Products and Polarizations of Super-Isolated Abelian Varieties

Stefano Marseglia, Travis Scholl

August 14, 2020

Abstract

In this paper we study super-isolated abelian varieties, that is, abelian varieties over finite fields whose isogeny class contains a single isomorphism class. The goal of this paper is to (1) characterize whether a product of super-isolated varieties is super-isolated, and (2) characterize which super-isolated abelian varieties admit principal polarizations, and how many up to polarized isomorphisms.

1 Introduction

An abelian variety $A/\mathbb{F}_q$ is *super-isolated* if its $\mathbb{F}_q$-isogeny class contains only the isomorphism class of A. Hence a super-isolated $A/\mathbb{F}_q$ is determined up to isomorphism by the characteristic polynomial of its Frobenius endomorphism. In [Sch19], the second author introduced super-isolated elliptic curves and surfaces in the context of cryptography, and in [Sch20] this was generalized to higher dimensional simple super-isolated abelian varieties. In this paper we continue on this path. In particular we focus on two questions:

1. When is the product of super-isolated varieties super-isolated?
2. When does a super-isolated variety admit a principal polarization and, if that is the case, how many are there up to polarized isomorphism?

In [Sch19] it is showed that simple super-isolated abelian varieties are rare, in the sense that the for most finite fields $\mathbb{F}_q$ there are no super-isolated varieties over $\mathbb{F}_q$. Trying to generalize this statement to non-simple abelian varieties leads to the first question. Our methods show that super-isolated products are even rarer and can be enumerated as efficiently as super-isolated simple varieties.

The second question is related to the problem of determining whether an abelian variety is a Jacobian of a curve. This is in general a difficult question, see [MN02] for the case of abelian surfaces. In the case of super-isolated abelian varieties all the arithmetic information is encoded in the Weil polynomial determining the isogeny class. Since every Jacobian admits a canonical

principal polarization, the second question is a first step towards characterizing super-isolated Jacobians.

In this paper, we first presents some general results about products of super-isolated abelian varieties, see Section 3.1. Then, in order to give answers to our questions, we focus on a class of abelian varieties that we call *ideal*, see Definition 14. For the category of such abelian varieties, we have functorial descriptions in terms of finitely generated free $\mathbb{Z}$-modules with a "Frobenius-like" endomorphism, see [Del69, CS15]. In the ordinary case, we can describe also dual varieties and polarizations, see [How95]. We exploit these descriptions in Theorem 16 where we exhibit a criterion to answer Question 1. It turns out that the technology developed to prove Theorem 16 in Sections 2 and 3 allows us to show that, for any fixed dimension, there are only finitely many super-isolated ideal abelian varieties that are not simple, see Corollary 19. In Section 3.3 we give an algorithm to enumerate them and we produce complete lists of such abelian varieties that are a product of elliptic curves and surfaces, see Algorithm 1 and Table 1.

In Section 4, we characterize which simple ordinary super-isolated varieties admit a principal polarization, see Theorem 27. We also show that if such a polarization exists, then it is unique, see Theorem 35. Moreover in Corollary 36 and Remark 37 we discuss the product case. These results give an answer to Question 2.

In Section 5 we apply the theory developed in the previous sections to prove some properties of super-isolated Jacobians, see Proposition 38.

In this paper, all morphisms between abelian varieties over a field k are defined over the same field k.

Acknowledgements

The first author was partially supported by the Max Planck Society (Postdoctoral Fellowship) and by the Dutch Research Council (NWO grant 613.001.651). The second author was partially supported by Alfred P. Sloan Foundation (grant number G-2014-13575). The second author would also like to thank Alice Silverberg and Karl Rubin for helpful discussions on abelian varieties and class field theory. The authors thank Jonas Bergström, Valentijn Karemaker, Christophe Ritzenthaler and Shahed Sharif for comments, and Everett Howe helpful discussion that lead to the results contained in Section 3.1.

2 Products of Weil generators

Weil generators in CM fields have been studied in [Sch19] and [Sch20]. They represent the Frobenius endomorphism of a super-isolated abelian variety. The purpose of this section is to generalize the notion of a Weil generator to a product of CM fields and give quantitative results. For a CM field K we will denote its CM involution by $\bar{\cdot}$.

Definition 1. Let K be a product of CM fields $K = K_1 \times \cdots \times K_n$. We say $\alpha \in K$ is a *Weil generator for* K if $\alpha\overline{\alpha} \in \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[\alpha, \overline{\alpha}]$, where $\mathcal{O}_K = \prod \mathcal{O}_{K_i}$. That is, $\alpha\overline{\alpha}$ lies in the image of the diagonal embedding $\mathbb{Z} \to K$, and the subring generated by α and $\overline{\alpha}$ is the integral closure of $\mathbb{Z}$ in K.

Let K be a CM-field. Denote by F the fixed field of the CM involution of K. Fix $\gamma \in K$ satisfying $\mathcal{O}_K = \mathcal{O}_F[\gamma]$. Let R be the set of all $\eta \in F$ such that $\mathcal{O}_F = \mathbb{Z}[\eta]$. Choose a set $T \subset R$ of representatives of $R/\sim$, where $\eta_1 \sim \eta_2$ if $\eta_1 - \eta_2 \in \mathbb{Z}$. If γ does not exist or $T = \emptyset$, then K has no Weil generators. Indeed, if α is a Weil generator for K then we could choose $\gamma = \alpha$ and $(\alpha + \overline{\alpha}) \in R$, see [Sch20, Lemma 3.13]. Given the order $\mathcal{O}_F$, the set T is always finite and can be effectively computed, see [Győ76]. By [Sch20, Lemma 3.15] every Weil generator $\alpha \in K$ can be written as

$$\alpha = \frac{u(\gamma - \overline{\gamma}) + \eta + a}{2} \tag{1}$$

for a unique triple $(u, \eta, a) \in \mathcal{O}_F^\times \times T \times \mathbb{Z}$.

Example 2. Let $K = \mathbb{Q}(i)$ and put $\gamma = i$ and $T = \{0\}$. Then every Weil generator is of the form $(\pm 2i + a)/2$ for some integer $a \in \mathbb{Z}$. Alternatively, every Weil generator can also be written as $b \pm i$ for some $b \in \mathbb{Z}$.

Example 3. Let $K = \mathbb{Q}(\zeta_5)$ and put $\gamma = \zeta_5$ and $T = \{(1+\sqrt{5})/2, (1-\sqrt{5})/2\}$. Then every generator can be expressed as $(u(\zeta_5 - \bar{\zeta}_5) + (1 \pm \sqrt{5})/2 + a)/2$ for some $u \in \mathcal{O}^\times_{\mathbb{Q}(\sqrt{5})}$ and $a \in \mathbb{Z}$.

Lemma 4. *Let K be a CM field with maximal real subfield F, and $\alpha \in K$ a Weil generator of K. Fix $\eta \in T$ and $a \in \mathbb{Z}$ as in Equation* (1)*. If $q = \alpha\overline{\alpha}$, then*

$$\operatorname{Norm}_{F/\mathbb{Q}}\left((\eta + a)^2 - 4q\right) = \frac{\operatorname{Disc}_{K/\mathbb{Q}}}{\operatorname{Disc}^2_{F/\mathbb{Q}}}.$$

Proof. Let $g = \deg F$ and $\beta = \alpha + \overline{\alpha}$. By [Mar18a, Ch.2 Ex. 23],

$$\operatorname{Disc}_{K/\mathbb{Q}}(1, \ldots, \beta^{g-1}, \alpha, \ldots, \alpha\beta^{g-1}) = \operatorname{Disc}_{F/\mathbb{Q}}(\beta)^2 \operatorname{Norm}_{F/\mathbb{Q}} \operatorname{Disc}_{K/F}(\alpha).$$

But $\{1, \alpha\}$ is a $\mathcal{O}_F$-basis for $\mathcal{O}_K$ and $\{1, \beta, \ldots, \beta^{g-1}\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_F$, so this reduces to $\operatorname{Disc}_K = \operatorname{Disc}_F^2 \operatorname{Norm}_{F/\mathbb{Q}} \operatorname{Disc}_{K/F}(\alpha)$. The result follows because

$$\operatorname{Disc}_{K/F}(\alpha) = \det \begin{pmatrix} \operatorname{Trace}_{K/F}(1) & \operatorname{Trace}_{K/F}(\alpha) \\ \operatorname{Trace}_{K/F}(\alpha) & \operatorname{Trace}_{K/F}(\alpha^2) \end{pmatrix} = (\alpha - \overline{\alpha})^2 = (\eta + a)^2 - 4q.$$

□

The expression in Lemma 4 can be viewed as the equation of a plane curve by replacing a and $4q$ with formal variables. Lemma 5 below together with the substitutions

$$\operatorname{Norm}_{F/\mathbb{Q}}\left((\eta + a)^2 - 4q\right) = \prod_{\sigma : F \to \mathbb{C}} \left((a + \sigma(\eta))^2 - 4q\right)$$

and $t = -\operatorname{Disc}_K / \operatorname{Disc}_F^2$ shows that this curve is geometrically irreducible.

