Chapter 4

Effective bounds for Brauer groups of Kummer surfaces over number fields

O dear Ophelia, I am ill at these numbers

Polonius, HAMLET, Scene 2.2, line 123

The following chapter was written together with Victoria Cantoral-Farfán, Yunqing Tang and Sho Tanimoto. It is published in the Journal of the London Mathematical Society as [CFTTV18].

The general idea of the proof of the main result arose from discussions between all authors during the Arizona Winter School in March 2015. Thereafter, the contributions of the author of this thesis largely lie in writing parts of §4.3 and the entirety of §4.5, as well as taking part in discussing and carefully checking every result in this chapter. In particular, the expertise of the author of this thesis does not lie in §4.2.

The numbering of results in this chapter only slightly differs from the published paper. Any result numbered `x` in the published paper, is numbered 4.`x` in this thesis.

4.1 Introduction

In 1971, Manin observed that failures of Hasse principle and weak approximation can be explained by Brauer–Manin obstructions for many examples [Man71]. Let X be a smooth projective variety defined over a number field k. *The Brauer group of* X is defined as

$$\mathrm{Br}(X) := \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m).$$

Then one can define an intermediate set using class field theory

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}(X)} \subset X(\mathbb{A}_k),$$

where $\mathbb{A}_k$ is the adèlic ring associated to k. It is possible that $X(\mathbb{A}_k) \neq \emptyset$, but $X(\mathbb{A}_k)^{\mathrm{Br}(X)} = \emptyset$, whereby the Hasse principle fails for X. When this happens, we say that there is *a Brauer–Manin obstruction to the Hasse principle*. When $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq X(\mathbb{A}_k)$, we say that there is *a Brauer–Manin obstruction to weak approximation*. There is a large body of work on Brauer–Manin obstructions to the Hasse principle and weak approximation (see, e.g., the work by Manin [Man86], or any of the following [BSD75], [CTCS80], [CTSSD87], [CTKS87], [SD93], [SD99], [KT04], [Bri06], [BBFL07], [KT08], [Log08], [VA08], [LvL09], [EJ10], [HVAV11], [ISZ11], [EJ12b], [HVA13], [CTS13], [MSTVA17], [SZ14], [IS15], [Wit16]) and it is an open question if for K3 surfaces, Brauer–Manin obstructions suffice to explain failures of Hasse principle and weak approximation, i.e., $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ (see [HS16] for some evidence supporting this conjecture.)

The main question discussed in this paper is of computational nature: how can one compute $\mathrm{Br}(X)$ explicitly? It is shown by Skorobogatov and Zarhin in [SZ08] that $\mathrm{Br}(X)/\mathrm{Br}(k)$ is finite for any K3 surface X defined over a number field k, but they did not provide any effective bound for this group. Such an effective algorithm is obtained for degree 2 K3 surfaces in [HKT13] using explicit constructions of moduli spaces of degree 2 K3 surfaces and principally polarized abelian varieties. In this paper, we provide an effective algorithm to compute a bound for the order of $\mathrm{Br}(X)/\mathrm{Br}(k)$ when X is the Kummer surface associated to the Jacobian of a curve of genus 2:

THEOREM 4.1.1. *There is an effective algorithm that takes as input an equation of a smooth projective curve C of genus 2 defined over a number field k, and outputs an effective bound for the order of* $\mathrm{Br}(X)/\mathrm{Br}(k)$ *where X is the Kummer surface associated to the Jacobian* $\mathrm{Jac}(C)$ *of the curve C.*

We obtain the following corollary as a consequence of results in [KT11] and [PTvL15]:

Corollary 4.1.2. *Given a smooth projective curve C of genus 2 defined over a number field k, there is an effective description of the set*

$$X(\mathbb{A}_k)^{\mathrm{Br}(X)}$$

where X is the Kummer surface associated to the Jacobian $\mathrm{Jac}(C)$ of the curve C.

Note that given a curve C of genus 2, the surface $Y = \mathrm{Jac}(C)/\{\pm 1\}$ can be realized as a quartic surface in $\mathbb{P}^3$ (see [FS97, §2]) and the Kummer surface X associated to $\mathrm{Jac}(C)$ is the minimal resolution of Y, so one can find defining equations for X explicitly.

The quartic surface Y has sixteen nodes, and by considering the projection from one of these nodes, we may realize Y as a double cover of the plane. Thus X can be realized as a degree 2 K3 surface and our Theorem 4.1.1 follows from [HKT13]. It is remarked in [HKT13] that using the algebraic correspondence between X and $\mathrm{Jac}(C)$ it is possible to make [HKT13] into an actual algorithm for Kummer surfaces. However we take a different approach from [HKT13], and instead of using the Kuga–Satake construction we use a result of [SZ12] reducing our problem to the case of abelian surfaces. In particular, our algorithm provides a large, but explicit bound for the Brauer group of X. (See the example we discuss in §4.6.)

The method in this paper combines many results from the literature. The first key observation is that the Brauer group $\mathrm{Br}(X)$ admits the following stratification:

Definition 4.1.3. Let $\overline{X}$ denote $X \times_k \operatorname{Spec} \overline{k}$ where $\overline{k}$ is a given separable closure of k. Then we write

$$\mathrm{Br}_0(X) = \mathrm{im}\,(\mathrm{Br}(k) \to \mathrm{Br}(X)) \text{ and } \mathrm{Br}_1(X) = \ker\left(\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})\right).$$

Elements in $\mathrm{Br}_1(X)$ are called *algebraic elements*; those in the complement $\mathrm{Br}(X) \setminus \mathrm{Br}_1(X)$ are called *transcendental elements*.

