_3, \alpha_2\alpha_3) \neq (0, 0, 0)$. Thus, $F(P_4) = 0$ gives a non-trivial linear relation among a_4, a_5, and a_6.

Suppose now $t \in C^0 \cap Q_1 \cap Q_2 \cap Q_3$ with $\mathbb{F}_{p^2}$-linear independent conics Q_1, Q_2, Q_3. It suffices to prove $|Q_1 \cap Q_2 \cap Q_3| \leq 3$. If $|Q_1 \cap Q_2| \leq 3$, then we are done. So suppose that $Q_1 \cap Q_2 = \{P_1, P_2, P_3, P_4\}$. If Q_3 contains these four points, then Q_3 is a linear combination of Q_1 and Q_2 over some extension of $\mathbb{F}_{p^2}$ and by descent an $\mathbb{F}_{p^2}$-linear combination of Q_1 and Q_2, contradiction. Thus, we have shown that $|Q_1 \cap Q_2 \cap Q_3| \leq 3$.

Definition 5.16. Let $\mathscr{P}_{C^0} \simeq C^0 \times \mathbb{P}^1$ be the fibre $\mathbb{P}_C(\mathscr{O}(-1) \oplus \mathscr{O}(1)) \times_C C^0$ over C^0, cf. Remark 5.8. For each $S \in S_3(\mathbb{F}_{p^2})$, we define a morphism $f_S : C^0 \to \mathscr{P}_{C^0}$ via the map $C^0 \ni t = (t_1 : t_2 : t_3) \mapsto (t^{(p)}, (1 : \psi_t(S)^p)) \in C^0 \times \mathbb{P}^1$. Observe from the computation in the proof of Proposition 5.13 that $\psi_t(S)$ is a polynomial function in $t_1^{p^{-1}}, t_2^{p^{-1}}, t_3^{p^{-1}}$, and hence that $\psi_t(S)^p$ is a polynomial function in t_1, t_2, t_3. The image of f_S defines a Cartier divisor $D_S \subseteq \mathscr{P}_{C^0}$, and we let D be the horizontal divisor

$$D = \sum_{S \in S_3(\mathbb{F}_{p^2})} D_S.$$

For $t \in C^0(k)$, let $D_t = \pi^{-1}(t) \cap D$. That is, $(u_1 : u_2) \in D_t$ if and only if $u_2u_1^{-1} \in \mathrm{Im}(\psi_t)$.

Lemma 5.17. *Let $t = (t_1 : t_2 : t_3) \in C^0(k)$.*

(1) *If $t \notin C^0(\mathbb{F}_{p^6})$, then*

$$\{\alpha \in \mathbb{F}_{p^2}^\times : u_2u_1^{-1}(1 - \alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)\} = \begin{cases} \mathbb{F}_{p^2}^\times & \text{if } (u_1 : u_2) \in D_t; \\ \mathbb{F}_p^\times & \text{otherwise.} \end{cases}$$

(2) *If $t \in C^0(\mathbb{F}_{p^6})$, then*

$$\{\alpha \in \mathbb{F}_{p^6}^\times : u_2u_1^{-1}(1 - \alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)\} = \begin{cases} \mathbb{F}_{p^6}^\times & \text{if } (u_1 : u_2) \in D_t; \\ \mathbb{F}_{p^3}^\times & \text{otherwise.} \end{cases}$$

Proof. (1) First we note that $\mathbb{F}_p^\times \subseteq \{\alpha \in \mathbb{F}_{p^2}^\times : u_2u_1^{-1}(1 - \alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)\}$. Since $\mathrm{Im}(\psi_t)$ is an $\mathbb{F}_{p^2}$-vector space, we have that if $(u_1 : u_2) \in D_t$, i.e., if $u_2u_1^{-1} \in \mathrm{Im}(\psi_t)$, then $u_2u_1^{-1}(1-\alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)$ for any $\alpha \in \mathbb{F}_{p^2}^\times$. Conversely if $u_2u_1^{-1}(1-\alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)$ for some $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, then $u_2u_1^{-1} \in \mathrm{Im}(\psi_t)$.

(2) If $t \in C^0(\mathbb{F}_{p^6})$, then $\mathrm{Im}(\psi_t) \subseteq \mathbb{F}_{p^6}$. Since $\dim_{\mathbb{F}_{p^2}}(\mathbb{F}_{p^6}) = 3$ and $d(t) \geq 3$ by Proposition 5.13, we must have that $\mathrm{Im}(\psi_t) = \mathbb{F}_{p^6}$. The proof now follows from a similar argument as in (1).

∎

Corollary 5.18. *We have*

$$\{A \in \mathrm{End}(t) \cap U_3(\mathbb{F}_p) : u_2 u_1^{-1}(1-\alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)\} \simeq$$

$$\begin{cases} \{\alpha \in \mathbb{F}_p : \alpha^{p+1} = 1\} & \text{if } t \notin C^0(\mathbb{F}_{p^6}) \text{ and } u \notin D_t; \\ \{\alpha \in \mathbb{F}_{p^2} : \alpha^{p+1} = 1\} & \text{if } t \notin C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t; \\ \{\alpha \in \mathbb{F}_{p^3} : \alpha^{p^3+1} = 1\} & \text{if } t \in C^0(\mathbb{F}_{p^6}) \text{ and } u \notin D_t; \\ \{\alpha \in \mathbb{F}_{p^6} : \alpha^{p^3+1} = 1\} & \text{if } t \in C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t. \end{cases}$$

Proof. This follows from combining Lemma 5.9 with Lemma 5.17. □

5.4. **Determining $[\mathrm{Aut}((M_2, \langle,\rangle_2)) : \mathrm{Aut}((M, \langle,\rangle))]$.**

By Corollary 5.11, Equation (40), and the results in the previous subsection, in particular Corollary 5.18, we immediately obtain the following result.

Lemma 5.19. *Define $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$. Then*

$$|G_{(M,\langle,\rangle)}| = \begin{cases} 2^{e(p)} p^{2(6-d(t))} & \text{if } u \notin D_t; \\ (p+1)p^{2(6-d(t))} & \text{if } t \notin C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t; \\ (p^3+1)p^6 & \text{if } t \in C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t. \end{cases} \tag{43}$$

Recall that $d(t) = 3$ when $t \in C^0(\mathbb{F}_{p^6})$. Combining Lemma 5.19 with Lemma 5.5, and using Remark 5.6, we conclude the following.

Corollary 5.20. *We have*

$$[\mathrm{Aut}((M_2, \langle,\rangle_2)) : \mathrm{Aut}((M, \langle,\rangle))] = [G_{(M_2,\langle,\rangle_2)} : G_{(M,\langle,\rangle)}] =$$

$$\begin{cases} 2^{-e(p)} p^{3+2d(t)}(p+1)(p^2-1)(p^3+1) & \text{if } u \notin D_t; \\ p^{3+2d(t)}(p^2-1)(p^3+1) & \text{if } t \notin C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t; \\ p^9(p+1)(p^2-1) & \text{if } t \in C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t. \end{cases} \tag{44}$$

Now Corollary 2.5(1) and Corollary 5.20 yield the main result of this section, i.e., the mass formula for a supersingular principally polarised abelian threefold $x = (X, \lambda)$ of a-number 1, cf. Theorem B.

Theorem 5.21. *Let $x = (X, \lambda) \in \mathscr{S}_{3,1}$ such that $a(X) = 1$. For $\mu \in P^1(E^3)$, consider the associated polarised flag type quotient $(Y_2, \mu) \to (Y_1, \lambda_1) \to (X, \lambda)$ which is characterised by the pair (t, u) with $t = (t_1 : t_2 : t_3) \in C^0(k)$ and $u = (u_1 : u_2) \in \mathbb{P}^1(k)$. Let $(M_2, \langle,\rangle_2)$ and $(M, \langle,\rangle)$ be the respective polarised Dieudonné modules of Y_2 and X, let D_t be as in Definition 5.16, and let $d(t)$ be as in Definition 5.12. Then*

$$\mathrm{Mass}(\Lambda_x) = \mathrm{Mass}(\Lambda_{3,1}) \cdot [\mathrm{Aut}((M_2, \langle,\rangle_2)) : \mathrm{Aut}((M, \langle,\rangle))] =$$

$$\frac{p^3}{2^{10} \cdot 3^4 \cdot 5 \cdot 7} \begin{cases} 2^{-e(p)} p^{2d(t)}(p^2-1)(p^4-1)(p^6-1) & \text{if } u \notin D_t; \\ p^{2d(t)}(p-1)(p^4-1)(p^6-1) & \text{if } t \notin C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t; \\ p^6(p^2-1)(p^3-1)(p^4-1) & \text{if } t \in C^0(\mathbb{F}_{p^6}) \text{ and } u \in D_t. \end{cases} \tag{45}$$

6. The intersection $C \cap \Delta$

Let $C \subseteq \mathbb{P}^2$ be the Fermat curve defined by the equation $X_1^{p+1} + X_2^{p+1} + X_3^{p+1} = 0$ and $\Delta \subseteq \mathbb{P}^2$ the curve defined in Proposition 5.13.