Lemma 5. *Let $t, a_1, \ldots, a_n \in \mathbb{C}$ and*

$$P(x,y) = \prod_{i=1}^{n} \Big((x-a_i)^2 - y \Big) + t.$$

If the a_i are distinct and $t \neq 0$, then $P(x,y)$ is irreducible.

Proof. Suppose that $P(x,y) = h(x,y)g(x,y)$ and that $h(x,y)$ is non-constant.

Let $L_i(x,y) = (x-a_i)^2 - y$ and $P_{i,j} = ((a_i+a_j)/2, ((a_i-a_j)/2)^2)$. Then $L_i(P_{i,j}) = L_j(P_{i,j}) = 0$.

Because $P(x,(x-a_i)^2) = t$, we must have that $h(x,(x-a_i)^2)$ is constant and non-zero. Let $c_i = h(x,(x-a_i)^2)$. Evaluating $h(x,y)$ at $P_{i,j}$ shows that $c_i = c_j$. Hence $c_1 = c_2 = \cdots = c_n$. Let c denote this value.

For every point Q with $L_i(Q) = 0$, we have that $h(Q) = c$. Therefore $L_i(x,y)$ divides $h(x,y) - c$. As the $L_i(x,y)$ are distinct and irreducible, we must have that their product divides $h(x,y) - c$. But $h(x,y)$ is non-constant, so $h(x,y) - c \neq 0$ and therefore $\deg h(x,y) = \deg P(x,y)$. It follows that $g(x,y)$ is constant. □

Proposition 6. *Let $K = K_1 \times \cdots \times K_n$ be a product of CM fields. For $i = 1, \ldots, n$ pick an algebraic integer $\alpha_i \in \mathcal{O}_{K_i}$ and put $\alpha = (\alpha_1, \ldots, \alpha_n)$. For each i denote by $g_i(x) \in \mathbb{Z}[x]$ the minimal polynomial of $\alpha_i + \overline{\alpha}_i$. Then $\mathbb{Z}[\alpha, \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i, \overline{\alpha}_i]$ if and only if $|\operatorname{Res}(g_i, g_j)| = 1$ for all $i \neq j$.*

Proof. First we will show that $\mathbb{Z}[\alpha, \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i, \overline{\alpha}_i]$ if and only if $\mathbb{Z}[\alpha + \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i + \overline{\alpha}_i]$. Let e_i be the i-th orthogonal idempotent of $K = \prod K_i$. Observe that $\mathbb{Z}[\alpha + \overline{\alpha}]$ is the subset of $\mathbb{Z}[\alpha, \overline{\alpha}]$ that is fixed by complex conjugation. Moreover, for every $i = 1, \ldots, n$, we have $e_i = \bar{e}_i$. The claim follows from the following chain of equivalences: we have $\mathbb{Z}[\alpha, \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i, \overline{\alpha}_i]$ if and only if $e_i \in \mathbb{Z}[\alpha, \overline{\alpha}]$ for all $i = 1, \ldots, n$ if and only if $e_i \in \mathbb{Z}[\alpha + \overline{\alpha}]$ for all $i = 1, \ldots, n$ if and only if $\mathbb{Z}[\alpha + \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i + \overline{\alpha}_i]$.

Next we claim that $\mathbb{Z}[\alpha + \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i + \overline{\alpha}_i]$ if and only if $|\operatorname{Res}(g_i, g_j)| = 1$ for all $i \neq j$. The map $\mathbb{Z}[x] \to \mathbb{Z}[\alpha + \overline{\alpha}]$ sending x to $\alpha + \overline{\alpha}$ is surjective. Therefore, it is equivalent to show that $\mathbb{Z}[x]/\operatorname{lcm}(g_i) \cong \prod \mathbb{Z}[x]/g_i$ if and only if $|\operatorname{Res}(g_i, g_j)| = 1$. The former holds if and only if the ideals $g_i\mathbb{Z}[x]$ are coprime. By [VS76, Lem. 11.3] (see also [Mye83, p. 420] for a slightly stronger version), this holds if and only if the pairwise resultants of the g_i are units. □

Corollary 7. *Let $K = K_1 \times \cdots \times K_n$ be a product of CM fields. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in K$, and g_i be the minimal polynomial for $\alpha_i + \overline{\alpha}_i$. Then α is a Weil generator for K if and only if each α_i is a Weil generator for K_i, $\alpha_1\overline{\alpha}_1 = \cdots = \alpha_n\overline{\alpha}_n$, and $|\operatorname{Res}(g_i, g_j)| = 1$ for all $i \neq j$.*

Proof. Suppose that α is a Weil generator for K Then $\alpha_1\overline{\alpha}_1 = \cdots = \alpha_n\overline{\alpha}_n \in \mathbb{Z}$. Moreoever, $\mathcal{O}_K = \mathbb{Z}[\alpha, \overline{\alpha}]$. Because $\mathcal{O}_K = \prod \mathcal{O}_{K_i}$, it follows that $\mathcal{O}_{K_i} = \mathbb{Z}[\alpha_i, \overline{\alpha}_i]$ for all i. So the resultant condition in the statement follows from Proposition 6.

Suppose that the latter conditions hold. By Proposition 6, we have $\mathbb{Z}[\alpha, \overline{\alpha}] = \prod \mathbb{Z}[\alpha_i, \overline{\alpha}_i] = \prod \mathcal{O}_{K_i} = \mathcal{O}_K$. Since $\alpha_i \overline{\alpha}_i$ is the same for each i, we also have that $\alpha\overline{\alpha}$ lies in the diagonal $\mathbb{Z} \to K$. Therefore α is a Weil generator for K. $\square$

Example 8. In Corollary 7, both the condition that $|\operatorname{Res}(g_i, g_j)| = 1$ for all $i \neq j$, and the condition that $\alpha_1\overline{\alpha}_1 = \cdots = \alpha_n\overline{\alpha}_n$ are necessary. To see this, let $K_1 = \mathbb{Q}(\sqrt{-11})$ and $K_2 = \mathbb{Q}(\sqrt{-19})$. Then $\alpha_1 = (3 - \sqrt{-11})/2$ and $\alpha_2 = (1 - \sqrt{-19})/2$ are Weil generators with norm 5 for K_1 and K_2 respectively. However, $|\operatorname{Res}(g_1, g_2)| = |\operatorname{Res}(x - 3, x - 1)| = 2$. If we instead set $K_2 = \mathbb{Q}(\sqrt{-13})$ and $\alpha_2 = 2 - i\sqrt{13}$ then $|\operatorname{Res}(g_1, g_2)| = |\operatorname{Res}(x - 3, x - 4)| = 1$ but $\operatorname{Norm}(\alpha_2) = 17$.