Thus to obtain an effective bound for $\mathrm{Br}(X)/\mathrm{Br}_0(X)$, it suffices to study $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ and $\mathrm{Br}(X)/\mathrm{Br}_1(X)$. The group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ is well-studied, and it admits the following isomorphism:

$$\mathrm{Br}_1(X)/\mathrm{Br}_0(X) \cong \mathrm{H}^1(k, \mathrm{Pic}(\overline{X})).$$

Note that for a K3 surface X, we have an isomorphism $\mathrm{Pic}(X) = \mathrm{NS}(X)$. Thus as soon as we compute $\mathrm{NS}(\overline{X})$ as a Galois module, we are able to compute $\operatorname{Br}_1(X)/\operatorname{Br}_0(X)$. An algorithm to compute $\operatorname{NS}(\overline{X})$ is obtained in [PTvL15], but we consider another algorithm which is based on [Cha14].

To study $\operatorname{Br}(X)/\operatorname{Br}_1(X)$, we use effective versions of Faltings' theorem and combine them with techniques in [SZ08] and [HKT13]. Namely, we have an injection

$$\operatorname{Br}(X)/\operatorname{Br}_1(X) \hookrightarrow \operatorname{Br}(\overline{X})^\Gamma$$

where Γ is the absolute Galois group of k. As a consequence of [SZ12], we have an isomorphism of Galois modules

$$\operatorname{Br}(\overline{X}) = \operatorname{Br}(\overline{A}),$$

where $A = \operatorname{Jac}(C)$ is the Jacobian of C. Thus it suffice to bound the size of $\operatorname{Br}(\overline{A})^\Gamma$. To bound the cardinal of this group, we consider the following exact sequence as in [SZ08]:

$$0 \to \left(\operatorname{NS}(\overline{A})/\ell^n\right)^\Gamma \xrightarrow{f_n} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma \to \operatorname{Br}(\overline{A})^\Gamma_{\ell^n} \to$$
$$\to \mathrm{H}^1(\Gamma, \operatorname{NS}(\overline{A})/\ell^n) \xrightarrow{g_n} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})),$$

where ℓ is any prime and $\operatorname{Br}(\overline{A})_{\ell^n}$ is the ℓ^n-torsion part of the Brauer group of $\overline{A}$. Using effective versions of Faltings' theorem, we bound the cokernel of f_n and the kernel of g_n independently of n.

We emphasize that our algorithm is practical for any genus 2 curve whose Jacobian has Néron–Severi rank 1, i.e., we can actually implement and compute a bound for such a curve. For example, consider the following hyperelliptic curve of genus 2 defined over $\mathbb{Q}$:

$$C : y^2 = x^6 + x^3 + x + 1.$$

Let $A = \operatorname{Jac}(C)$ and let $X = \operatorname{Kum}(A)$ be the Kummer surface associated to A. The geometric Néron–Severi rank of A is 1. Combining our algorithm with the work of [Die02] and [Sko17], we show that

$$|\operatorname{Br}(X)/\operatorname{Br}(\mathbb{Q})| < 2^{10} \cdot 10^{805050}.$$

Our effective bound explicitly depends on the Faltings height of the Jacobian of C, so it does not provide any uniform bound as conjectured in [TVA16], [AVA18], and [VA17]. However, it is an open question whether the Faltings height in Theorem 4.2.13 is needed. If there is a uniform bound for Theorem 4.2.13 which does not depend on the Faltings height, then our proof provides a uniform bound for the Brauer group. Such a uniform bound is obtained for elliptic curves in [VAV17].

Even though our method can handle any curve of genus 2 defined over a number field k, we will focus on the case of curves whose Jacobians have the geometric Picard rank 1. In other cases (non-simple cases), we can provide better bounds but we will not discuss them in this paper. The reader who is interested in these cases is encouraged to refer to the arXiv version of this paper. ([CFTTV16])

The paper is organized as follows. In §4.2 we review effective versions of Faltings' theorem and consequences that will be useful for our purposes. In §4.3 we review methods from the literature in order to compute the Néron–Severi lattice as a Galois module. §4.4 proves our bounds for the size of the transcendental part. §4.5 is devoted to Magma computations in the lowest rank case and §4.6 explores an example.

Acknowledgments

The authors would like to thank Martin Bright, Edgar Costa, Éric Gaudron, Brendan Hassett, David Holmes, Hendrik Lenstra, Ronald van Luijk, Chloe Martindale, Rachel Newton, Fabien Pazuki, Dan Petersen, Padmavathi Srinivasan and Yuri Tschinkel for useful discussions and comments. In particular they would like to thank Rachel Newton for her comments on the early draft of this paper. They also would like to thank Andreas-Stephan Elsenhans for providing them with the Magma code of the algorithm in [EJ12a]. They would like to thank Alexei Skorobogatov for pointing out a mistake in the earlier version of this paper. They would also like to thank the anonymous referees for suggestions to improve the exposition and the bound in §4.6 using [Die02] and [Sko17].