In the previous section we have seen the inclusion

$$C(\mathbb{F}_{p^2}) \coprod C^0(\mathbb{F}_{p^6}) \coprod C^0(\mathbb{F}_{p^8}) \coprod C^0(\mathbb{F}_{p^{10}}) \subseteq C \cap \Delta$$

for $p > 2$. In this section we study the complement of this inclusion. This is an independent section; the results will not be used elsewhere in this paper.

6.1. **Bounds for the degrees.**

Let $\mathscr{Q}$ denote the set of all conics (including degenerate ones) $Q \subseteq \mathbb{P}^2$ defined over $\mathbb{F}_{p^2}$. Then $\Delta = \cup_{Q\in\mathscr{Q}} Q$. If $t \in C \cap \Delta$, then $t \in C \cap Q$ for some $Q \in \mathscr{Q}$ and hence $\deg_{\mathbb{F}_{p^2}}(t) := [\mathbb{F}_{p^2}(t) : \mathbb{F}_{p^2}] \le 2(p+1)$. We need the following well-known result.

Theorem 6.1 (Kummer's Theorem). *Let K be any field and $n \ge 1$ an integer and $a \in K^\times$. If $(n, \operatorname{char} K) = 1$, and $\mu_n(K^{\mathrm{sep}}) \subseteq K$, and the element $a \pmod{(K^\times)^n}$ in $K^\times/(K^\times)^n$ has order n, then $[K(a^{1/n}) : K] = n$.*

The authors are grateful to Ming-Lun Hsieh for providing the following proposition.

Proposition 6.2. *There exist a conic $Q \in \mathscr{Q}$ and a point $t \in C \cap Q$ such that $\deg_{\mathbb{F}_{p^2}}(t) = (p+1)$.*

Proof. Choose a generator u_1 of $\mathbb{F}_{p^2}^\times$ such that $u_1^p + u_1 = -a \ne 0$. Put $u := a^{-1}u_1$ and let α be a $p+1$-th root of u. As $a \in \mathbb{F}_p^\times$, we have $u^p + u = -1$. Since the element $u \pmod{(\mathbb{F}_{p^2}^\times)^{p+1}}$ in $\mathbb{F}_{p^2}^\times/(\mathbb{F}_{p^2}^\times)^{p+1} = \mathbb{F}_{p^2}^\times/(\mathbb{F}_p^\times)$ has order $p+1$, one has $[\mathbb{F}_{p^2}(\alpha) : \mathbb{F}_{p^2}] = p+1$ by Kummer's Theorem. Let

$$Q : X_1X_2 = uX_3^2 \quad \text{and} \quad t := (\alpha : u\alpha^{-1} : 1).$$

One sees $t \in C$ as $\alpha^{p+1} + (u\alpha^{-1})^{p+1} + 1 = u + u^{p+1} \cdot u^{-1} + 1 = 0$. So $t \in C \cap Q$ and $\deg_{\mathbb{F}_{p^2}}(t) = p+1$. □

The following result, due to Akio Tamagawa, says that the upper bound $2(p+1)$ for $\deg_{\mathbb{F}_{p^2}}(t)$ in $C \cap \Delta$ can be realised.

Proposition 6.3. *There exist a conic $Q \in \mathscr{Q}$ and a point $t \in C \cap Q$ such that $\deg_{\mathbb{F}_{p^2}}(t) = 2(p+1)$.*

Construction. We first consider the case $p = 2$. Let ζ be a primitive fifth roof of unity in $\overline{\mathbb{F}}_2$. Since $(\mathbb{Z}/5\mathbb{Z})^\times \simeq \langle 2 \bmod 5\rangle$, we have $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^4}$. One computes that $(1+\zeta)^3 = 1+\zeta+\zeta^2+\zeta^3 \ne 1$ and $(1+\zeta)^5 = 1+\zeta^2+\zeta^3 \ne 1$. Therefore $1+\zeta$ generates the cyclic group $\mathbb{F}_{2^4}^\times \simeq C_{15}$. Choose $x, y, z \in \overline{\mathbb{F}}_2$ such that $x = 1$, $y^3 = \zeta$ and $z^3 = 1+\zeta$, and put $t := (x : y : z)$; we have $1 + \zeta + (1+\zeta) = 0$. Since $\mathbb{F}_2(z)$ contains $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^4}$, we have $\mathbb{F}_2(z) = \mathbb{F}_{2^4}(z)$. Since $\langle 1+\zeta\rangle = \mathbb{F}_{2^4}^\times$, by Kummer's Theorem, $\mathbb{F}_2(z) = \mathbb{F}_{2^4}(z) = \mathbb{F}_{2^{12}}$ and hence $\deg_{\mathbb{F}_4}(t) = 6 = 2(p+1)$. Since $x, y \in \mathbb{F}_{2^4}$, there exist $a, b, c \in \mathbb{F}_{2^2}$ such that $ax^2 + bxy + cy^2 = 0$. Let $Q \subset \mathbb{P}^2$ be the (degenerate) conic defined by the equation $aX_1^2 + bX_1X_2 + cX_2^2$. Then the point $t \in C \cap Q$ satisfies the desired property.

Assume now that $p > 2$. We would like to find solutions $t = (x : y : z)$ with $x \in \mathbb{F}_{p^{4(p+1)}}^\times$, $y \in \mathbb{F}_{p^4}^\times \setminus \mathbb{F}_{p^2}^\times$, and $z \in \mathbb{F}_{p^2}^\times$ satisfying the desired properties.

Let

$$f : \mathbb{F}_{p^4}^\times \to \mathbb{F}_{p^4}^\times/(\mathbb{F}_{p^4}^\times)^{2(p+1)}$$

be the natural projection; one has $\mathbb{F}_{p^4}^\times/(\mathbb{F}_{p^4}^\times)^{2(p+1)} \simeq C_{2(p+1)}$ as $p \ne 2$. Consider the following three sets:

$$\begin{aligned} & Z := \{z^{p+1} : z \in \mathbb{F}_{p^2}^\times\} \simeq \mathbb{F}_p^\times; \\ & Y := \{y^{p+1} : y \in \mathbb{F}_{p^4}^\times\} \setminus Z; \\ & X := \{\xi \in \mathbb{F}_{p^4}^\times : f(\xi) \text{ generates the cyclic group } C_{2(p+1)}\}. \end{aligned} \tag{46}$$

The sets Y and Z are equipped with an $\mathbb{F}_p^\times$-action and we have

$$|Z| = p-1, \quad |Y| = p^2(p-1), \quad |X| = (p^4-1) \cdot \frac{\varphi(2(p+1))}{2(p+1)}. \tag{47}$$

Let g be the composition

$$g : \mathbb{F}_{p^4}^\times \xrightarrow{N} \mathbb{F}_{p^2}^\times \xrightarrow{\text{proj.}} \mathbb{F}_{p^2}^\times/(\mathbb{F}_p^\times)^2 \simeq C_{2(p+1)},$$

where $N(\alpha) = \alpha^{p^2+1}$ is the norm map. The map f can be identified with g by a suitable choice of the generators. Since the image $g(\mathbb{F}_p^\times)$ is trivial, the image $f(\mathbb{F}_p^\times)$ is also trivial. Thus, X is also equipped with an $\mathbb{F}_p^\times$-action and hence $-X = X$.

We would like to find

$$\eta + \zeta = \xi \tag{48}$$

for some $\eta \in Y$, $\zeta \in Z$ and $\xi \in -X = X$.

Note that X, Y and Z are mutually disjoint: that $Y \cap Z = \emptyset$ follows by definition, and $X \cap Z = \emptyset$ follows from the fact that $\mathbb{F}_p^\times \subseteq \ker(f)$. Since $f((\mathbb{F}_{p^4}^\times)^{p+1})$ is the 2-torsion subgroup of $\mathbb{F}_{p^4}^\times/(\mathbb{F}_{p^4}^\times)^{2(p+1)} \simeq C_{2(p+1)}$ and $f(Y) \subseteq f((\mathbb{F}_{p^4}^\times)^{p+1})$, the image $f(Y)$ contains no generator of $C_{2(p+1)}$. Therefore, we also have $Y \cap X = \emptyset$.