Lemma 9. *Let K_1 and K_2 be CM fields. Then there are finitely many Weil generators in $K_1 \times K_2$.*

Proof. For $i = 1, 2$, choose γ_i and T_i for K_i as in the beginning of Section 2. If for some i, γ_i does not exist or $T_i = \emptyset$, then K_i does not have any Weil generators and we are done. So we will assume that γ_1, γ_2 exist and both T_1 and T_2 are nonempty. Now we may write any Weil generator α_i in K_i as in Equation (1), that is, there is a unique triple $(u_i, \eta_i, a_i) \in \mathcal{O}_{F_i}^\times \times T_i \times \mathbb{Z}$ such that

$$\alpha_i = \frac{u_i(\gamma_i - \overline{\gamma}_i) + \eta_i + a_i}{2}.$$

For each pair $(\eta_1, \eta_2) \in T_1 \times T_2$, let X_{η_1,η_2} denote the affine variety cut out by the following equations in $\mathbb{Q}[x_1, x_2, y]$:

$$\prod_{\sigma: F_1 \to \mathbb{C}} \left((\sigma(\eta_1) + x_1)^2 - 4y\right) = \frac{\operatorname{Disc}_{K_1}}{\operatorname{Disc}_{F_1}^2} \tag{2}$$

$$\prod_{\tau: F_2 \to \mathbb{C}} \left((\tau(\eta_2) + x_2)^2 - 4y\right) = \frac{\operatorname{Disc}_{K_2}}{\operatorname{Disc}_{F_2}^2} \tag{3}$$

$$\prod_{\substack{\sigma: F_1 \to \mathbb{C} \\ \tau: F_2 \to \mathbb{C}}} \left((\sigma(\eta_1) + x_1) - (\tau(\eta_2) + x_2)\right)^2 = 1. \tag{4}$$

By [Győ76] the sets T_i are finite, so there is a finite number of the X_{η_1,η_2}. Let $\mathcal{X}$ denote their union.

We will now construct a finite-to-one map ψ from Weil generators of $K_1 \times K_2$ to $\mathcal{X}(\mathbb{Z})$. Let (α_1, α_2) be a Weil generator in $K_1 \times K_2$. Then α_i corresponds to a unique triple $(u_i, \eta_i, a_i) \in \mathcal{O}_{F_i}^\times \times T_i \times \mathbb{Z}$. Let $q = \alpha_1\overline{\alpha}_1 = \alpha_2\overline{\alpha}_2$. Define ψ by sending $(\alpha_1, \alpha_2) \mapsto (a_1, a_2, q)$. The image of ψ satisfies Equations (2) and (3) by Lemma 4, and Equation (4) by Corollary 7. Next we will show that ψ is finite-to-one. It suffices to show that for a given a_i and q in $\mathbb{Z}$, there are finitely many $u_i \in \mathcal{O}_{F_i}^\times$ and $\eta_i \in T_i$ such that $\alpha_i = (u_i(\gamma_i - \overline{\gamma}_i) + \eta_i + a_i)/2$ is a Weil generator for K_i with $\alpha_i\overline{\alpha}_i = q$. Every such Weil generator satisfies $4\alpha_i\overline{\alpha}_i = 4q = u_i^2 \operatorname{Norm}_{K_i/F_i}(\gamma_i - \overline{\gamma}_i) + (\eta_i + a_i)^2$. In particular, u_i is determined up to sign by a_i, q, and η_i. Since T_i is finite, there are only finitely many possible η_i. Hence there are only finitely many possible u_i as well.

It suffices to show that each component X_{η_1,η_2} has dimension 0, as this implies that $\mathcal{X}(\mathbb{Z})$ is finite. Let $(\eta_1, \eta_2) \in T_1 \times T_2$, and let $X = X_{\eta_1,\eta_2}$. Notice that Equation (4) is a polynomial equation in $x_1 - x_2$. Therefore there are complex numbers β_k for $k = 1, \ldots, \tilde{k}$, with $\tilde{k} = 2[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]$, such that

$$\left(\prod_{\substack{\sigma:F_1\to\mathbb{C} \\ \tau:F_2\to\mathbb{C}}} (x_1 - x_2 + \sigma(\eta_1) - \tau(\eta_2))^2 \right) - 1 = \prod_{k=1}^{\tilde{k}} (x_1 - x_2 - \beta_k). \tag{5}$$

Hence we can write X as a union of subvarieties X_k, for $k = 1, \ldots, \tilde{k}$, where X_k is the intersection of the geometrically irreducible surfaces (see Lemma 5) defined by Equations (2) and (3) and by

$$x_1 - x_2 - \beta_k = 0.$$

In particular we can eliminate x_2 and describe X_k as the intersection of the two irreducible plane curves

$$\prod_{\sigma:F_1\to\mathbb{C}} \left((\sigma(\eta_1) + x_1)^2 - 4y\right) - \frac{\mathrm{Disc}_{K_1}}{\mathrm{Disc}_{F_1}^2} = 0, \tag{6}$$

$$\prod_{\tau:F_2\to\mathbb{C}} \left((\tau(\eta_2) + x_1 - \beta_k)^2 - 4y\right) - \frac{\mathrm{Disc}_{K_2}}{\mathrm{Disc}_{F_2}^2} = 0. \tag{7}$$

By Bézout's theorem, the intersection of two geometrically irreducible plane curves has dimension 0 as long as the curves are distinct. So it is sufficient to show that the polynomials in Equations (6) and (7) are not proportional. We will prove this by contradiction.

Suppose that the two polynomials in Equations (6) and (7) are proportional. By comparing the highest degree monomial in y we must have that Equations (6) and (7) are equal. Note that this also implies $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$. Setting $y = 0$ leads to

$$\prod_{\sigma:F_1\to\mathbb{C}} (\sigma(\eta_1) + x_1)^2 = \prod_{\tau:F_2\to\mathbb{C}} (\tau(\eta_2) + x_1 - \beta_k)^2.$$

By comparing the zeros we see that, for each k, there is a bijection $\sigma \mapsto \tau_{\sigma,k}$ such that $\sigma(\eta_1) = \tau_{\sigma,k}(\eta_2) - \beta_k$. Fix a $1 \le k_0 \le \tilde{k}$ substituting $\sigma(\eta_1) = \tau_{\sigma,k_0}(\eta_2) - \beta_{k_0}$ and $x_2 = x_1 - \beta_{k_0}$ in Equation (5) yields

$$\prod_{k=1}^{\tilde{k}} (x_1 - (x_1 - \beta_{k_0}) - \beta_k) = \left(\prod_{\sigma,\tau} x_1 - (x_1 - \beta_{k_0}) + \tau_{\sigma,k_0}(\eta_2) - \beta_{k_0} - \tau(\eta_2) \right)^2 - 1$$

$$0 = \left(\prod_{\sigma,\tau} (\tau_{\sigma,k}(\eta_2) - \tau(\eta_2))^2 \right) - 1$$

Since the product is taken over all embeddings σ (and τ) we have that the right hand side is equal to -1, which is a contradiction. □

Theorem 10. *Let $K = K_1 \times \cdots \times K_n$ be a product of CM fields. If $n > 1$ then K has finitely many Weil generators.*

Proof. This follows directly from Lemma 9 and the fact that every Weil generator for K projects to a Weil generator for each product $K_i \times K_j$, with $i \neq j$. □

3 Products of super-isolated varieties

In this section, we study products of super-isolated abelian varieties. Recall that the *Weil polynomial* h of a d-dimensional abelian variety $A/\mathbb{F}_q$ is defined as the characteristic polynomial of the Frobenius endomorphism of A. The polynomial h lies in $\mathbb{Z}[x]$, it has degree $2d$ and all its complex roots have absolute value $\sqrt{q}$. Also we define the *real Weil polynomial* of A the unique polynomial g in $\mathbb{Z}[x]$ such that $h(x) = x^d g(x + q/x)$. In particular if h is irreducible and π is a root of h, then g is the minimal polynomial of $\pi + q/\pi$.