This paper began as a project in Arizona Winter School 2015 "Arithmetic and Higher-dimensional varieties". The authors would like to thank AWS for their hospitality and travel support. Finally the authors are grateful to Tony Várilly-Alvarado for suggesting this project, many conversations where he patiently answered our questions, and for his constant encouragement. This project and AWS have been supported by NSF grant DMS-1161523. Cantoral-Farfán was supported by the Conacyt fellowship. Tang was a member at the Institute for Advanced Study, supported by NSF grant DMS-1128155 to IAS. Tanimoto is partially supported by Lars Hesselholt's Niels Bohr professorship and MEXT Japan, Leading Initiative for Excellent Young Researchers (LEADER).

4.2 Effective version of Faltings' theorem

One important input of our main theorem is an effective version of Faltings' isogeny theorem. Such a theorem was first proved by Masser and Wüstholz in [MW95] and the computation of the constants involved was made explicit by Bost [Bos96] and Pazuki [Paz12]. The work of Gaudron and Rémond [GR14] gives a sharper bound. Although the general results are valid for any abelian variety over a number field, we will only focus on abelian surfaces.

The main result of this section is in §4.2.4. The reader may skip §4.2.2 and §4.2.3 on a first reading and refer to them later for the proof of the main result. We use the idea of Masser and Wüstholz to reduce the effective Faltings theorem to bound the minimal isogeny degree between certain abelian varieties and to bound the volume of the $\mathbb{Z}$-lattice of the endomorphism ring of the given abelian surface. These two things are bounded by a constant only depending on the Faltings height and the degree of the field of definition using the idea of Gaudron and Rémond. To compute a bound of Faltings height, we use a formula due to Pazuki and Magma.

Let A be an abelian surface defined over a number field k. Without further indication, A will be the Jacobian of some hyperelliptic curve C, principally polarized by the theta divisor, and we use L to denote the line bundle on A corresponding to the theta divisor. Throughout this section, when we say there is an isogeny between abelian varieties A_1 and A_2 of degree at most D, it means that there exist isogenies $A_1 \to A_2$ and $A_2 \to A_1$ both whose degrees are at most D.

4.2.1 Faltings height

The bounds in the effective Faltings theorems discussed in our paper depend on the stable Faltings height of the given abelian surface. We denote the stable Faltings height of A by $h(A)$ (with the normalization as in the original work of Faltings [Fal86]). In order to obtain a bound without Faltings height, we now describe how to obtain an upper bound of $h(\mathrm{Jac}(C))$ using the work of Pazuki [Paz14] and Magma.

Assume that the hyperelliptic curve C is given by $y^2 + G(x)y = F(x)$, where $G(x), F(x)$ are polynomials in x of degrees at most 3 and 6 respectively.

PROPOSITION 4.2.1. *Given a complex embedding σ of k, we use τ_σ to denote a period matrix of the base change $C_{\mathbb{C}}$ via σ. Let Δ be $2^{-12}\operatorname{Disc}_6(4F+G^2)$, where Disc_6 means taking the discriminant of a degree 6 polynomial. Then $h(\operatorname{Jac}(C))$ is bounded from above by*

$$-\log(2\pi^2) + \frac{1}{[k:\mathbb{Q}]}\Big(\frac{1}{10}\log(\Delta) - \sum_{\sigma}\log(2^{-1/5}|J_{10}(\tau_\sigma)|^{1/10}\det(\Im\tau_\sigma)^{1/2})\Big),$$

where σ runs through all complex embeddings of k.

Notice that the functions *AnalyticJacobian* and *Theta* in MAGMA compute period matrices τ_σ of $\operatorname{Jac}(C)$ and $J_{10}(\tau_\sigma)$, which is the square of the product of all even theta functions.

Proof. Let k' be a finite extension of k such that after base change to k', the variety $\operatorname{Jac}(C)_{k'}$ has semistable reduction everywhere. For example, k' can be taken to be the field of definition of all 12-torsion points. Then the stable Faltings height of $\operatorname{Jac}(C)$ is given by the Faltings height of $\operatorname{Jac}(C)$ over k'.

The inequality in the proposition follows from Pazuki's formula [Paz14, Thm. 2.4] once we bound the non-archimedean local term

$$\frac{1}{d}\sum_{v|\Delta_{min}} d_v f_v \log N_{k'/\mathbb{Q}}(v),$$

where $d = [k':\mathbb{Q}]$, $d_v = [k'_v:\mathbb{Q}_p]$ if $v|p$, Δ_{min} is the minimal discriminant of C over k', and $10 f_v \le \operatorname{ord}_v(\Delta_{min})$. By definition of minimal discriminant, we have $\Delta_{min}|\Delta$ and hence the local term is bounded by $\frac{1}{d}\sum_{v|\Delta} d_v \frac{\operatorname{ord}_v(\Delta)}{10}\log N_{k'/\mathbb{Q}}(v) = \frac{\log(\Delta)}{10[k:\mathbb{Q}]}$. □

REMARK 4.2.2. Following [Kau99, Sec. 4,5], one can compute the exact local contribution in Pazuki's formula at $v \nmid 2$ by studying the roots of $F(x)$ assuming $G = 0$.

4.2.2 Preliminary results

In this subsection, we recall some key facts about Euclidean lattices and results in transcendence theory that will be used to obtain an effective version of Faltings' theorem.