We are working on the space $\mathbb{P} := \mathbb{F}_{p^4}^\times/\mathbb{F}_p^\times \simeq \mathbb{P}^3(\mathbb{F}_p)$. The images of X, Y and Z in $\mathbb{P}$ are written as $\overline{X}$, $\overline{Y}$ and $\overline{Z}$, respectively. So $\overline{Z} = \{\bar{\zeta}\}$ and

$$|\overline{Z}| = 1, \quad |\overline{Y}| = p^2, \quad |\overline{X}| = (p^2+1) \cdot \frac{\varphi(2(p+1))}{2}.$$

For each point $\bar{\eta} \in \overline{Y}$ ($\bar{\eta} \neq \bar{\zeta}$), denote by $L_{\bar{\eta}} \subseteq \mathbb{P}$ the line joining the points $\bar{\eta}$ and $\bar{\zeta}$. To solve (48), it suffices to prove that

$$\left(\bigcup_{\bar{\eta} \in \overline{Y}} L_{\bar{\eta}} \right) \cap \overline{X} \neq \emptyset. \tag{49}$$

This is because if $\bar{\xi} \in L_{\bar{\eta}} \cap \overline{X}$ for some $\bar{\eta} \in \overline{Y}$, then we have $a\eta + b\zeta = c\xi$ with $a, b, c \in \mathbb{F}_p^\times$ and hence $\eta' + \zeta' = \xi'$ with $\eta' \in Y, \zeta' \in Z$ and $\xi' \in X$.

Lemma 6.4. *For any two distinct points $\bar{\eta}_1$ and $\bar{\eta}_2$ of $\overline{Y}$, one has $L_{\bar{\eta}_1} \cap L_{\bar{\eta}_2} = \{\bar{\zeta}\}$.*

Proof. Suppose that $L_{\bar{\eta}_1} \cap L_{\bar{\eta}_2} \supsetneq \{\bar{\zeta}\}$. Then $L_{\bar{\eta}_1} = L_{\bar{\eta}_2}$ and $\bar{\eta}_2 \in L_{\bar{\eta}_1}$. Therefore, $-\eta_2 = a\eta_1 + b\zeta$ for $a, b \in \mathbb{F}_p^\times$ and hence we have

$$\eta_2 + \eta_1' + \zeta' = 0$$

for some $\eta_1' \in Y$ and $\zeta' \in Z$. Now write

$$\eta_2 = (y_2)^{p+1}, \quad \eta_1' = (y_1')^{p+1}, \quad \zeta' = (z')^{p+1},$$

with $y_2, y_1' \in \mathbb{F}_{p^4}^\times \setminus \mathbb{F}_{p^2}^\times$ and $z' \in \mathbb{F}_{p^2}^\times$. That is, we get a point $(y_2 : y_1' : z') \in C(\mathbb{F}_{p^4})$. Since $C(\mathbb{F}_{p^4}) = C(\mathbb{F}_{p^2})$ by Lemma 3.3, we have $y_2, y_1' \in \mathbb{F}_{p^2}$, contradiction. □

By Lemma 6.4,

$$\bigcup_{\bar{\eta} \in \overline{Y}} L_{\bar{\eta}} = \{\bar{\zeta}\} \amalg \coprod_{\bar{\eta} \in \overline{Y}} L_{\bar{\eta}} - \{\bar{\zeta}\},$$

and hence

$$|\bigcup_{\bar{\eta} \in \overline{Y}} L_{\bar{\eta}}| = 1 + |\overline{Y}| \cdot p = p^3 + 1, \quad \text{and} \quad |\mathbb{P} - \bigcup_{\bar{\eta} \in \overline{Y}} L_{\bar{\eta}}| = p^2 + p.$$

To show (48), we check the inequality

$$|\overline{X}| = (p^2+1) \cdot \frac{\varphi(2(p+1))}{2} > p^2 + p \tag{50}$$

for all $p \neq 2$. If $p = 3$, then $|\overline{X}| = 20 > 12$ holds. For $p \geq 5$, by the inequality $\varphi(n) \geq \sqrt{n/2}$, it suffices to show

$$(p^2+1) \cdot \frac{\sqrt{p+1}}{2} > p^2 + p.$$

This follows from

$$(p^2+1)^2(p+1) - 4(p^2+p)^2 = (p+1)(p^4 - 4p^3 - 2p^2 + 1) > 0$$

for $p \geq 5$. Therefore, the inequality (50) holds and we have found η, ζ, ξ as in (48).

Now write

$$\zeta = z^{p+1} \ \ (\text{ for } z \in \mathbb{F}_{p^2}^{\times}), \quad \eta = y^{p+1} \ \ (\text{ for } y \in \mathbb{F}_{p^4}^{\times} \setminus \mathbb{F}_{p^2}^{\times}).$$

Choose an element $x \in \overline{\mathbb{F}}_p$ such that $x^{p+1} = -\xi \in \mathbb{F}_{p^4}^{\times}$. Since the element $\xi \pmod{(\mathbb{F}_{p^4}^{\times})^{p+1}}$ is a generator in $\mathbb{F}_{p^4}^{\times}/(\mathbb{F}_{p^4}^{\times})^{p+1}$, by Kummer's Theorem we have

$$[\mathbb{F}_{p^4}(x) : \mathbb{F}_{p^4}] = p + 1. \tag{51}$$

We claim that $\xi \notin \mathbb{F}_{p^2}^{\times}$. Suppose for contradiction that $\xi \in \mathbb{F}_{p^2}^{\times}$. Then

$$f(\xi) = g(\xi) \in g(\mathbb{F}_{p^2}^{\times}) = (\mathbb{F}_{p^2}^{\times})^2/(\mathbb{F}_p^{\times})^2 \subsetneq \mathbb{F}_{p^2}^{\times}/(\mathbb{F}_p^{\times})^2 \simeq C_{2(p+1)}.$$

Therefore, $f(\xi)$ cannot be a generator of $C_{2(p+1)}$, contradiction. So since $\xi \in \mathbb{F}_{p^4}^{\times} \setminus \mathbb{F}_{p^2}^{\times}$, we have $\mathbb{F}_{p^2}(x) \supset \mathbb{F}_{p^2}(\xi) = \mathbb{F}_{p^4}$. This shows that

$$\mathbb{F}_{p^2}(x) = \mathbb{F}_{p^4}(x), \quad \text{and} \quad [\mathbb{F}_{p^2}(x) : \mathbb{F}_{p^2}] = 2(p+1)$$

by (51). Put $t := (x : y : z) = (x/z : y/z : 1) \in C(\overline{\mathbb{F}}_p)$. Then we get

$$[\mathbb{F}_{p^2}(t) : \mathbb{F}_{p^2}] = 2(p+1). \tag{52}$$

Since $y/z \in \mathbb{F}_{p^4}^{\times} \setminus \mathbb{F}_{p^2}^{\times}$, there exist $b, c \in \mathbb{F}_{p^2}$ such that

$$\left(\frac{y}{z}\right)^2 + b\left(\frac{y}{z}\right) + c = 0, \quad \text{or} \quad y^2 + byz + cz^2 = 0.$$

Let $Q \in \mathscr{Q}$ be the (degenerate) conic defined by the equation $X_2^2 + bX_2X_3 + cX_3^2 = 0$. Then $t \in C \cap Q$ and $\deg_{\mathbb{F}_{p^2}}(t) = 2(p+1)$. This completes the construction. $\square$

6.2. **Estimate of $|C \cap \Delta|$.**

In this subsection, points in C will mean geometric points and $C \cap \Delta$ will mean the set-theoretic intersection. Define

$$\mathscr{X} := \{(t, Q) \in C \times \mathscr{Q} : t \in \mathscr{Q}\}$$

and consider the following natural maps:

$$\begin{array}{ccc} & \mathscr{X} & \\ \swarrow^{\pi} & & \searrow^{q} \\ C & & \mathscr{Q} \end{array}$$

The degree of the map q is $2(p+1)$. For each $Q \in \mathscr{Q}$, the fibre over Q has size

$$2(p+1) - \varepsilon_Q,$$

where $\varepsilon_Q = \sum_{r \geq 2} \varepsilon_{Q,r}$ with

$$\varepsilon_{Q,r} = \#\{t \in C \cap Q : \mathrm{mult}_{C \cap \Delta}(t) = r\} \cdot (r-1).$$

Thus, $|\mathscr{X}| = 2(p+1)(p^{10}+p^8+p^6+p^4+p^2+1) - \varepsilon$, where

$$\varepsilon := \sum_{Q\in\mathscr{Q}} \varepsilon_Q \tag{53}$$

is the error term coming from intersection multiplicities.

Proposition 6.5. *We have $|C\cap\Delta| = p^{11} + o(p^{11}) - \varepsilon$ as $p\to\infty$, where ε is defined in* (53).

Remark 6.6. We expect that $\varepsilon = o(p^{11})$. Then we would have $|C\cap\Delta| = p^{11}+o(p^{11})$ as $p\to\infty$.