3.1 Glueing exponent and super isolated abelian varieties

Lemma 11. *Let A_1 and A_2 be abelian varieties over a finite field $\mathbb{F}_q$. Assume that A_1 and A_2 have no isogeny factor in common. If the product $A_1 \times A_2$ is super-isolated, then both A_1 and A_2 are super-isolated.*

Proof. Let B_1 and B_2 be abelian varieties isogenous to A_1 and A_2, respectively. Since $A_1 \times A_2$ is super-isolated then there exists an isomorphism $\varphi : A_1 \times A_2 \to B_1 \times B_2$. Observe that

$$\mathrm{Hom}_{\mathbb{F}_q}(A_1 \times A_2, B_1 \times B_2) = \mathrm{Hom}_{\mathbb{F}_q}(A_1, B_1) \times \mathrm{Hom}_{\mathbb{F}_q}(A_2, B_2),$$

because A_1 and A_2 have no isogeny factor in common. Hence there are isomorphisms $\varphi_1 : A_1 \to B_1$ and $\varphi_2 : A_2 \to B_2$ such that $\varphi = \varphi_1 \times \varphi_2$. In particular A_1 and A_2 are super-isolated. □

Definition 12 (cf. [HL12, Def. 2.1])**.** Let A_1 and A_2 be abelian varieties over $\mathbb{F}_q$. The *glueing exponent* $e(A_1, A_2)$ of A_1 and A_2 is the greatest common divisor of the exponent of Δ, where Δ ranges over all finite group schemes that embed in both A_1 and A_2.

Lemma 13. *Let A_1 and A_2 be abelian varieties over a finite field $\mathbb{F}_q$ with no isogeny factor in common. If A_1 and A_2 are super-isolated and $e(A_1, A_2) = 1$ then the product $A_1 \times A_2$ is super-isolated.*

Proof. It is a direct application of [HL12, Lemma 2.3]. □

Lemmas 11 and 13 allow us to understand super-isolated products (of abelian varieties with no isogeny factors in common) in terms of the glueing exponent. In general the glueing exponent is tricky to compute. Nevertheless one can use [HL12, Prop.2.8] to show that for abelian varieties A and B over $\mathbb{F}_q$ with no isogeny factor in common the glueing exponent divides the resultant of the

radicals of the real Weil polynomials g_A and g_B of A and B. In particular if such a resultant is 1 then also $e(A,B) = 1$. In particular Corollary 7 can be considered as a reformulation in terms of Weil generators (restricted to ideal abelian varieties) of Lemma 13.

In what follows we will use a different strategy: We will restrict ourselves to a subcategory of abelian varieties and give conditions for them (and their products) to be super-isolated in terms of Weil generators. The upshot of this approach is that it is more computationally friendly, since Weil generators can be enumerated. Moreover, in such a subcategory, we will be able to study powers of super-isolated abelian varieties.

3.2 Weil generators and super isolated abelian varieties

From now on we will focus on squarefree varieties. That is, abelian varieties whose Weil polynomial is squarefree. Our main tool is the equivalence of categories between certain abelian varieties $A/\mathbb{F}_q$ and $\mathbb{Z}$-modules with extra structure.

Definition 14. Let $A/\mathbb{F}_q$ be an abelian variety, and let h denote its Weil polynomial. Let p be the characteristic of $\mathbb{F}_q$. Then A is *ideal* if the following holds:

1. the polynomial h factors into distinct irreducible factors.
2. the polynomial h has no real roots.
3. the polynomial h is ordinary (meaning half of the roots of h are p-adic units) or q is prime.

Suppose that $A/\mathbb{F}_q$ is ideal. Then there is an isogeny

$$A \sim A_1 \times \ldots \times A_n,$$

where the A_i are simple and pairwise non-isogenous abelian varieties. By Honda-Tate theory the Weil polynomial factors into $h = h_1 \cdots h_n$, where h_i is the Weil polynomial of A_i. Because of the ordinary condition (or the condition that q is prime), the polynomials h_i are irreducible. In particular, if we let π_i denote a root of h_i and put $K_i = \mathbb{Q}(\pi_i)$, then K_i is a CM field of degree $2 \dim A_i$. Let $K = \prod K_i$ and consider the subring $\mathbb{Z}[\pi, \overline{\pi}] \subseteq K$ where $\pi = (\pi_1, \ldots, \pi_n)$ and $\overline{\pi} = (\overline{\pi}_1, \ldots, \overline{\pi}_n)$ with $\overline{\pi}_i = q/\pi_i$. We will identify K with $\operatorname{End} A \otimes \mathbb{Q}$. Let $\mathcal{O}_K = \prod \mathcal{O}_{K_i}$, that is, the integral closure of $\mathbb{Z}$ in K. Note that $\mathcal{O}_K$ and $\mathbb{Z}[\pi, \overline{\pi}]$ are free finitely generated $\mathbb{Z}$-modules of rank $\dim_{\mathbb{Q}}(K)$. In particular we have a finite-index inclusion $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$ and one can show that $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \operatorname{End} A \subseteq \mathcal{O}_K$.

By [Mar18b, Thm. 4.3] the *ideal* abelian varieties can be functorially described in terms of fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals. Such a description builds on the equivalences of categories established in [Del69] and [CS15].

Theorem 15. *If $A/\mathbb{F}_q$ is ideal and simple, then A is super-isolated if and only if K has class number 1 and $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$. Equivalently, A is super-isolated if and only if K has class number 1 and π is a Weil generator for K.*

Proof. The result for ordinary varieties is given in [Sch19, Thm. 7.4]. The extension to the case where q is prime follows from [WM71, Thm. 6.1]. □

Theorem 16. *If $A/\mathbb{F}_q$ is ideal, then A is super-isolated if and only if each A_i is super-isolated and $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$. Equivalently, A is super-isolated if and only if $\mathrm{Pic}(\mathcal{O}_K)$ is trivial and π is a Weil generator for K.*

Proof. By [Mar18b, Thm. 4.3] we have that A is super-isolated if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ and $\mathrm{Pic}(\mathcal{O}_K)$ is trivial. Moreover by Theorem 15 we have that each simple factor A_i is super-isolated if and only if $\mathbb{Z}[\pi_i, \overline{\pi}_i] = \mathcal{O}_{K_i}$ and $\mathrm{Pic}(\mathcal{O}_{K_i})$ is trivial. The result follows from the equality $\mathrm{Pic}(\mathcal{O}_K) = \prod \mathrm{Pic}(\mathcal{O}_{K_i})$. □

By using Theorem 16 it is easy to construct super-isolated products of big dimension as shown in the following example.

Example 17. Consider the polynomials

$$
\begin{aligned}
h_1(x) &= (x^4 - 2x^3 + 3x^2 - 4x + 4),\\
h_2(x) &= (x^6 - 4x^5 + 9x^4 - 15x^3 + 18x^2 - 16x + 8),\\
h_3(x) &= (x^6 - 3x^5 + 6x^4 - 9x^3 + 12x^2 - 12x + 8),\\
h_4(x) &= (x^8 - 5x^7 + 12x^6 - 20x^5 + 29x^4 - 40x^3 + 48x^2 - 40x + 16),\\
h_5(x) &= (x^8 - 5x^7 + 13x^6 - 25x^5 + 39x^4 - 50x^3 + 52x^2 - 40x + 16),\\
h_6(x) &= (x^8 - 4x^7 + 5x^6 + 2x^5 - 11x^4 + 4x^3 + 20x^2 - 32x + 16).
\end{aligned}
$$

One can check that each factor h_i determines a Weil generator α_i for a CM field $K_i = \mathbb{Q}[x]/h_i$, and that $(\alpha_1, \ldots, \alpha_6)$ is a Weil generator for the product $K_1 \times \cdots \times K_6$. Therefore $h = \prod_i h_i$ is the Weil polynomial for a 20-dimensional super-isolated variety over $\mathbb{F}_2$.