Let B be the abelian variety $A \times A$ principally polarized by $pr_1^*L \otimes pr_2^*L$ and B' an abelian variety over k isogenous to B over k. Let $\widehat{B}'$ be the dual abelian variety of B' and let $Z(B')$ be the principally polarizable abelian variety $(B')^4 \times (\widehat{B}')^4$. We fix a principal polarization on $Z(B')$.

Since A (resp. B and $Z(B')$) is principally polarized, one defines the Rosati involution $(-)^\dagger$ on $\mathrm{End}_k(A)$ (resp. going from $\mathrm{Hom}_k(B, Z(B'))$ to $\mathrm{Hom}_k(Z(B'), B)$). The quadratic form $\mathrm{Tr}(\varphi\varphi^\dagger)$ defines a norm on $\mathrm{End}_k(A)$ (resp. $\mathrm{Hom}_k(B, Z(B'))$).[1] We use $v(A)$ to denote $\mathrm{vol}(\mathrm{End}_k(A))$ with respect to this norm. Let k_1 be a Galois extension of k. We denote by Λ (resp. Λ', Λ'_{k_1}) the smallest real number which bounds from above the norms of all elements in some $\mathbb{Z}$-basis of some sub-lattice (of finite index) of $\mathrm{End}_k(A)$ (resp. $\mathrm{Hom}_k(B, Z(B'))$, $\mathrm{Hom}_{k_1}(B, Z(B'))$)[2].

By definition, $v(A) \leq \Lambda^r$, where r is the $\mathbb{Z}$-rank of $\mathrm{End}_k(A)$. Moreover, Λ'_{k_1} is also the smallest real number which bounds from above the norms of all elements in some $\mathbb{Z}$-basis of $\mathrm{Hom}_{k_1}(A, Z(B'))$.

Lemma 4.2.3 ([GR14, Lem. 3.3]). *We have* $\Lambda' \leq [k_1 : k]\Lambda'_{k_1}$.

The following three results are consequences of Faltings' isogeny formula and Bost's lower bound for Faltings heights.

Lemma 4.2.4 (Faltings). *Let $\phi : A_1 \to A_2$ be an isogeny between abelian varieties. Then*

$$h(A_1) - \frac{1}{2}\log\deg(\phi) \leq h(A_2) \leq h(A_1) + \frac{1}{2}\log\deg(\phi).$$

Lemma 4.2.5 (Bost). *For any abelian variety A_1, one has*

$$h(A_1) \geq -\tfrac{3}{2}\dim A_1.$$

Lemma 4.2.6 (See for example [GR14, p. 2096]). *Let H be a sub abelian variety of a principally polarized abelian variety A_1 and* $\deg H$ *the degree of H with respect to the polarization line bundle on A_1. Then we have*

$$h(H) \leq h(A_1) + \log\deg H + \frac{3}{2}(\dim A_1 - \dim H).$$

[1] This quadratic form is positive definite by [Mum70, p. 192] and [GR14, Prop. 2.5].

[2] This means that if r is the rank of $\mathrm{End}_k(A)$, then there exists a free family $w_1, \ldots, w_r \in \mathrm{End}_k(A)$ such that the norm of w_i is no greater than Λ.

The following result is a direct consequence of the Theorem of Periods by Gaudron and Rémond. See for example [GR14, p. 2095–2096].

Lemma 4.2.7 (Theorem of Periods). *Let H be a polarized abelian variety over k_1. Fix an embedding of k_1 into $\mathbb{C}$ and let Ω_H be the period lattice of $H(\mathbb{C})$ endowed with the norm $||\cdot||$ given by the real part of the Riemann form of the polarization. Assume that $\omega \in \Omega_H$ is not contained in the period lattice of any proper sub abelian variety of H. Then we have*

$$(\deg H)^{1/\dim H} \leq 50[k_1 : \mathbb{Q}]h^{2\dim H+6} \max(1, h(H), \log \deg H)||\omega||^2.$$

Proof. Gaudron and Rémond's Theorem of Periods implies that the same inequality holds by replacing $||\omega||^2$ by δ^2, where δ is the supremum among all proper sub abelian varieties H' of H of the minimum distance from $\omega \in \Omega_H \backslash \Omega'_H$ to the tangent space of H'. By our assumption on ω, one has $\delta \leq ||\omega||$. □

The following lemma is a direct consequence of Autissier's Matrix Lemma and it will be used to bound the norm of elements in period lattices.

Lemma 4.2.8 (Autissier). *Let A_1 be a principally polarized abelian variety over k_1 and for any embedding $\sigma : k_1 \to \mathbb{C}$, let Ω_σ be the period lattice of $A_{1,\sigma}(\mathbb{C})$. We denote by Λ_σ the smallest real number which bounds the norms of all elements in some $\mathbb{Z}$-basis of some sub-lattice (of finite index) of Ω_σ. Then for any $\epsilon \in (0,1)$*

$$\sum_\sigma \Lambda_\sigma^2 \leq \frac{6[k_1 : \mathbb{Q}](2\dim A_1)^2}{(1-\epsilon)\pi}\left(h(A_1) + \frac{\dim A_1}{2}\log\left(\frac{2\pi^2}{\epsilon}\right)\right).$$

Proof. This follows from [Aut13, Cor. 1.4] and [GR14, Cor. 3.6]. See also the proof of [GR14, Lem. 8.4]. □

Lemma 4.2.9 ([Sil92, Thm. 4.1, 4.2, Cor. 3.3]). *Given abelian varieties A_1, A_2 of dimension g, g' defined over k, let K be the smallest field where all the $\overline{k}$-endomorphisms of $A_1 \times A_2$ are defined. Then we have*

$$[K : k] \leq 4(9g)^{2g}(9g')^{2g'}.$$

The following elementary lemma is useful.