Proof. For any integer $i\geq 1$, define

$$C_i := \{t\in C(\overline{\mathbb{F}}_p) : \deg_{\mathbb{F}_{p^2}}(t) = i\}.$$

By Lemma 3.3, we have

$$|C_1| = |C(\mathbb{F}_{p^2})| = p^3+1, \quad |C_3| = |C^0(\mathbb{F}_{p^6})| = p^6+p^5-p^4-p^3,$$
$$|C_4| = |C^0(\mathbb{F}_{p^8})| = p^8-p^6+p^5-p^3, \quad |C_5| = |C^0(\mathbb{F}_{p^{10}})| = p^{10}+p^7-p^6-p^3.$$

For each point $t=(t_1:t_2:t_3)\in C$, the fibre $\pi^{-1}(t)$ is the set $(W_t-\{0\})/\mathbb{F}_{p^2}^\times$, where

$$W_t := \{F\in\mathbb{F}_{p^2}[X_1,X_2,X_3]_2 : F(t)=0\}$$

and where $\mathbb{F}_{p^2}[X_1,X_2,X_3]_2$ denotes the subspace of homogeneous polynomials of degree two. They fit into the following exact sequence

$$0 \longrightarrow W_t \longrightarrow \mathbb{F}_{p^2}[X_1,X_2,X_3]_2 \xrightarrow{\ \mathrm{ev}_t\ } \mathbb{F}_{p^2}\langle t_1^2,t_2^2,t_3^2,t_1t_2,t_1t_3,t_2t_3\rangle \longrightarrow 0.$$

It follows that $\dim(W_t) = 6-d(t)$ and $\pi^{-1}(t)\simeq\mathbb{P}^{5-d(t)}(\mathbb{F}_{p^2})$, where we redefine $d(t)$ as the dimension of $\mathbb{F}_{p^2}\langle t_1^2,t_2^2,t_3^2,t_1t_2,t_1t_3,t_2t_3\rangle$ – even for $p=2$. Therefore, the numbers of fibres over C_i for $i=1,3,4,5$ are

$$(p^8+p^6+p^4+p^2+1), \quad (p^4+p^2+1), \quad (p^2+1), \quad 1,$$

respectively. Then the number of points in $\mathscr{X}$ over the union of C_i for $i=1,3,4,5$ is given by

$$\begin{aligned} A &:= (p^3+1)(p^8+p^6+p^4+p^2+1) + (p^6+p^5-p^4-p^3)(p^4+p^2+1) \\ &\quad + (p^8-p^6+p^5-p^3)(p^2+1) + (p^{10}+p^7-p^6-p^3) \\ &= p^{11}+3p^{10}+2p^9+p^8+3p^7-p^6+p^5-2p^3+p^2+1. \end{aligned}$$

Thus,

$$\begin{aligned} B &:= \#\{(t,Q)\in\mathscr{X} : \deg_{\mathbb{F}_{p^2}}(t) > 5\} = |\mathscr{X}| - A \\ &= p^{11}-p^{10}+p^8-p^7+3p^6+p^5+2p^4+4p^3+p^2+2p+1-\varepsilon. \end{aligned}$$

Finally,

$$\begin{aligned} |C\cap\Delta| &= |\mathrm{Im}(\pi)| = |C_1|+|C_3|+|C_4|+|C_5|+B \\ &= p^{11}+2p^8+2p^6+3p^5+p^4+2p^3+p^2+2p+2-\varepsilon. \end{aligned} \tag{54}$$

□

7. The automorphism groups

In this section we discuss the automorphism groups of principally polarised abelian threefolds (X,λ) over an algebraically closed field $k\supseteq\mathbb{F}_p$ with $a(X)=1$. We shall first focus on an open dense locus in $\mathscr{P}_\mu(a=1)$ (the a-number one locus in $\mathscr{P}_\mu$) in Subsection 7.2 and then discuss a few other cases in Subsections 7.3 and 7.4. To get started, we record some preliminaries in the next subsection.

7.1. **Arithmetic properties of definite quaternion algebras over $\mathbb{Q}$.**

Let C_n denote the cyclic group of order $n \ge 1$. Let $B_{p,\infty}$ denote the definite quaternion $\mathbb{Q}$-algebra ramified exactly at $\{\infty, p\}$. The class number $h(B_{p,\infty})$ of $B_{p,\infty}$ was determined by Deuring, Eichler and Igusa (cf. [9]) as follows:

$$h(B_{p,\infty}) = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right), \tag{55}$$

where $(\cdot/p)$ is the Legendre symbol. If $h(B_{p,\infty}) = 1$, then the type number of $B_{p,\infty}$ is one and hence all maximal orders are conjugate. It follows from (55) that

$$h(B_{p,\infty}) = 1 \iff p \in \{2, 3, 5, 7, 13\}. \tag{56}$$

If $p = 2$, the quaternion algebra $B_{2,\infty} \simeq \left(\frac{-1,-1}{\mathbb{Q}}\right)$ is generated by i, j with relations $i^2 = j^2 = -1$ and $k := ij = -ji$, and the $\mathbb{Z}$-lattice

$$O_{2,\infty} := \mathrm{Span}_{\mathbb{Z}}\left\{1, i, j, \frac{1+i+j+k}{2}\right\} \tag{57}$$

is a maximal order of $B_{2,\infty}$. Moreover,

$$O_{2,\infty}^{\times} = \left\{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\right\} =: E_{24}, \tag{58}$$

and one has $E_{24} \simeq \mathrm{SL}_2(\mathbb{F}_3)$ and $E_{24}/\{\pm 1\} \simeq A_4$.

If $p = 3$, the quaternion algebra $B_{3,\infty} \simeq \left(\frac{-1,-3}{\mathbb{Q}}\right)$ is generated by i, j with relations $i^2 = -1, j^2 = -3$ and $k := ij = -ji$, and the $\mathbb{Z}$-lattice

$$O_{3,\infty} := \mathrm{Span}_{\mathbb{Z}}\left\{1, i, \frac{1+j}{2}, \frac{1+i+j+k}{2}\right\} \tag{59}$$

is a maximal order of $B_{2,\infty}$. Moreover,

$$O_{3,\infty}^{\times} = \langle i, \zeta_6 \rangle =: T_{12}, \quad \zeta_6 = (1+j)/2, \tag{60}$$

and one has $T_{12} \simeq C_4 \rtimes C_3$ and $T_{12}/\{\pm 1\} \simeq D_3$, the dihedral group of order six.

If $p \ge 5$, then $O^\times \in \{C_2, C_4, C_6\}$ for any maximal order O in $B_{p,\infty}$ [17, V Proposition 3.1, p. 145]. Fix O a maximal order in $B_{p,\infty}$ and let $h(O, C_{2n})$ the number of right O-ideal classes $[I]$ with $O_\ell(I)^\times \simeq C_{2n}$, where $O_\ell(I)$ is the left order of I. Then (see [9])

$$h(O, C_4) = \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right) \quad \text{and} \quad h(O, C_6) = \frac{1}{2}\left(1 - \left(\frac{-3}{p}\right)\right). \tag{61}$$

Lemma 7.1.

(1) *Let Q be a definite quaternion $\mathbb{Q}$-algebra and O a $\mathbb{Z}$-order stable under the canonical involution $*$, and let $n \ge 1$ be a positive integer. Then the integral quaternion hermitian group $U(n, O) = \{A \in \mathrm{Mat}_n(O) : A \cdot A^* = \mathbb{I}_n\}$ is equal to the permutation unit group* $\mathrm{diag}(O^\times, \dots, O^\times) \cdot S_n$.

(2) *Let O be a maximal order in $B_{2,\infty}$. Let $m_2 : U(n, O) \to \mathrm{GL}_n(O) \to \mathrm{GL}_n(O/2O)$ be the reduction-modulo-2 map. Then* $\ker(m_2) = \mathrm{diag}(\{\pm 1\}, \dots, \{\pm 1\}) \simeq C_2^n$.

Proof. (1) Let $A = (a_{ij}) \in U(n, O)$. Then since $AA^* = \mathbb{I}_n$, we have $\sum_k a_{ik} a_{ik}^* = 1$ for any $1 \le i \le n$. Since $a_{jk} a_{jk}^* = 0$ or 1, for any $1 \le i \ne n$, there is only one integer $1 \le k \le n$ such that $a_{ik} \ne 0$ and $a_{ik} \in O^\times$. On the other hand, since $A^* A = \mathbb{I}_n$, for any $1 \le k \le n$, there is a only one integer $1 \le i \le n$ such that $a_{ik} \ne 0$ and $a_{ik} \in O^\times$. Thus, $A \in \mathrm{diag}(O^\times, \dots, O^\times) \cdot S_n$. Checking the reverse containment $\mathrm{diag}(O^\times, \dots, O^\times) \cdot S_n \subseteq U(n, O)$ is straightforward.

(2) By (56), we may assume that $O = O_{2,\infty}$. Since the diagonal entries of elements in $\ker(m_2)$ are all not zero, by part (1) we find $\ker(m_2) \subseteq \operatorname{diag}(O^\times, \dots, O^\times)$. Therefore, it suffices to show that the kernel of the reduction-modulo-2 map $m_2 : O^\times \to (O/2O)^\times$ is isomorphic to C_2. Using (58) and $2O = \{a_1 + a_2 i + a_3 j + a_4 k : a_i \in \mathbb{Z},\ a_1 \equiv a_2 \equiv a_3 \equiv a_4 \pmod 2\}$, one checks that indeed $\ker(m_2) = \{\pm 1\} \subseteq O^\times$.