Example 18. Let $A/\mathbb{F}_5$ be the product of the elliptic curves $E_1 : y^2 = x^3+4x+2$ and $E_2 : y^2 = x^3+3x+2$. The Weil polynomials of E_1 and E_2 are $h_1 = x^2-3x+5$ and $h_2 = x^2 - x + 5$, respectively. Using Corollary 7 and Theorem 16, it is straightforward to check that E_1 and E_2 are super-isolated, but A is not, see also Example 8. Therefore A must be isogeneous, but not isomorphic, to some other abelian surface over $\mathbb{F}_5$. One way to verify this claim is to observe that $\mathbb{Z}[\pi, \bar{\pi}] \subsetneq \mathcal{O}_K = \mathbb{Z}[\pi_1] \times \mathbb{Z}[\pi_2] = \mathrm{End}_{\mathbb{F}_5}(A)$. By [WM71, Thm 6.1] we have that there exists an abelian variety A' isogenous to A with $\mathrm{End}_{\mathbb{F}_5}(A') = \mathbb{Z}[\pi, \bar{\pi}]$. In particular A is not isomorphic to A'. More precisely, since $\mathcal{O}_K$ is the unique over-order of $\mathbb{Z}[\pi, \bar{\pi}]$ and $\mathrm{Pic}(\mathbb{Z}[\pi, \bar{\pi}]) \simeq \mathbb{Z}/3\mathbb{Z}$, by using [Mar18b, Thm. 4.3] we can conclude that the isogeny class of A contains exactly 4 isomorphism classes of abelian varieties, 3 of which have endomorphism ring $\mathbb{Z}[\pi, \bar{\pi}]$.

Corollary 19. *Let g be a positive integer. There are only finitely many ideal super-isolated abelian varieties of dimension g that are not simple. In particular, there are only finitely many finite fields $\mathbb{F}_q$ for which such a variety may exist.*

Proof. By Theorem 16 it is sufficient to count Weil generators in products of CM fields with class number 1. In [Sta74, Thm. 2, p. 136], Stark showed that for any fixed degree, there are finitely many CM fields with class number 1 with that degree. Hence there are finitely many products $K_1 \times \cdots \times K_n$ with $\sum \deg K_i = 2g$ such that each K_i is a CM field with class number 1. By Theorem 10, any such product of fields contains only finitely many Weil generators. □

3.3 Products of super-isolated elliptic curves and abelian surfaces

In this section we outline a general strategy to enumerate certain products of super-isolated varieties.

Algorithm 1 Enumerate Weil Generators

Require: A product K of CM fields K_1 and K_2, with maximal totally real subfields F_1 and F_2, respectively.
Ensure: All Weil generators for K.

$F \leftarrow F_1 \times F2$
Find γ_i such that $\mathcal{O}_K = \mathcal{O}_F[\gamma_i]$
$T_i \leftarrow$ a complete set of $\eta_i \in F_i$ such that $\mathcal{O}_{F_i} = \mathbb{Z}[\eta_i]$ up to integer translation
for all $(\eta_1, \eta_2) \in T_1 \times T_2$ **do**
  $X_{\eta_1,\eta_2} \leftarrow$ the variety defined in the proof of Lemma 9
  for all $P \in X_{\eta_1,\eta_2}(\mathbb{Q})$ **do**
    for all $u_i \in \mathcal{O}_{F_i}^{\times}$ with $u_i^2 \operatorname{Norm}_{K/F}(\gamma_i - \overline{\gamma}_i) + (\eta_i + P_{x_i})^2 = 4P_y$ **do**
      $\alpha_i \leftarrow (u_i(\gamma_i - \overline{\gamma}_i) + \eta_i + P_{x_i})/2$
      if $\alpha_1 \in \mathcal{O}_{K_1}$ and $\alpha_2 \in \mathcal{O}_{K_2}$ **then**
        print (α_1, α_2)
      end if
    end for
  end for
end for

Proposition 20. *Let K be a product of CM fields K_1 and K_2, with maximal totally real subfields F_1 and F_2, respectively. Algorithm 1 exactly outputs all Weil generators for $K_1 \times K_2$.*

Proof. As seen in the proof of Lemma 9, every Weil generator (α_1, α_2) of K corresponds to a rational point on one of the varieties X_{η_1,η_2} for some $\eta_1, \eta_2 \in T_1 \times T_2$. The algorithm ranges over all rational points on all such varieties and finds all possible pairs (α_1, α_2) which could be Weil generators. This means that the output will include all Weil generators.

It remains to show that everything the algorithm outputs is a Weil generator for $K_1 \times K_2$. Suppose that the algorithm outputs (α_1, α_2) from a point on X_{η_1,η_2} for some $(\eta_1, \eta_2) \in T_1 \times T_2$. It is straightforward to check that if $\alpha_i \in \mathcal{O}_{K_i}$ then it is indeed a Weil generator for K_i using [Sch19, Lem. 3.13]. By construction of X_{η_1,η_2}, it follows that (α_1, α_2) satisfies the resultant condition in Corollary 7. Therefore (α_1, α_2) is a Weil generator for $K_1 \times K_2$. □

Remark 21. Algorithm 1 can be extended to arbitrary products $K_1 \times \cdots \times K_n$ in a straightforward way: First compute the set $W_{i,j}$ of all Weil generators in the sub-product $K_i \times K_j$ for all $1 \leq i, j \leq n$. Then search for tuples $(\alpha_1, \ldots, \alpha_n)$ with $(\alpha_i, \alpha_j) \in W_{i,j}$ for all $1 \leq i, j \leq n$.

Using Tables of CM fields of degree 2 and 4 with class number one, we can enumerate all ideal superisolated abelian varieties that factor into products of elliptic curves and surfaces.

Corollary 22. *There are* 240 *ideal super-isolated abelian varieties that factor into a product of curves and surfaces. A summary of some of their characteristics are given in Table 1.* [1]

Proof. We implemented Algorithm 1 in `Sage` and found all ideal super-isolated abelian varieties that decompose into a product of curves and surfaces. This was done by first finding a complete list of CM fields with class number 1 and degree ≤ 4 (see [Sch19, Tbl. 3] for references). For each pair K_i, K_j of such fields, we computed the set of Weil generators $W_{i,j}$ in $K_i \times K_j$. We filtered the Weil generators whose minimal polynomials satisfy the conditions in Definition 14, as these correspond to simple ideal varieties. Next we organized the data into a graph $\mathcal{G}$ as follows. The vertex set of $\mathcal{G}$ is given by all Weil generators appearing as part of a pair in some $W_{i,j}$. We add an edge between α_1 and α_2 if $(\alpha_1, \alpha_2) \in W_{i,j}$ for some i, j. That is, the edge set of $\mathcal{G}$ is the union of the $W_{i,j}$. Finally, we used standard methods to enumerate all complete subgraphs (cliques) of size ≥ 2 in $\mathcal{G}$. □

Remark 23. Observe that by [Sch19, Cor. 7.6], for every fixed dimension $g > 2$ we have only finitely many (ordinary) super-isolated abelian varieties. This was shown by mapping Weil generators to integral points on degree g plane curves. Given a way to enumerate the integral points on such a curve, it is straightforward to enumerate super-isolated abelian varieties of dimension g. However, computing integral points on high degree curves (which often have high genus) is a difficult problem. If instead we restrict to enumerating non-trivial products of super-isolated g-folds, then Algorithm 1 only requires enumerating points on a dimension 0 variety (of degree $\approx g^3$). This seems to suggest that finding products of super-isolated varieties is easier than finding singletons.

[1] The raw data collected and source code can be found at `https://github.com/tscholl2/siav-polarizations-products`.

q	1×1	1×2	$1\times 1\times 2$	$1\times 2\times 2$	2×2
2	4	24	10	12	18
3	4	24	6	12	18
4		2			
5	2	12		2	6
7		8			
8		2			
9		2			
11	2	8	2	4	4
13		6			
17	2	8	2		
19					2
32		2			
41		2			
47		4			
59		2			
61		2			
83	2				
101	2				
173		2			
227	2				
257	2				
283		2			
383		2			
1523	2				
1601	2				
18131		2			

Table 1: The number of ideal super-isolated products of elliptic curves and abelian surfaces over each finite field $\mathbb{F}_q$. Each column represents a decomposition type, so for example 1×1 represents the product of two non-isogenous elliptic curves. If the cell is empty, it means there is no super-isolated abelian variety over $\mathbb{F}_q$ with the prescribed decomposition type.

3.4 Powers of super-isolated abelian varieties

In the case where A is isogenous to a power, we can apply the results from [Mar19] to prove the following Theorem.