Lemma 4.2.10 ([GR14, Lem. 8.5]). *Let $u \geq e^{1/2}$ and $v \geq 0$ be real numbers. Assume that $x > 0$ and $x \leq u(v + \log x)$. Then $x \leq 2u(\log u + v)$.*

4.2.3 The bound of isogeny degrees

This subsection includes some upper bounds of the minimal isogeny degree between B and any B' over k isogenous to B. Here we will obtain an upper bound depending on $h(B')$ and in the proof of main theorem in next subsection, we will use the properties of the Faltings height to obtain a bound only depending on $h(A)$ and $[k:\mathbb{Q}]$. This upper bound is a key input to obtain our effective Faltings theorem.

An explicit bound of minimal isogeny degrees is given for general abelian varieties in [GR14, Thm. 1.4] so readers may use their bound and Lemma 4.2.14 later to finish the proof of Theorem 4.2.13 when $\mathrm{End}_k(A) = \mathbb{Z}$. However, we give a proof here since the same technique is used to bound Λ, which in turn will be used to deduce the effective Faltings theorem from the upper bound of minimal isogeny degree when $\mathrm{End}_k(A) \neq \mathbb{Z}$.

PROPOSITION 4.2.11. *There exists an isogeny $B' \to B$ over k of degree at most $2^{48}(\Lambda')^{16}\Lambda^{16r}$, where Λ, Λ' are defined in §4.2.2 and r is the $\mathbb{Z}$-rank of* $\mathrm{End}_k(A)$.

Proof. This follows from [GR14, Prop. 6.2] by noticing that the $\widehat{W_i}$ term there is not needed since A is principally polarized and by the fact that $v(A) \leq \Lambda^r$. □

LEMMA 4.2.12. *Let m_A and $m_{A,B'}$ denote* $\max(1, h(A))$ *and respectively* $\max(1, h(A), h(B'))$. *We have*

$$\Lambda \leq \begin{cases} 2 & \text{if } \bar{r} = 1, \\ 4^5 \cdot 9^8 \Big[5.04 \cdot 10^{24}[k:\mathbb{Q}] m_A & \\ \quad \cdot \left(\frac{5}{4} m_A + \log[k:\mathbb{Q}] + \log m_A + 60\right) \Big]^{8/\bar{r}} & \text{if } \bar{r} = 2 \text{ or } 4. \end{cases}$$

and

$$\Lambda_{B,B'} \leq 4^{11} \cdot 9^{12} \Big[(4.4 \cdot 10^{46}[k:\mathbb{Q}] m_{A,B'} \\ \left(9 m_{A,B'} + 8 \log m_{A,B'} + 8 \log[k:\mathbb{Q}] + 920\right) \Big]^{16/\bar{r}}.$$

Proof. Recall that $\bar{r}$ denotes the $\mathbb{Z}$-rank of $\mathrm{End}_{\bar{k}}(A)$. To deduce the bound of Λ, we first study the case $\bar{r} = 1$. In this case, $\mathrm{End}_{\bar{k}}(A) = \mathbb{Z}$ and by definition the norm of the identity map is $\sqrt{\mathrm{Tr}(\mathrm{id})} = \sqrt{4} = 2$. In other words, $\Lambda = 2$.

We postpone the discussion of Λ for $\bar{r} = 2, 4$, since it is a simplified version of the following discussion on the bound of Λ'. The estimate of Λ' is essentially [GR14, Lem. 9.1]. We modify its proof here to obtain a sharper bound for this special case.

Let k_1 be the field where all the $\overline{k}$-endomorphisms of $A \times B'$ are defined. Then by Lemma 4.2.9, we have $[k_1 : k] \leq 4 \cdot 18^4 \cdot 36^8 = 4^{11} \cdot 9^{12}$. For any complex embedding $\sigma : k_1 \to \mathbb{C}$, we may view A and $Z(B')$ as abelian varieties over $\mathbb{C}$ and let $\Omega_{A,\sigma}$ and $\Omega_{Z(B'),\sigma}$ be the period lattices. The principal polarization induces a metric on $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$). More precisely, the polarization line bundle gives rise to the Riemann form (a Hermitian form) on the tangent space of A (resp. $Z(B)$) and its real part defines a norm on the real tangent space and hence on $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$). We use $\Lambda(\Omega_{A,\sigma})$ (resp. $\Lambda(\Omega_{Z(B'),\sigma})$) to denote the smallest real number which bounds from above the norms of all elements in some $\mathbb{Z}$-basis of some sublattice (of finite index) of $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$).