□

Lemma 7.2. *Let D_p be the quaternion division $\mathbb{Q}_p$-algebra and O_p its maximal order. Let Π be a uniformiser of O_p, and put $V_p := 1 + \Pi \operatorname{Mat}_n(O_p) \subseteq \operatorname{GL}_n(O_p)$. If $p \geq 5$, then the torsion subgroup $(V_p)_{\mathrm{tors}}$ of V_p is trivial.*

Proof. Let $\alpha \in (V_p)_{\mathrm{tors}}$; we must show that $\alpha = 1$. Since V_p is a pro-p group, we have $\alpha^{p^r} = 1$ for some $r \geq 1$. By induction, we may assume that $\alpha^p = 1$. Put $A := \mathbb{Z}_p[\alpha] \subseteq \operatorname{Mat}_n(O_p)$ and $K := \mathbb{Q}_p[\alpha] \subseteq \operatorname{Mat}_n(D_p)$. Then $K \simeq \mathbb{Q}_p, \mathbb{Q}_p(\zeta_p)$ or $\mathbb{Q}_p \times \mathbb{Q}_p(\zeta_p)$, where ζ_p is a primitive pth root of unity. Then $K \simeq \mathbb{Q}_p$ if and only if $\operatorname{ord}(\alpha) = 1$.

Suppose first that $K \simeq \mathbb{Q}_p(\zeta_p)$. Write $\alpha - 1 = \Pi\beta$ for some $(0 \neq)\beta \in \operatorname{Mat}_n(O_p)$. The reduced characteristic polynomial of α is $\det(t \cdot \mathbb{I}_{2n} - \iota(\alpha)) = \Phi_p(t)^{2n/(p-1)}$, where $\iota : \operatorname{Mat}_n(O_p) \hookrightarrow \operatorname{Mat}_{2n}(\overline{\mathbb{Q}_p})$ is an algebra embedding and Φ_p is the pth cyclotomic polynomial. Putting $t = 1$, one obtains $\operatorname{Nr}(1 - \alpha) = \Phi_p(1)^{2n/(p-1)} = p^{2n/(p-1)}$, where Nr is the reduced norm from $\operatorname{Mat}(D_p)$ to $\mathbb{Q}_p$. Taking the p-adic valuation v_p of the above equation, we obtain

$$\frac{2n}{p-1} = n + v_p(\operatorname{Nr}(\beta)) \geq n,$$

which is impossible because $p \geq 5$.

Suppose now that $K = \mathbb{Q}_p \times \mathbb{Q}_p(\zeta_p)$ and write $\alpha = (1, \alpha_2)$, where $\alpha_2 \in \mathbb{Q}_p(\zeta_p)$. Since $K \subseteq \operatorname{Mat}_n(D_p) = \operatorname{End}_{D_p}(D_p^n)$, the faithful action of K on D_p^n gives a decomposition $D_p^n = V_1 \oplus V_2$, where $V_1 \simeq D_p^{n_1}$, $V_2 \simeq D_p^{n_2}$, and $n_1, n_2 \geq 1$ with $n_1 + n_2 = n$. Now we regard α_2 as an element in $\operatorname{End}_{D_p}(V_2)$ and write $\alpha_2 - 1 = \Pi\beta_2$ for an element β_2 which is integral over $\mathbb{Z}_p$. By the same argument as in part (1), we obtain

$$\frac{2n_2}{p-1} = n_2 + v_p(\operatorname{Nr}(\beta_2)) \geq n_2,$$

which is again impossible. □

7.2. The region outside the divisor D.

Recall from Subsection 3.1 that E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $\pi_E = -p$. Let $\mu_{\mathrm{can}} \in P(E^3)$ be the threefold self-product of the canonical principal polarisation on E; this is also called the canonical polarisation on E^3.

Theorem 7.3. *Let $x = (X, \lambda) \in \mathscr{S}_{3,1}(k)$ with $a(X) = 1$. For $\mu \in P(E^3)$, consider the associated polarised flag type quotient $(Y_2, p\mu) \to (Y_1, \lambda_1) \to (X, \lambda)$ which is characterised by the pair (t, u) with $t = (t_1 : t_2 : t_3) \in C^0(k)$ and $u = (u_1 : u_2) \in \mathbb{P}^1(k)$. Let $(M_2, \langle , \rangle_2)$ and $(M, \langle , \rangle)$ be the respective polarised Dieudonné modules of (Y_2, μ) and (X, λ), let D_t be as in Definition 5.16 and let $d(t)$ be as in Definition 5.12. Assume that $(t, u) \notin D$, that is, $u \notin D_t$.*

(1) *If $p = 2$, then $\operatorname{Aut}(X, \lambda) \simeq C_2^3$.*
(2) *If $p \geq 5$, or $p = 3$ and $d(t) = 6$, then $\operatorname{Aut}(X, \lambda) \simeq C_2$.*

Proof. By Proposition 3.12, $(Y_2, p\mu) \to (X, \lambda)$ is the minimal isogeny. Therefore,

(62) $$\operatorname{Aut}(X, \lambda) = \{h \in \operatorname{Aut}(Y_2, \mu) : m_p(h) \in G_{(M, \langle , \rangle)}\}.$$

By Proposition 5.10, we have an exact sequence

(63) $$1 \to \ker(\psi_t) \to G_{(M,\langle , \rangle)} \xrightarrow{m_\Pi} \overline{G}_{(M,\langle , \rangle)} \to 1.$$

(1) As $p = 2$, we have $|\Lambda_{3,1}| = 1$ by Hashimoto's result [4]. Thus, we may assume that $(Y_2, \mu) = (E^3, \mu_{\rm can})$, and we have $\mathrm{Aut}(Y_2, \mu) = \mathrm{diag}(O^\times, O^\times, O^\times) \cdot S_3$ by Lemma 7.1 with $O = \mathrm{End}(E)$. As $u \notin D_t$, Corollary 5.18 yields $\overline{G}_{(M,\langle,\rangle)} = \{\pm 1\} = 1$. We see from the proof of Proposition 5.13 that $\ker(\psi_t)$ is the $\mathbb{F}_{p^2}$-subspace generated by $I_{12} + I_{21}$, $I_{13} + I_{31}$ and $I_{23} + I_{32}$ (in the notation of that proof). Therefore,

$$G_{(M,\langle,\rangle)} = \left\{ \begin{pmatrix} \mathbb{I}_3 & 0 \\ S & \mathbb{I}_3 \end{pmatrix} : S = (s_{ij}) \in S_3(\mathbb{F}_{p^2}), s_{ii} = 0 \; \forall 1 \le i \le 3 \right\}. \tag{64}$$

Let $h \in \mathrm{Aut}(X, \lambda) \subseteq \mathrm{diag}(O^\times, O^\times, O^\times) \cdot S_3$. Since $m_2(h)$ has non-zero diagonal entries, $h \in \mathrm{diag}(O^\times, O^\times, O^\times)$. One deduces $m_2(h) = 1$ from (64). Thus, $h \in \ker(m_2) = C_2^3$, by Lemma 7.1. On the other hand, $\ker(m_2) \subseteq \mathrm{Aut}(X, \lambda)$ from (62). This proves (1).

(2) Assume $p \ge 5$. As $u \notin D_t$, Corollary 5.18 implies that $\overline{G}_{(M,\langle,\rangle)} = \{\pm 1\}$. Lemma 7.2 implies that the map $m_\Pi : \mathrm{Aut}(X, \lambda) \to \overline{G}_{(M,\langle,\rangle)}$ is injective, because $\ker(m_\Pi)$ is contained in $(V_p)_{\rm tors}$. Thus, $\mathrm{Aut}(X, \lambda) \simeq C_2$. Now assume $p = 3$ and $d(t) = 6$. In this case $G_{(M,\langle,\rangle)} = \{\pm 1\}$ follows from (63) and Corollary 5.18. By a lemma of Serre [13, p. 207], the map $m_3 : \mathrm{Aut}(X, \lambda) \to G_{(M,\langle,\rangle)}$ is injective and hence $\mathrm{Aut}(X, \lambda) \simeq C_2$.

□

Corollary 7.4. *Let the notation and assumptions be as in Theorem 7.3.*

(1) *If* $p = 2$, *then* $|\Lambda_x| = 4$.
(2) *If* $p = 3$ *and* $d(t) = 6$, *then* $|\Lambda_x| = 3^{11} \cdot 13$.
(3) *If* $p \ge 5$, *then*

$$|\Lambda_x| = \frac{p^{3+2d(t)}(p^2 - 1)(p^4 - 1)(p^6 - 1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}. \tag{65}$$

Proof. All statements follow from Theorems 5.21 and 7.3. For $p = 2$,

$$|\Lambda_x| = \frac{2^3 \cdot 2^9 \cdot 3 \cdot (3 \cdot 5) \cdot (3^2 \cdot 7)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7} = 4. \tag{66}$$

For $p = 3$,

$$|\Lambda_x| = \frac{3^{3+2d(t)} \cdot 2^3 \cdot (2^4 \cdot 5) \cdot (2^3 \cdot 7 \cdot 13)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7} = 3^{2d(t)-1} \cdot 13 = 3^{11} \cdot 13, \tag{67}$$

and we obtain (65) for $p \ge 5$. □

A g-dimensional principally polarised supersingular abelian variety (X, λ) over k is said to be *generic* if the moduli point $\mathrm{Spec}\, k \to \mathscr{S}_{g,1}$ factors through a generic point of $\mathscr{S}_{g,1}$. Recall that the supersingular locus $\mathscr{S}_{g,1} \subseteq \mathscr{A}_{g,1} \otimes \overline{\mathbb{F}}_p$ is a scheme of finite type over $\overline{\mathbb{F}}_p$ which is defined over $\mathbb{F}_p$. Moreover, every geometrically irreducible component of $\mathscr{S}_{g,1}$ is defined over $\mathbb{F}_{p^2}$, cf. [24, Section 2.2].