Theorem 24. *Let $A/\mathbb{F}_q$ be an ideal abelian variety. If A is super-isolated, then A^n is super-isolated for every $n\geq 1$. Conversely, if there exists $n\geq 1$ such that A^n is super-isolated then A is super-isolated.*

Proof. By Theorem 15 we have that A is super-isolated if and only if K has class number 1 and $\mathbb{Z}[\pi,\overline{\pi}]=\mathcal{O}_K$. By Steinitz theory, this is equivalent to having

a unique isomorphism class of torsion-free $\mathbb{Z}[\pi, \overline{\pi}]$-modules of rank n (for any $n \geq 1$), which is represented by

$$\mathcal{O}_K^n = \mathcal{O}_K \oplus \ldots \oplus \mathcal{O}_K.$$

Using the classification given in [Mar19, Theorem 4.1], one sees that this happens if and only if A^n is super-isolated. □

4 Principal polarizations

In general, (principal) polarizations of abelian varieties in an ordinary square-free isogeny class can be computed up to polarized isomorphisms using [Mar18b, Alg. 3]. However, in this section we show that if the isogeny class is super-isolated, then the situation is much simpler. For a CM type Φ of a CM field K we denote by N_Φ the associated norm, that is,

$$N_\Phi(\alpha) = \prod_{\varphi \in \Phi} \varphi(\alpha),$$

for every $\alpha \in K$.

4.1 Existence of principal polarizations

Lemma 25. *Let K be a CM field of degree $2g$ with maximal totally real subfield F. Let Φ be a CM type of K, and $\alpha \in K$ satisfying $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. Then the following statements are equivalent:*

1. *K/F is unramified at all finite primes.*
2. *$\alpha - \overline{\alpha} \in \mathcal{O}_K^\times$.*
3. *$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - \overline{\alpha}) = 1$.*
4. *$N_\Phi(\alpha - \overline{\alpha}) = \pm 1$.*

Moreover, if any of the statements holds then g is even.

Proof. Observe that we have

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - \overline{\alpha}) = N_\Phi(\alpha - \overline{\alpha}) N_\Phi(\overline{\alpha} - \alpha) = (-1)^g N_\Phi(\alpha - \overline{\alpha})^2. \tag{8}$$

By [Neu99, Ch. III, Prop. 2.4], $(\alpha - \overline{\alpha})\mathcal{O}_K$ is the relative different ideal $\mathrm{Diff}_{K/F}$. So K/F is unramified at all finite primes if and only if $\alpha - \overline{\alpha} \in \mathcal{O}_K^\times$. As all norms in CM fields are non-negative, this is equivalent to $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - \overline{\alpha}) = 1$. Hence we have proved that (1), (2) and (3) are equivalent. Using Equation (8) we get that (3) is also equivalent to

$$1 = (-1)^g N_\Phi(\alpha - \overline{\alpha})^2.$$

If K/F is unramified at all finite primes, then g is even by [How95, Lem. 10.2] and we get that $N_\Phi(\alpha - \overline{\alpha}) = \pm 1$. Conversely if $N_\Phi(\alpha - \overline{\alpha}) = \pm 1$ then by Equation (8) we get $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - \overline{\alpha}) = (-1)^g$. Since norms are positive in CM-fields, we deduce that g is even and K/F is unramified. This concludes the proof. □

Let $A/\mathbb{F}_q$ be a simple ordinary super-isolated abelian variety of dimension g. Let h be the Weil polynomial of A. Put $K = \mathbb{Q}[x]/h = \mathbb{Q}(\pi)$. Fix an isomorphism $j : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$ and let Φ be the set of embeddings $\phi : K \to \mathbb{C}$ such that $\nu(\phi(\pi)) > 0$, where ν is the p-adic valuation on $\mathbb{C}$ induced by j. Since A is ordinary, precisely half of the roots of h are p-adic units. Therefore Φ is a CM-type of K.

Lemma 26. *The abelian variety A does not admit a principal polarization if and only if $N_\Phi(\pi - \overline{\pi}) = -1$.*

Proof. Suppose A does not admit a principal polarization. Then by [How95, Cor. 11.4] we have that K/F is unramified at all finite primes and $N_\Phi(\pi - \overline{\pi}) < 0$. Because π is a Weil generator for K, it follows that $\mathcal{O}_K = \mathcal{O}_F[\pi]$ by [Sch20, Lem. 3.13]. So by Lemma 25, we have $N_\Phi(\pi - \overline{\pi}) = -1$.

Conversely, suppose that $N_\Phi(\pi - \overline{\pi}) = -1$. By Lemma 25 it follows that K/F is unramified at all finite primes, and that $(\pi - \bar{\pi}) \in \mathcal{O}_K^\times$. In particular there is no prime of F dividing $(\pi - \bar{\pi})$ which is inert in K/F. It now follows from [How95, Cor. 11.4] that A does not admit a principal polarization. □

Theorem 27. *The abelian variety A does not admit a principal polarization if and only if $\mathrm{Norm}_{K/\mathbb{Q}}(\pi - \overline{\pi}) = 1$ and the middle coefficient a_g of the Weil polynomial is $-1 \bmod q$ if $q > 2$ and $-1 \bmod 4$ if $q = 2$.*

Proof. By Lemmas 25 and 26, it is enough to show that if $K/\mathbb{Q}$ is unramified at all finite primes, then $N_\Phi(\pi - \overline{\pi}) = -1$ if and only if a_g satisfies the congruence condition in the statement. By [How95, Prop. 11.5], if K/F is unramified at all finite primes then $N_\Phi(\pi - \overline{\pi}) \equiv a_g \bmod q$ if $q > 2$ and $N_\Phi(\pi - \overline{\pi}) \equiv a_g \bmod 4$ if $q = 2$. As these moduli are enough to distinguish ± 1, the result follows. □

Example 28. Let π denote a root of $h(x) = x^8 + x^7 - 3x^6 - x^5 + 7x^4 - 2x^3 - 12x^2 + 8x + 16$. Then π is a Weil generator for the CM field $K = \mathbb{Q}(\pi)$ of degree 8. So π corresponds to a super-isolated abelian fourfold A over $\mathbb{F}_2$. One can check that $\mathrm{Norm}_{K/\mathbb{Q}}(\pi - \overline{\pi}) = 1$. Also, the middle coefficient of $h(x)$ is $7 \equiv -1 \bmod 4$, so A does not admit a principal polarization.

Example 29. We will show that the two conditions in Theorem 27 are independent. Let α_1 denote a root of $h_1 = x^2 - x + 3$ and α_2 a root of $h_2 = x^4 - 5x^2 + 9$. Then α_1 and α_2 are Weil generators for the CM fields $K_i = \mathbb{Q}(\alpha_i)$. Let $q_i = \alpha_i \overline{\alpha}_i$. One can compute that $\mathrm{Norm}_{K_1/\mathbb{Q}}(\alpha_1) = 11$ and $\mathrm{Norm}_{K_2/\mathbb{Q}}(\alpha_2) = 1$. The middle coefficients of h_1 and h_2 are $-1 \bmod q_1$ and $1 \bmod q_2$ respectively. Therefore α_1 satisfies the second hypothesis but not the first of Theorem 27, while α_2 satisfies the first but not the second.

Remark 30. One can show that any abelian variety admits a principal polarization if and only if its quadratic twist does. But for super-isolated varieties, this follows almost immediately from Theorem 27. If $h(x)$ is the Weil polynomial of $A/\mathbb{F}_q$, then $h(-x)$ is the Weil polynomial for its twist. Then because $\mathrm{Norm}_{K/\mathbb{Q}}(\pi-\overline{\pi}) = \mathrm{Norm}_{K/\mathbb{Q}}((-\pi)-(-\overline{\pi}))$ and $h(x)$ and $h(-x)$ share the same middle coefficient, the criterion in Theorem 27 holds for one if and only if it holds for the other.

Given any super-isolated abelian variety A, we can always construct one with a principal polarization using Zarhin's trick and Theorem 24.

Proposition 31. *Let A be a super-isolated abelian variety. Then A^8 is principally polarized.*

Proof. Since A is super-isolated it is isomorphic to its dual $A^\vee$. Hence there is an isomorphism $\varphi : A^8 \to (A \times A^\vee)^4$. By Zahrin's trick (see [Zar74]), the product $(A \times A^\vee)^4$ admits a principal polarization μ. Then $\varphi^*\mu = \phi^\vee \circ \mu \circ \phi$ is a principal polarization of A^8, see for example [Mum08, p.143]. □

4.2 Uniqueness of principal polarizations

In this section, we prove that if a super-isolated abelian variety admits a principal polarization, then such a polarization is unique up to polarized isomorphism.