Let $\omega_1, \ldots, \omega_4$ (resp. $\chi_1, \ldots, \chi_{64}$) be a free family in $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$) such that $||\omega_i|| \leq \Lambda(\Omega_{A,\sigma})$ (resp.$||\chi_i|| \leq \Lambda(\Omega_{Z(B'),\sigma})$) hold. Let ω be $(\omega_1, \chi_1, \ldots, \chi_{64}) \in \Omega_{A,\sigma} \oplus (\Omega_{Z(B'),\sigma})^{64}$ and let H be the smallest abelian subvariety of $A \times (Z(B'))^{64}$ whose Lie algebra (over $\mathbb{C}$) contains ω. Since $\chi_1, \ldots, \chi_{64}$ generate a sublattice of finite index of $\Omega_{Z(B'),\sigma}$, then for any $\chi \in \Omega_{Z(B'),\sigma}$, there exist $\ell, m_1, \ldots, m_{64}$ such that $\ell\chi + \sum m_i\chi_i = 0$ and hence H satisfies the assumption of [GR14, Prop. 7.1]. Therefore

$$\Lambda'_{k_1} \leq (\deg H)^2.$$

Let $h = \dim H$. By [GR14, Lem. 8.1], we have $2 \leq h \leq 8/\bar{r} \leq 8$ and by Lemma 4.2.7,

$$(\deg H)^{1/h} \leq 50[k_1\mathbb{Q}]h^{2h+6} \max(1, h(H), \log\deg H)||\omega||^2.$$

Now we bound $||\omega||$. Notice that by definition, we have

$$||\omega||^2 = ||\omega_1||^2 + \sum_i ||\chi_i||^2 \leq \Lambda(\Omega_{A,\sigma})^2 + 64\Lambda(\Omega_{Z(B'),\sigma})^2.$$

From now on, we fix a σ such that $\Lambda(\Omega_{A,\sigma})^2 + 64\Lambda(\Omega_{Z(B'),\sigma})^2$ is the smallest.

Then by Lemma 4.2.8, we have that, for any $\epsilon \in (0, 1)$,

$$||\omega||^2 \leq \frac{6}{(1-\epsilon)\pi}\left(16h(A) + 8^7h(B') + (16 + 16^4)\log\left(\frac{2\pi^2}{\epsilon}\right)\right).$$

By taking $\epsilon = \frac{1}{40}$, we have $||\omega||^2 \leq 5 \times 10^6 \max(1, h(A), h(B'))$. Combining the above inequalities, we have the bound

$$(\deg H)^{\bar{r}/8} \leq 1.85 \times 10^{28} [k_1 : \mathbb{Q}] \max(1, h(A), h(B')) \cdot \left(9 \max(1, h(A), h(B')) + \log \deg H + 48\right),$$

where we use Lemma 4.2.6 to obtain

$$h_F(H) \leq 9 \max(1, h(A), h(B')) + \log \deg H + 48.$$

Then by Lemma 4.2.10, we have

$$\deg H \leq \Big[3.7 \cdot 10^{28} [k_1 : \mathbb{Q}] m_{A,B'} \cdot \left(9 m_{A,B'} + 48 + \frac{8}{\bar{r}} \log \left(1.85 \cdot 10^{28} [k_1 : \mathbb{Q}] \frac{8 m_{A,B'}}{\bar{r}} \right) \right) \Big]^{8/\bar{r}}.$$

Then we have (by Lemma 4.2.3) that Λ' can be bounded from above by

$$[k_1 : k] \Lambda'_{k_1} \leq [k_1 : k] (\deg H)^2$$

and subsequently by

$$\begin{aligned}
&[k_1 : k] \Big[3.7 \cdot 10^{28} [k_1 : \mathbb{Q}] m_{A,B'} \cdot \left(9 m_{A,B'} + 48 + \frac{8}{\bar{r}} \log \left(1.85 \cdot 10^{28} [k_1 : \mathbb{Q}] \frac{8 m_{A,B'}}{\bar{r}} \right) \right) \Big]^{16/\bar{r}} \\
&\leq 4^{11} \cdot 9^{12} \Big[4.4 \cdot 10^{46} [k : \mathbb{Q}] m_{A,B'} \cdot \left(9 m_{A,B'} + 8 \log m_{A,B'} + 8 \log [k : \mathbb{Q}] + 920 \right) \Big]^{16/\bar{r}}.
\end{aligned}$$

Now we assume that $\bar{r} = 2$ or 4. In this case we cannot compute Λ so we apply the same strategy as for the bound on Λ'. The proof is practically identical, but the bounds are different. In this case we bound the degree $[k_1 : k] \leq 4 \cdot 18^8$ and there exists an abelian subvariety H of $A \times A^4$ over k_1 such that the bounds

$$\Lambda \leq [k_1 : k] (\deg H)^2$$

and

$$\deg H \leq \Big[100 \cdot 4^{19} \cdot 9^8 \cdot 1063 \cdot [k : \mathbb{Q}] m_A \cdot (5 m_A + 4 \log [k : \mathbb{Q}] + 4 \log m_A + 240) \Big]^{8/\bar{r}}$$

are satisfied. Combining these two inequalities together, we obtain the bound for Λ. □

4.2.4 Effective Faltings' theorem in the geometrically simple case

We assume that A is geometrically simple. Equivalently, A is not isogenous to a product of two elliptic curves over $\bar{k}$. Let Γ be its absolute Galois group. For a positive integer m, let A_m be the $\mathbb{Z}[\Gamma]$-module of m-torsion points of $A(\bar{k})$.