Oort's conjecture [1, Problem 4] asserts that for any integer $g \ge 2$ and any prime number p, every generic g-dimensional principally polarised supersingular abelian variety (X, λ) over k of characteristic p has automorphism group $\{\pm 1\}$. Oort's conjecture fails with counterexamples in $(g, p) = (2, 2)$ or $(g, p) = (3, 2)$; see [7, 15].

For fixed $g \ge 2$ and prime number p, consider the refined Oort conjecture:

$(\mathrm{O})_{g,p}$: Every generic g-dimensional principally polarised supersingular abelian variety (X, λ) over k of characteristic p has automorphism group $\{\pm 1\}$.

Corollary 7.5. *Let (X,λ) be a generic principally polarised supersingular abelian threefold over k of characteristic $p>0$. Then*

$$\mathrm{Aut}(X,\lambda)\simeq\begin{cases} C_2^3 & \text{for } p=2;\\ C_2 & \text{for } p\ge 3.\end{cases}$$

Proof. This follows immediately from Theorem 7.3. □

In other words, Oort's Conjecture $(\mathrm{O})_{3,p}$ holds precisely when $p\neq 2$.

Remark 7.6. (1) It is shown [15, Theorem 5.6, p. 270] that if (X,λ) is a principally polarised supersingular abelian threefold over k of characteristic 2, then $\mathrm{Aut}(X,\lambda)\supseteq C_2^3$. By Corollary 7.5, the smallest group C_2^3 also appears as $\mathrm{Aut}(X,\lambda)$ for some (X,λ). We have seen that the unique member (E^3,μ_{can}) in $\Lambda_{3,1}$ has automorphism group $E_{24}^3\rtimes S_3$ (of order $2^{10}\cdot 3^4$). We expect that $2^{10}\cdot 3^4$ is the maximal order of automorphism groups of *all* principally polarised abelian threefolds over k of any characteristic (including zero).

(2) According to Hashimoto's result [4], we have $|\Lambda_{3,1}|=2$ for $p=3$. In this case, we have two isomorphism classes, represented by (E^3,μ_{can}) and (E^3,μ). Using Lemma 7.1, we compute $|\mathrm{Aut}(E^3,\mu_{\mathrm{can}})|=2^7\cdot 3^4$ and conclude $|\mathrm{Aut}(E^3,\mu)|=2^7\cdot 3^4$ from the mass formula $\mathrm{Mass}(\Lambda_{3,1})=1/(2^6\cdot 3^4)$.

7.3. The region where $t\notin C(\mathbb{F}_{p^6})$ and $(t,u)\in D$.

In this subsection we consider the region $(t,u)\in D$ and assume that $t\notin C(\mathbb{F}_{p^6})$. This extends the region considered in Subsection 7.2.

Lemma 7.7. *Let $(X,\lambda)\in\mathscr{S}_{3,1}(k)$ with $a(X)=1$. If $p\ge 3$ and $\mathrm{Aut}(X,\lambda)\subseteq C_{p+1}$, then $\mathrm{Aut}(X,\lambda)\subseteq\{C_2,C_4,C_6\}$.*

Proof. Suppose that $\mathrm{Aut}(X,\lambda)=C_{2d}$ with $2d|(p+1)$. Then we have a ring homomorphism $\mathbb{Z}[C_{2d}]\to\mathrm{End}(X)$ which maps C_{2d} bijectively to $\mathrm{Aut}(X,\lambda)$. The $\mathbb{Q}$-algebra homomorphism

$$\mathbb{Q}[C_{2d}]=\prod_{d'|2d}\mathbb{Q}[\zeta_{d'}]\to\mathrm{End}^0(X)=\mathrm{Mat}_3(B_{p,\infty})$$

factors through an injective $\mathbb{Q}$-algebra homomorphism

$$\prod_{i=1}^r\mathbb{Q}[\zeta_{d_i}]\hookrightarrow\mathrm{End}^0(X)=\mathrm{Mat}_3(B_{p,\infty}),$$

where $\{d_i|2d\}\subseteq\{d'|2d\}$. Since the composition gives an embedding $C_{2d}\hookrightarrow\mathrm{Aut}(X)$, the integers $\{d_i\}$ satisfy $\mathrm{lcm}(d_1,\dots,d_r)=2d$. Since $p\nmid 2d$, the algebra $\mathbb{Z}_p[C_{2d}]$ is étale over $\mathbb{Z}_p$ and is the maximal order in $\mathbb{Q}_p[C_{2d}]$. This gives rise to an embedding $\prod_{i=1}^r\mathbb{Z}[\zeta_{d_i}]\otimes\mathbb{Z}_p\hookrightarrow\mathrm{End}(X)\otimes\mathbb{Z}_p\simeq\mathrm{End}(X[p^\infty])$. Thus, the decomposition $X[p^\infty]=H_1\times\cdots\times H_r$ into a product of supersingular p-divisible groups shows $a(X)\ge r$ and hence $r=1$. Therefore, there is a $\mathbb{Q}$-algebra embedding of $\mathbb{Q}(\zeta_{2d})$ into $\mathrm{Mat}_3(B_{p,\infty})$. This implies that $\varphi(2d)|6$ (where φ denotes Euler's totien function) and hence $2d\in\{2,4,6,14,18\}$.

If $2d=14$, then $p\equiv -1 \pmod 7$ and $\mathrm{ord}(p)=2$ in $(\mathbb{Z}/7\mathbb{Z})^\times$. This gives rise to an embedding $\mathbb{Z}[\zeta_{14}]\otimes\mathbb{Z}_p=\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}\hookrightarrow\mathrm{End}(X[p^\infty])$ and hence $a(X)=3$, a contradiction. If $2d=18$, then $p\equiv -1 \pmod 9$ and $\mathrm{ord}(p)=2$ in $(\mathbb{Z}/9\mathbb{Z})^\times$. Similarly, we get an embedding $\mathbb{Z}[\zeta_{18}]\otimes\mathbb{Z}_p=\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}\hookrightarrow\mathrm{End}(X[p^\infty])$ and $a(X)=3$, again a contradiction. □

Recall that $\mathbb{F}_{p^2}^1:=\{\alpha\in\mathbb{F}_{p^2}^\times:\alpha^{p+1}=1\}\simeq C_{p+1}$ denotes the group of norm one elements in $\mathbb{F}_{p^2}^\times$.

Theorem 7.8. *Let the notation be as in Theorem 7.3. Assume that* $(t,u) \in D$ *and* $t \notin C(\mathbb{F}_{p^6})$.

(1) *If* $p = 2$, *then* $\mathrm{Aut}(X,\lambda) \simeq C_2^3 \times C_3$.
(2) *If* $p = 3$ *and* $d(t) = 6$, *then* $\mathrm{Aut}(X,\lambda) \in \{C_2, C_4\}$.
(3) *For* $p \geq 5$, *we have the following cases:*
 (i) *If* $p \equiv -1 \pmod 4$, *then* $\mathrm{Aut}(X,\lambda) \in \{C_2, C_4\}$.
 (ii) *If* $p \equiv -1 \pmod 3$, *then* $\mathrm{Aut}(X,\lambda) \in \{C_2, C_6\}$.
 (iii) *If* $p \equiv 1 \pmod{12}$, *then* $\mathrm{Aut}(X,\lambda) \simeq C_2$.

Proof. (1) By Hashimoto's result [4], we may assume that $(Y_2,\mu) = (E^3, \mu_{\mathrm{can}})$, and by Lemma 7.1 we have $\mathrm{Aut}(Y_2,\mu) = \mathrm{diag}(O^\times, O^\times, O^\times) \cdot S_3$. Then

$$\begin{aligned}
\mathrm{Aut}(X,\lambda) &= \left\{ h \in \mathrm{Aut}(Y_2,\mu) : m_2(h) = \begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix}, a \in \mathbb{F}_4^1 \right\} \\
&= \left\{ h \in \mathrm{diag}(O^\times, O^\times, O^\times) : m_2(h) = \begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix}, a \in \mathbb{F}_4^1 \right\} \\
&= \left\{ \begin{pmatrix} \pm w^j & & \\ & \pm w^j & \\ & & \pm w^j \end{pmatrix} : 0 \leq j \leq 5 \right\} \simeq C_2^3 \times C_3,
\end{aligned}$$

where $w = (1+i+j+k)/2$ satisfies $w^6 = 1$.