First, we set the following notation. For a number field L, we let U_L denote the group of units of $\mathcal{O}_L$, and the group of totally positive units is U_L^+. The Hilbert class field of L is denoted by H_L, and the narrow Hilbert class field is H_L^+. Recall that H_L is the maximal unramified abelian extension of L and that H_L^+ is the maximal abelian extension of L unramified outside of the infinite primes[2] (see [Cox13, Ch. 5.C, Thm. 5.18] and [Mar18a, Ch. 8, p. 167]). Moreover, the Galois group $\mathrm{Gal}(H_L/L)$ is isomorphic to the class group of L, see [Cox13, Ch. 5.C, Thm. 5.23].

Lemma 32. *If F is a totally real field, then*

$$[U_F^+ : U_F^2] = [H_F^+ : H_F].$$

Proof. If r is the number of real embeddings of F, then $2^r = [U_F : U_F^+][H_F^+ : H_F]$ by [Jan96, Thm. 3.1, p. 242]. Since F is totally real, $2^r = [U_F : U_F^2]$ as $U_F \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{r-1}$. □

Lemma 33. *Let K be a CM field with class number 1, and let F be the maximal totally real subfield of K. Then $\mathrm{Norm}_{K/F}(U_K) = U_F^+$.*

Proof. By [Mar18a, Ch. 8, Ex. 27, p. 176], $H_F^+ K \subseteq H_K^+$. Since K has no real embeddings because it is a CM field, we have $H_K^+ = H_K$ because the infinite primes of K are unramified in every extension. Moreover, the assumption that K

[2] A real archimedean prime ramifies in an extension if it extends to a non-real embedding [Cox13, Ch. 5.C, p. 94].

has class number 1 means that $H_K = K$. Therefore we have that $F \subseteq H_F^+ \subseteq K$, and either $H_F^+ = F$ or $H_F^+ = K$. By Lemma 32, U_F^2 has index 1 or 2 in U_F^+ depending on which equality holds.

If K/F is ramified at a finite prime, then $H_F^+ = F$. Hence by Lemma 32 we have $U_F^+ = U_F^2$, and the conclusion follows from the fact that

$$U_F^2 \subseteq \mathrm{Norm}_{K/F}(U_K) \subseteq U_F^+.$$

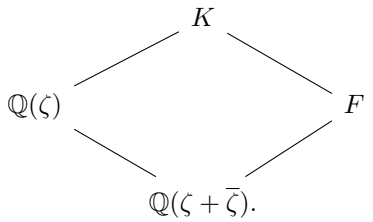
It remains to consider the case where K/F is unramified. Here we have that $H_F^+ = K$, so $[U_F^+ : U_F^2] = 2$. To prove the claim, we will show that there is a unit $u \in U_K$ such that $\mathrm{Norm}_{K/F}(u) \notin U_F^2$.

By Kummer theory, $K = F(\sqrt{-\varepsilon})$ for some totally positive element $\varepsilon \in F$. We claim that for every prime $\mathfrak{p}$ of F, the valuation $v_\mathfrak{p}(\epsilon)$ is even. To see this, let $\mathfrak{P}$ be a prime of K lying over $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in K/F, then we have $v_\mathfrak{p}(\epsilon) = v_\mathfrak{P}(\epsilon)$. The latter is even because $v_\mathfrak{P}(\epsilon) = 2v_\mathfrak{P}(\sqrt{-\epsilon})$.

By above, we can write $\varepsilon\mathcal{O}_F = \mathfrak{p}_1^{2e_1} \cdots \mathfrak{p}_k^{2e_k}$ for primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of F. Because K has class number 1, so does F, see [Was97, Thm. 4.10]. So there are generators β_i for each $\mathfrak{p}_i$, and we may write $\varepsilon = \varepsilon' \beta_1^{2e_1} \cdots \beta_k^{2e_k}$ for some $\varepsilon' \in U_F$. The extension $F(\sqrt{-\varepsilon})/F$ depends only on the residue of ε in $F^\times/(F^\times)^2$. Therefore we may assume that $\varepsilon = \varepsilon'$, i.e. that $\varepsilon \in U_F$.

Note that $\mathrm{Norm}_{K/F}(\sqrt{-\varepsilon}) = \varepsilon$. If $\varepsilon \notin U_F^2$, then we are done. Otherwise, $F(\sqrt{-\varepsilon}) = F(\sqrt{-1})$, so we may assume that $\varepsilon = 1$. In particular, it remains to consider the case where $K = F(i)$.

Let ζ be a primitive 2^nth root of unity in K such that n is maximal (by above we know that $n \geq 2$). Then we have a tower of the form



Recall that since ζ is a primitive 2^nth root of unity, the rational prime 2 is totally ramified in $\mathbb{Q}(\zeta)$. Moreover, $2\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathfrak{b}^{2^{n-1}}$ where $\mathfrak{b}$ is the prime ideal generated by $b = 1 - \zeta$ [Mar18a, Ch. 2, Ex. 34, p. 34]. In particular $\mathfrak{b} = \overline{\mathfrak{b}}$. Put $\mathfrak{a} = \mathfrak{b} \cap \mathbb{Q}(\zeta + \overline{\zeta})$, which is the unique prime ideal of $\mathbb{Q}(\zeta + \overline{\zeta})$ above 2. Let $a = b\overline{b}$. Observe that $a \in \mathbb{Q}(\zeta + \overline{\zeta})$ and that a is a generator of $\mathfrak{a}\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathfrak{b}^2$. Therefore $v_\mathfrak{b}(a) = 2v_\mathfrak{a}(a)$, and $v_\mathfrak{b}(a) = 2$ by construction. Hence a is a generator of $\mathfrak{a}$. As mentioned above, the ramification index $e(\mathfrak{b}/\mathfrak{a}) = 2$. So, since K/F is unramified, we deduce that there exists an ideal $\mathfrak{c}$ of F such that $\mathfrak{c}^2 = \mathfrak{a}\mathcal{O}_F$. Moreover since F has class number 1, the ideal $\mathfrak{c}$ admits a generator $c \in F$. Then $c^2 = au$ for some $u \in U_F$. Moreover we have that

$$c^2\mathcal{O}_K = \mathfrak{c}^2\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K = \mathfrak{b}^2\mathcal{O}_K = b^2\mathcal{O}_K.$$

Hence $c/b \in U_K$. Also, by construction,

$$\mathrm{Norm}_{K/F}\left(\frac{c}{b}\right) = \frac{au}{a} = u.$$

We conclude the proof by proving that $u \notin U_F^2$. Indeed, assume that $u = u_0^2$ for some $u_0 \in U_F$. Then

$$\left(\frac{c}{bu_0}\right)^2 = \frac{a}{b^2} = \frac{a}{b\overline{b}(-\zeta)} = (-\zeta)^{-1}.$$

This implies that cu_0/b is a primitive 2^{n+1} root of unity in K, contradicting the maximality of n. □

In the next example we show that the assumption on the class number of K is necessary for Lemma 33 to hold.

Example 34. Let $K = \mathbb{Q}[x]/(x^4 - x^3 + x^2 - 3x + 9)$, which has class number 2. Then K is a CM field with maximal totally real subfield $F = \mathbb{Q}(\sqrt{21})$. A fundamental unit of F is $\epsilon = (5-\sqrt{21})/2$, which is totally positive. One can show that $U_K = U_F$. Therefore $\epsilon \notin \mathrm{Norm}_{K/F}(U_K) = \langle \epsilon^2 \rangle$, so $U_F^+/\mathrm{Norm}_{K/F}(U_K) \cong \mathbb{Z}/2\mathbb{Z}$.