THEOREM 4.2.13. *For any integer m, let M_m be the smallest positive integer such that the cokernel of the map $\mathrm{End}_k(A) \to \mathrm{End}_\Gamma(A_m)$ is killed by M_m.*[3] *There exists an upper bound $\widetilde{M}$ for M_m depending on $h(A)$ and $[k:\mathbb{Q}]$ which is independent of m. Explicitly, when $\bar{r}=1$, then $\widetilde{M}$ equals*

$$2^{4664} c_1^{16} c_2(k)^{256} \left(2h(A) + \tfrac{8}{17}\log[k:\mathbb{Q}] + 8\log c_1 + 128\log c_2(k) + 1503\right)^{512},$$

and when $\bar{r} = 2$ or 4,

$$\widetilde{M} = (r/4)^{r/2} 2^{48} \cdot c_1^{16} c_2(k)^{256} c_8(A,k)^{17r} \cdot \Big(16\log c_1 + \frac{256}{\bar{r}}\log c_2(k) + 16r\log c_8(A,k) + 4h(A) + \tfrac{16}{17}\log[k:\mathbb{Q}] + 1400\Big)^{512/\bar{r}}.$$

Here r (resp. $\bar{r}$) is the $\mathbb{Z}$-rank of $\mathrm{End}_k(A)$ (resp. $\mathrm{End}_{\bar{k}}(A)$). We have that $r, \bar{r} \in \{1,2,4\}$ and $r \leq \bar{r}$.

The constants c_1 and c_2 are $c_1 = 4^{11}\cdot 9^{12}$ and $c_2(k) = 7.5\cdot 10^{47}[k:\mathbb{Q}]$, and $c_8(A,k)$ is

$$4^5 \cdot 9^8 \left(5.04\cdot 10^{24}[k:\mathbb{Q}] m_A \left(\tfrac{5}{4}m_A + \log[k:\mathbb{Q}] + \log m_A + 60\right)\right)^{8/\bar{r}},$$

where m_A is $\max(1, h(A))$.

We denote by $b(B)$ the smallest integer such that for any abelian variety B' defined over k, if B' is isogenous to B over k, then there exists an isogeny $\phi : B' \to B$ over k of degree at most $b(B)$.

LEMMA 4.2.14. *With notation as above, $M_m \leq (r/4)^{r/2}\Lambda^r b(B)$.*

[3] Such M_m exists since $\mathrm{End}_\Gamma(A_m)$ is a finite group.

Proof. By [MW95, Lem. 3.2], one bounds M_m by $i(A)b(B)$, where $i(A)$ is the class index of the order $\mathrm{End}_k(A)$. By [MW95, eqn. 2.2] we have $i(A) \leq d(A)^{1/2}$, where $d(A)$ is the discriminant of $\mathrm{End}_k(A)$ as a $\mathbb{Z}$-module. Finally, by definition, $d(A)^{1/2} = (r/4)^{r/2}v(A) \leq (r/4)^{r/2}\Lambda^r$. $\square$

Proof of Theorem 4.2.13. We start by bounding the smallest degree of isogenies from B' to B, for which we have used the notation $b(B)$. Let $\phi : B' \to B$ be an isogeny of the smallest degree d. We want to bound d in terms of $h(A)$ and $[k : \mathbb{Q}]$. First, by Lemma 4.2.4, we have

$$h(B') \leq h(B) + \tfrac{1}{2}\log\deg(\phi) = 2h(A) + \tfrac{1}{2}\log\deg(\phi) = 2h(A) + \tfrac{1}{2}\log d.$$

Then $m_{A,B'} = \max(1, h(A), h(B')) \leq 2h(A) + \frac{1}{2}\log d + 7$, since $h(A) \geq -3$ by Lemma 4.2.5. Then by Lemma 4.2.12 and the fact $m_{A,B'} \geq \log m_{A,B'}$, we have

$$\Lambda' \leq c_1 \left(c_2(k)\left(c_3(A,k) + \tfrac{1}{2}\log d\right)^2\right)^{\frac{16}{\bar{r}}}, \tag{4.2.1}$$

where $\bar{r} = 1, 2$ or 4 and the constants are defined as

$$\begin{cases} c_1 = 4^{11} \cdot 9^{12}, \\ c_2(k) = 7.5 \cdot 10^{47}[k : \mathbb{Q}], \\ c_3(A,k) = 2h(A) + \frac{8}{17}\log[k : \mathbb{Q}] + \frac{1039}{17}. \end{cases}$$

We furthermore introduce the constants

$$\begin{cases} c_4(A,k) = \sqrt{c_2(k)}c_3(A,k), \\ c_5(k) = \dfrac{\sqrt{c_2(k)}}{2}, \\ c_6(A,k) = 2^{48} \cdot c_1^{16} \cdot \Lambda^{16r}, \end{cases}$$

and we rewrite inequality (4.2.1) as:

$$\Lambda' \leq c_1[c_4(A,k) + c_5(k)\log d]^{\frac{32}{\bar{r}}}.$$

Then by Lemma 4.2.11, we have

$$d = \deg\phi \leq 2^{48}(\Lambda')^{16}\Lambda^{16r} \leq c_6(A,k)\,[c_4(A,k) + c_5(k)\log d]^{\frac{32\cdot 16}{\bar{r}}}. \tag{4.2.2}$$