(2) In this case, $\overline{G}_{(M,\langle,\rangle)} = \mathbb{F}_9^1 \simeq C_4$ by Corollary 5.18. The proof then follows from the fact that the reduction-modulo-3 map is injective.

(3) In this case, $\overline{G}_{(M,\langle,\rangle)} = \mathbb{F}_{p^2}^1 \simeq C_{p+1}$ by Corollary 5.18. It follows from Lemma 7.2 that $\mathrm{Aut}(X,\lambda)$ can be identified with a subgroup of $\overline{G}_{(M,\langle,\rangle)} \simeq C_{p+1}$ as $p \geq 5$. By Lemma 7.7, $\mathrm{Aut}(X,\lambda) \in \{C_2, C_4, C_6\}$. The assertions for (i), (ii) and (iii) follow from this assertion.

□

Write D_μ for $D \subseteq \mathscr{P}_\mu(a=1)$ to emphasise its dependence on $\mu \in P(E^3)$. Recall that $\Psi_\mu : \mathscr{P}_\mu \to \mathscr{S}_{3,1}$ is the map $(Y_\bullet, \rho_\bullet) \mapsto (Y_0, \lambda_0)$. Put $D_{\mu, C(\mathbb{F}_{p^6})^c} := \{(t,u) \in D_\mu : t \notin C(\mathbb{F}_{p^6})\}$.

Let Λ_1 denote the set of $\mathbb{F}_{p^2}$-isomorphism classes of supersingular elliptic curves E' over $\mathbb{F}_{p^2}$ with Frobenius endomorphism $\pi_{E'} = -p$. This set is in bijection with the set $\mathrm{Cl}(B_{p,\infty})$ of right O-ideal classes for a fixed maximal order O in $B_{p,\infty}$, cf. [18, Theorem 2.1] and [23, Theorem 2.2].

Proposition 7.9.

(1) *If* $p = 3$ *and* $d(t) = 6$, *then for all* $(X,\lambda) \in \Psi_\mu(D_{\mu, C(\mathbb{F}_{p^6})^c})$ *with* $\mu = \mu_{\mathrm{can}}$, *one has* $\mathrm{Aut}(X,\lambda) \simeq C_4$.
(2) *If* $p \geq 5$ *and* $p \equiv 3 \pmod 4$, *then there exists* $\mu \in P(E^3)$ *such that for all* $(X,\lambda) \in \Psi_\mu(D_{\mu, C(\mathbb{F}_{p^6})^c})$ *one has* $\mathrm{Aut}(X,\lambda) \simeq C_4$.
(3) *If* $p \geq 5$ *and* $p \equiv 2 \pmod 3$, *then there exists* $\mu \in P(E^3)$ *such that for all* $(X,\lambda) \in \Psi_\mu(D_{\mu, C(\mathbb{F}_{p^6})^c})$ *one has* $\mathrm{Aut}(X,\lambda) \simeq C_6$.
(4) *If* $p \geq 11$, *then there exists* $\mu \in P(E^3)$ *such that for all* $(X,\lambda) \in \Psi_\mu(D_{\mu, C(\mathbb{F}_{p^6})^c})$ *one has* $\mathrm{Aut}(X,\lambda) \simeq C_2$.

Proof. We use the results from Subsection 7.1. If $p = 3$, then $O^\times = \mathrm{Aut}(E) = \langle i, \zeta_6 \rangle$. If $p \geq 5$ and $p \equiv 2 \pmod 3$ (resp. $p \equiv 3 \pmod 4$), there exists a unique supersingular elliptic curve E' in Λ_1 such that $O^\times := \mathrm{Aut}(E') \simeq C_6$ (resp. C_4). If $p \geq 11$, then there exists a supersingular elliptic curve E' in Λ_1 such that $O^\times := \mathrm{Aut}(E') \simeq C_2$. Note that if $p \ge 11$ then either $h(B_{p,\infty}) \ge 2$ or $p \equiv 1 \pmod{12}$. For cases (2), (3), and (4) we choose a polarisation $\mu \in P(E^3)$ such that $(E^3, \mu) \simeq (E'^3, \mu'_{\mathrm{can}})$, where μ'_{can} is the canonical polarisation on E'^3 as before. (In case (1) $\mu = \mu_{\mathrm{can}}$ is the unique choice of polarisation.) Then using the same argument as in Theorem 7.8, the automorphism group $\mathrm{Aut}(X, \lambda)$ for $(X, \lambda) \in \Psi_\mu(D_{\mu, C(\mathbb{F}_{p^6})^c})$ consists of elements of the form $\mathrm{diag}(a, a, a)$ with $a \in O^\times$ satisfying $m_3(a) \in \mathbb{F}_4^1$ if $p = 3$ (resp. $m_\Pi(a) \in \mathbb{F}_{p^2}^1$ if $p \ge 5$). If $p = 3$, we have $m_3(\langle i \rangle) = C_4$. If $p \equiv 3 \pmod 4$, we have $m_\Pi(\langle i \rangle) = C_4$. If $p \equiv 2 \pmod 3$, we have $m_\Pi(\langle \zeta_6 \rangle) = C_6$. Thus, $\mathrm{Aut}(X, \lambda) \simeq C_4$ for $p \equiv 3 \pmod 4$ and $\mathrm{Aut}(X, \lambda) \simeq C_6$ for $p \equiv 2 \pmod 3$. In case (4), we have $\mathrm{Aut}(X, \lambda) \simeq C_2$. □

Remark 7.10. (1) Given Proposition 7.9, it remains to check whether the group C_2 also appears as $\mathrm{Aut}(X, \lambda)$ in the region $\Psi_\mu(D_{\mu, C(\mathbb{F}_{p^6})^c})$ for some $\mu \in P(E^3)$ when $p = 3, 5, 7$.
(2) We assume the condition $d(t) = 6$ when $p = 3$ in Theorems 7.3 and 7.8. It remains to determine which other automorphism groups occur if this condition is dropped.

7.4. **The superspecial case.**

As we have seen in the previous subsection, to investigate the automorphism groups in some special region of $\mathscr{P}_\mu(a = 1)$, the knowledge of automorphism groups arising from the superspecial locus $\Lambda_{3,1}$ also plays an important role. In this subsection, we discuss only preliminary results on the automorphism groups of members in $\Lambda_{3,1}$. A complete list of all possible automorphism groups requires much more work; see Question (2) below.

We briefly recall some results. For $p = 2$, we have $|\Lambda_{3,1}| = 1$ and the unique isomorphism class represented by (X, λ) has automorphism group $E_{24}^3 \rtimes S_3$. For $p = 3$, we have $|\Lambda_{3,1}| = 2$ by Hashimoto's result. In this case, the two isomorphism classes are represented by $(E^3, \mu_{\mathrm{can}})$ and (E^3, μ), respectively, and we have $\mathrm{Aut}(E^3, \mu_{\mathrm{can}}) = T_{12}^3 \rtimes S_3$ so $|\mathrm{Aut}(E^3, \mu)| = 2^7 \cdot 3^4$, cf. Remark 7.6. For $p \ge 5$, the following non-abelian groups occur:

$$\begin{cases} C_2^3 \rtimes S_3 & \text{for } p \equiv 1 \pmod{12}; \\ C_4^3 \rtimes S_3 & \text{for } p \equiv 3 \pmod 4; \\ C_6^3 \rtimes S_3 & \text{for } p \equiv 2 \pmod 6, \end{cases}$$

cf. Lemma 7.1.

Unlike the a-number one case, it is more difficult to construct a member (X, λ) in $\Lambda_{3,1}$ such that $\mathrm{Aut}(X, \lambda) \simeq C_2$. However, it is expected that when p goes to infinity, most members of $\Lambda_{g,1}$ have automorphism group C_2. The following result confirms this expectation for $g = 3$, based on Hashimoto's result [4].