Theorem 35. *Let A be a simple super-isolated ordinary abelian variety over $\mathbb{F}_q$ which admits a principal polarization. Then the polarization is unique up to polarized isomorphism.*

Proof. We have that $\mathrm{End}(A) = \mathcal{O}_K$ for a CM-number field K with class number 1. By [Mar18b, Thm. 5.4], the number of principal polarizations is given by the size of the quotient

$$\frac{U_F^+}{\mathrm{Norm}_{K/F}(U_K)},$$

and this is trivial by Lemma 33. □

4.3 Products of principal polarizations

Let K be a CM field. Recall that for a CM type Φ of K we say that a totally imaginary element $\lambda \in K$ is Φ-positive if $\Im(\varphi(\lambda)) > 0$ for every $\varphi \in \Phi$. Also, for a fractional ideal I of some order R in K, we denote by I^t its trace dual ideal, which is defined as

$$I^t = \{z \in K : \mathrm{Trace}_{K/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\}.$$

Also, we define $\overline{I}$ as the image of I by the CM involution of K.

Corollary 36. *Let A be an ordinary squarefree super-isolated abelian variety, say $A = \prod_1^n A_i$ with A_i simple. Then A admits a principal polarization if and only if each A_i does. If this is the case, the principal polarization is unique up to polarized isomorphism.*

Proof. Let h (resp. h_i) be the Weil polynomial of A (resp. A_i). Put $K = \mathbb{Q}[x]/h$ and $K_i = \mathbb{Q}[x]/h_i$ for each i, so that $K = \prod_{i=1}^n K_i$. For each i let F_i be the maximal totally real subfield of K_i and put $F = \prod_i F_i$. Since the abelian variety A is ordinary, by [Mar18b, Thm. 5.4] we have that A is principally polarized if and only there exist a $\lambda \in K^*$ which is totally imaginary, Φ-positive, and such that

$$\lambda \mathcal{O}_K = \overline{\mathcal{O}}_K^t. \tag{9}$$

Since $\mathcal{O}_K = \oplus_i \mathcal{O}_{K_i}$ and $\overline{\mathcal{O}}_K^t = \oplus_i \overline{\mathcal{O}}_{K_i}^t$, if we write $\lambda = (\lambda_1, \ldots, \lambda_n)$ with λ_i in K_i, then λ is totally imaginary and Φ-positive if and only if the same holds for each λ_i. Also, Equation (9) holds if and only if

$$\lambda_i \mathcal{O}_{K_i} = \overline{\mathcal{O}}_{K_i}^t$$

for each i. The statement about the uniqueness follows from the equality

$$\frac{U_F^+}{\mathrm{Norm}_{K/F}(U_K)} = \prod_{i=1}^n \frac{U_{F_i}^+}{\mathrm{Norm}_{K_i/F_i}(U_{K_i})}.$$

□

Remark 37. Let A be an ordinary simple super-isolated abelian variety admitting a principal polarization. Then also A^n admits a principal polarization, but this is in general not unique, see [Mar19, Ex. 6.5, Ex. 6.6].

5 Jacobians

Proposition 38. *Let C and C' be smooth, projective and geometrically integral curves of genus $g > 1$ defined over $\mathbb{F}_q$ with the same zeta function. Assume that $\mathrm{Jac}(C)$ is ordinary, ideal, and super-isolated. Then the curves C and C' are isomorphic.*

Proof. Observe that by assumption $\mathrm{Jac}(C')$ is isogenous to $\mathrm{Jac}(C)$, and hence isomorphic since $\mathrm{Jac}(C)$ is super-isolated. Denote by θ and θ' the canonical principal polarizations of $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$, respectively. By Theorem 35 we deduce that $(\mathrm{Jac}(C), \theta)$ is isomorphic to $(\mathrm{Jac}(C'), \theta')$. Therefore by Torelli's Theorem we deduce that $C \simeq C'$. □

The next example shows that given a Weil generator π for a number field $K = \mathbb{Q}(\pi)$ with non-trivial class group, we can have two non-isomorphic Jacobians as polarized abelian varieties which are isomorphic as unpolarized abelian varieties in the isogeny class determined by the minimal polynomial of π. For more examples and a general method to construct such curves see [How96].

Example 39. Consider the hyperelliptic curves over $\mathbb{F}_3$ defined by

$$C_1 : y^2 = 2x^5 + 2x^4 + x^3 + 2x^2 + 1 \text{ and } C_2 : y^2 = 2x^5 + x^4 + x + 1.$$

Observe (or use `Magma` to verify) that C_1 and C_2 are not isomorphic. Their Jacobians lie in the same isogeny class, which is determined by the Weil polynomial

$$h = x^4 - x^3 + x^2 - 3x + 9.$$

Let $K = \mathbb{Q}[x]/(h) = \mathbb{Q}(\pi)$, which is the same field as in Example 34. Note that π is a Weil generator for K but that the isogeny class is not super-isolated because the class group of K has order two. Using [Mar19, Thm. 4.3] we deduce that there are two isomorphism classes of abelian varieties in the isogeny class, represented by say A_1 and A_2. Using [Mar19, Thm. 5.4], we compute that one of the isomorphism classes admits two non-isomorphic principal polarizations, say (A_1, θ_1) and (A_1, θ_2), while A_2 is not principally polarized. Note that it is not surprising that A_1 has two non-isomorphic polarizations: indeed by [Mar19, Thm. 5.4] the number of non-isomorphic polarizations equals the size of $U_F^+ / \operatorname{Norm}_{K/F}(U_K)$ and in Example 34 we showed that it is 2. Denote by θ_1' (resp. θ_2') the canonical polarization of $\operatorname{Jac}(C_1)$ (resp. $\operatorname{Jac}(C_2)$). We deduce that, after possibly relabelling θ_1 and θ_2, we have isomorphisms $(\operatorname{Jac}(C_1), \theta_1') \simeq (A, \theta_1)$ and $(\operatorname{Jac}(C_2), \theta_2') \simeq (A, \theta_2)$. In particular we have $\operatorname{Jac}(C_1) \simeq \operatorname{Jac}(C_2) \simeq A_1$ as unpolarized abelian varieties.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix. Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$. *Algebra Number Theory*, 9(1):225–265, 2015.

[Del69] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.*, 8:238–243, 1969.

[Győ76] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné. III. *Publ. Math. Debrecen*, 23(1-2):141–165, 1976.

[HL12] Everett W. Howe and Kristin E. Lauter. New methods for bounding the number of points on curves over finite fields. In *Geometry and arithmetic*, EMS Ser. Congr. Rep., pages 173–212. Eur. Math. Soc., Zürich, 2012.

[How95] Everett W. Howe. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.*, 347(7):2361–2401, 1995.

[How96] Everett W. Howe. Constructing distinct curves with isomorphic Jacobians. *J. Number Theory*, 56(2):381–390, 1996.

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[Mar18a] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[Mar18b] Stefano Marseglia. Computing square-free polarized abelian varieties over finite fields. 2018.

[Mar19] Stefano Marseglia. Computing abelian varieties over finite fields isogenous to a power. *Res. Number Theory*, 5(4):Paper No. 35, 17, 2019.

[MN02] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[Mye83] Gerald Myerson. On resultants. *Proc. Amer. Math. Soc.*, 89(3):419–420, 1983.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Sch19] Travis Scholl. Super-isolated elliptic curves and abelian surfaces in cryptography. *Exp. Math.*, 28(4):385–397, 2019.

[Sch20] Travis Scholl. Super-isolated abelian varieties. *J. Number Theory*, 206:138–168, 2020.

[Sta74] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[The19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.7)*, 2019. `https://www.sagemath.org`.

[VS76] L. N. Vaserštein and A. A. Suslin. Serre's problem on projective modules over polynomial rings, and algebraic K-theory. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(5):993–1054, 1199, 1976.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[WM71] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. pages 53–64, 1971.

[Zar74] Ju. G. Zarhin. A remark on endomorphisms of abelian varieties over function fields of finite characteristic. *Izv. Akad. Nauk SSSR Ser. Mat.*, 38:471–474, 1974.

S. Marseglia, Mathematical Institute, Utrecht University, Utrecht, The Netherlands
E-mail: s.marseglia@uu.nl

T. Scholl, University of California, Irvine
E-mail: traviswscholl@gmail.com