Proposition 7.11. *Let* $\Lambda_{3,1}(C_2) := \{(X, \lambda) \in \Lambda_{3,1} : \mathrm{Aut}(X, \lambda) \simeq C_2\}$. *Then*

$$\frac{|\Lambda_{3,1}(C_2)|}{|\Lambda_{3,1}|} \to 1 \quad \textit{as } p \to \infty. \tag{68}$$

Proof. Put $h_2(p) := |\Lambda_{3,1}(C_2)|$. By [4, Main Theorem], the main term of $h(p) := |\Lambda_{3,1}|$ is $H_1(p) := (p-1)(p^2+1)(p^3-1)/(2^9 \cdot 3^4 \cdot 5 \cdot 7)$ and the error term $\varepsilon(p)$ is $O(p^5)$. Observe that $\mathrm{Mass}(\Lambda_{3,1}) = H_1(p)/2$. If $(X, \lambda) \notin \Lambda_{3,1}(C_2)$, then $|\mathrm{Aut}(X, \lambda)| \ge 4$. This gives the inequality

$$\mathrm{Mass}(\Lambda_{3,1}) \le \frac{h_2(p)}{2} + \frac{h(p) - h_2(p)}{4} = \frac{h_2(p)}{4} + \frac{H_1(p) + \varepsilon(p)}{4}.$$

From $\mathrm{Mass}(\Lambda_{3,1}) = H_1(p)/2$ one deduces that $h_2(p) \ge H_1(p) - \varepsilon(p)$. Since

$$\frac{H_1(p) - \varepsilon(p)}{H_1(p) + \varepsilon(p)} \le \frac{|\Lambda_{3,1}(C_2)|}{|\Lambda_{3,1}|} \le 1 \quad \text{and} \quad \frac{H_1(p) - \varepsilon(p)}{H_1(p) + \varepsilon(p)} \to 1 \quad \text{as } p \to \infty,$$

we get the assertion (68). □

We end the paper with some open problems.

Questions. (1) Let X be a principally polarisable supersingular abelian variety over k, and let $P(X)$ be the set of isomorphism classes of principally polarisations on X. The mass of $P(X)$ is defined as

$$\mathrm{Mass}(P(X)) := \sum_{\lambda\in P(X)} \frac{1}{|\operatorname{Aut}(X,\lambda)|}. \tag{69}$$

One would like to find a mass formula for $\mathrm{Mass}(P(X))$ and understand the relationship between the sets $P(X)$ and $\Lambda_{(X,\lambda)}$ for a polarisation $\lambda \in P(X)$ when $\dim(X) = 3$. Ibukiyama [7] studied $P(X)$ for $\dim(X) = 2$. He gave a mass formula for $\mathrm{Mass}(P(X))$ and also showed that $P(X)$ is in bijection with the set $\Lambda_{(X,\lambda)}$ for any principal polarisation λ on X. Note that not every supersingular abelian threefold is principally polarisable: by [12, Theorem 10.5, p. 71] we see that the supersingular locus $S_{3,d} \subseteq \mathscr{A}_{3,d} \otimes \overline{\mathbb{F}}_p$ is three-dimensional if d is divisible by a high power of p, while $\dim(\mathscr{S}_{3,1}) = 2$.

(2) In order to study the automorphism groups of (X,λ) with $a(X) = 2$, we also need to study the automorphism groups arising from the non-principal genus $\Lambda_{3,p}$; see Proposition 3.12. Do we have an asymptotic result similar to Proposition 7.11 for $\Lambda_{3,p}$? What are the possible automorphism groups arising from $\Lambda_{3,1}$ or from $\Lambda_{3,p}$? We refer to Ibukiyama-Katsura-Oort [8], Katsura-Oort [10] and Ibukiyama [6] for detailed investigations for the principal genus case $\Lambda_{2,1}$ and the non-principal genus case $\Lambda_{2,p}$. Observe that there are natural maps $\Lambda_{2,1} \times \Lambda_{1,1} \to \Lambda_{3,1}$ and $\Lambda_{2,p} \times \Lambda_{1,1} \to \Lambda_{3,p}$. Following the references mentioned above, these maps already produce many automorphism groups of members of $\Lambda_{3,1}$ and $\Lambda_{3,p}$.

(3) We say two polarised abelian varieties (X_1,λ_1) and (X_2,λ_2) are isogenous, denoted $(X_1,\lambda_1) \sim (X_2,\lambda_2)$, if there exists a quasi-isogeny $\varphi : X_1 \to X_2$ such that $\varphi^*\lambda_2 = \lambda_1$. Let $x = (X_0,\lambda_0) \in \mathscr{A}_{g,1}(k)$ be a geometric point. Define

$$\Lambda_x := \{(X,\lambda) \in \mathscr{A}_{g,1}(k) : (X,\lambda) \sim (X_0,\lambda_0) \text{ and } (X,\lambda)[p^\infty] \simeq (X_0,\lambda_0)[p^\infty]\}. \tag{70}$$

Using the foliation structure on Newton strata due to Oort [16], one can show that the set Λ_x is finite. Note that any two principally polarised supersingular abelian varieties over k are isogenous, cf. [19, Corollary 10.3]. Thus, the definition of Λ_x in (70) coincides that of Λ_x in (3) when $x \in \mathscr{S}_{g,1}$. That is, a mass function

$$\mathrm{Mass} : \mathscr{A}_{g,1}(k) \to \mathbb{Q}, \quad x \mapsto \mathrm{Mass}(\Lambda_x) \tag{71}$$

would extend the mass function $\mathrm{Mass}(x) := \mathrm{Mass}(\Lambda_x)$ defined on $\mathscr{S}_{g,1}(k)$ as before. One would like to compute or study the properties of such a mass function on $\mathscr{A}_{g,1}(k)$, starting in low genus g. This problem may require developing more explicit descriptions of the foliation structure on Newton strata.

References

[1] S. J. Edixhoven, B. J. J. Moonen, and F. Oort, *Open problems in algebraic geometry*, Bull. Sci. Math. **125** (2001), no. 1, 1–22.

[2] Torsten Ekedahl, *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), no. 2, 151–178.

[3] Shushi Harashita, *Ekedahl-Oort strata contained in the supersingular locus and Deligne-Lusztig varieties*, J. Algebraic Geom. **19** (2010), no. 3, 419–438.

[4] Ki-ichiro Hashimoto, *Class numbers of positive definite ternary quaternion Hermitian forms*, Proc. Japan Acad. Ser. A Math. Sci. **59** (1983), no. 10, 490–493.

[5] Ki-ichiro Hashimoto and Tomoyoshi Ibukiyama, *On class numbers of positive definite binary quaternion Hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), no. 3, 549–601.

[6] Tomoyoshi Ibukiyama, *On automorphism groups of positive definite binary quaternion Hermitian lattices and new mass formula*, Automorphic forms and geometry of arithmetic varieties, Adv. Stud. Pure Math., vol. 15, Academic Press, Boston, MA, 1989, pp. 301–349.

[7] ______, *Principal polarizations of supersingular abelian surfaces*, to appear in J. Math. Soc. Japan (2019).

[8] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152.

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

[10] Toshiyuki Katsura and Frans Oort, *Families of supersingular abelian surfaces*, Compositio Math. **62** (1987), no. 2, 107–167.

[11] ______, *Supersingular abelian varieties of dimension two or three and class numbers*, Algebraic geometry, Sendai, 1985, Adv. Stud. Pure Math., vol. 10, North-Holland, Amsterdam, 1987, pp. 253–281.

[12] Ke-Zheng Li and Frans Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998.

[13] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay, 2008, With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[14] Frans Oort, *Which abelian surfaces are products of elliptic curves?*, Math. Ann. **214** (1975), 35–47.

[15] ______, *Hyperelliptic supersingular curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 247–284.

[16] ______, *Foliations in moduli spaces of abelian varieties*, J. Amer. Math. Soc. **17** (2004), no. 2, 267–296.

[17] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.

[18] Jiang Wei Xue and Chia-Fu Yu, *On counting certain abelian varieties over finite fields*, Acta Math. Sin. (Engl. Ser.) (2019 (to appear in print)).

[19] Chia-Fu Yu, *On the supersingular locus in Hilbert-Blumenthal 4-folds*, J. Algebraic Geom. **12** (2003), no. 4, 653–698.

[20] ______, *On the mass formula of supersingular abelian varieties with real multiplications*, J. Aust. Math. Soc. **78** (2005), no. 3, 373–392.

[21] ______, *The supersingular loci and mass formulas on Siegel modular varieties*, Doc. Math. **11** (2006), 449–468.

[22] ______, *On finiteness of endomorphism rings of abelian varieties*, Math. Res. Lett. **17** (2010), no. 2, 357–370.

[23] ______, *Simple mass formulas on Shimura varieties of PEL-type*, Forum Math. **22** (2010), no. 3, 565–582.

[24] ______, *On fields of definition of components of the Siegel supersingular locus*, Proc. Amer. Math. Soc. **145** (2017), no. 12, 5053–5058.

[25] Chia-Fu Yu and Jeng-Daw Yu, *Mass formula for supersingular abelian surfaces*, J. Algebra **322** (2009), no. 10, 3733–3743.

MATHEMATICAL INSTITUTE, UTRECHT UNIVERSITY, UTRECHT, THE NETHERLANDS AND DEPARTMENT OF MATHEMATICS, STOCKHOLM UNIVERSITY, STOCKHOLM, SWEDEN
E-mail address: `V.Z.Karemaker@uu.nl`

GRADUATE SCHOOL OF MATHEMATICS, NAGOYA UNIVERSITY, NAGOYA, JAPAN
E-mail address: `yobuko@math.nagoya-u.ac.jp`

INSTITUTE OF MATHEMATICS, ACADEMIA SINICA AND NATIONAL CENTER FOR THEORETIC SCIENCES, TAIPEI, TAIWAN
E-mail address: `chiafu@math.sinica.edu.tw`