We define $c_7(A,k) = 2^{48} \cdot c_1^{16} \cdot c_8(A,k)^{16r}$ with $c_8(A,k)$ defined as

$$c_8(A,k) = \begin{cases} 2 & \text{if } \bar{r} = 1, \\ 4^5 \cdot 9^8 \cdot \Big(5.04 \cdot 10^{24}[k : \mathbb{Q}]m_A & \\ \quad \cdot \left(\frac{5}{4}m_A + \log[k : \mathbb{Q}] + \log m_A + 60\right)\Big)^{8/\bar{r}} & \text{if } \bar{r} = 2, 4. \end{cases}$$

Then by Lemma 4.2.12, $c_6(A,k) \le c_7(A,k)$. We rewrite inequality (4.2.2) as

$$d^{\frac{\bar{r}}{32\cdot 16}} \le u(A,k)\left(\tfrac{\bar{r}}{32\cdot 16}\log d + v(A,k)\right),$$

where

$$\begin{cases} u(A,k) = c_7(A,k)^{\frac{\bar{r}}{32\cdot 16}} c_5(A,k)\cdot \dfrac{32\cdot 16}{\bar{r}}, \\ v(A,k) = \dfrac{c_4(A,k)\bar{r}}{32\cdot 16 c_5(A,k)}. \end{cases}$$

Then by Lemma 4.2.10, we have

$$d^{\frac{\bar{r}}{32\cdot 16}} \le 2u(A,k)[\log u(A,k) + v(A,k)].$$

Define

$$C(A,k) = 2u(A,k)[\log u(A,k) + v(A,k)],$$

which only depends on $h(A)$ and $[k:\mathbb{Q}]$. Then we find

$$b(B) \le C(A,k)^{\frac{32\cdot 16}{\bar{r}}}.$$

By Lemmas 4.2.14, 4.2.12, we obtain:

$$M_m \le (r/4)^{r/2}\Lambda^r b(B) \le (r/4)^{r/2} c_8(A,k)^r C(A,k)^{\frac{32\cdot 16}{\bar{r}}}.$$

Using $r \le \bar{r}$, in the case $\bar{r} = 1$ we find

$$M_m \le 2^{4664} c_1^{16} c_2(k)^{256}\Big(2h(A) + \tfrac{8}{17}\log[k:\mathbb{Q}] + 8\log c_1 + 128\log c_2(k) + 1503\Big)^{512},$$

and in the case $\bar{r} = 2$ or 4 we find that M_m is bounded above by

$$(r/4)^{r/2} 2^{48}\cdot c_1^{16} c_2(k)^{256} \cdot\Big(4^5\cdot 9^8\big(5.04\cdot 10^{24}[k:\mathbb{Q}]m_A\big(\tfrac{5}{4}m_A + \log[k:\mathbb{Q}] + \log m_A + 60\big)\big)^{8/\bar{r}}\Big)^{17r} \cdot\Big[16\log c_1 + \frac{256}{\bar{r}}\log c_2(k) + 16r\log c_8(A,k) + 4h(A) + \tfrac{16}{17}\log[k:\mathbb{Q}] + 1400\Big]^{512/\bar{r}}.$$

The constants c_1, $c_2(k)$ and $c_8(A,k)$ only depend on the Faltings height and the degree of the field extension $[k:\mathbb{Q}]$. □

4.3 Effective computations of the Néron–Severi lattice as a Galois module

Our goal of this section is to prove the following theorem:

THEOREM 4.3.1. *There is an explicit algorithm that takes input a smooth projective curve C of genus 2 defined over a number field k, and outputs a bound of the algebraic Brauer group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ where X is the Kummer surface associated to the Jacobian $\mathrm{Jac}(C)$.*

A general algorithm to compute Néron–Severi groups for arbitrary projective varieties is developed in [PTvL15], so here we consider algorithms specialized to the Kummer surface X associated to a principally polarized abelian surface A.

4.3.1 The determination of the Néron–Severi rank of A

THEOREM 4.3.2. *The following is a complete list of possibilities for the rank ρ of $\mathrm{NS}(\overline{A})$. For any prime $\mathfrak{p}$ we denote by $\rho_{\mathfrak{p}}$ the reduction of ρ modulo $\mathfrak{p}$.*

1. *When A is geometrically simple, we consider $D = \mathrm{End}_{\bar{k}}(A) \otimes \mathbb{Q}$, which has the following possibilities:*

   (a) *$D = \mathbb{Q}$ and $\rho = 1$. There exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 2$.*

   (b) *D is a totally real quadratic field. Then $\rho = 2$ and there exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 2$.*

   (c) *D is a indefinite quaternion algebra over $\mathbb{Q}$. Then $\rho = 3$ and there exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 4$.*

   (d) *D is a degree 4 CM field. Then $\rho = 2$ and there exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 2$. In fact this holds for the set of $\mathfrak{p}$'s such that A has ordinary reduction at $\mathfrak{p}$.*

2. *When A is isogenous over $\bar{k}$ to $E_1 \times E_2$ for two elliptic curves. Then*

   (a) *if E_1 is isogenous to E_2 and CM, then $\rho = 4$ and $\rho_{\mathfrak{p}} = 4$ for all ordinary reduction places.*

(b) *if* E_1 *is isogenous to* E_2 *but not CM, then* $\rho = 3$ *and* $\rho_{\mathfrak{p}} = 4$ *for all ordinary reduction places.*

(c) *if* E_1 *is not isogenous to* E_2*, then* $\rho = 2$ *and there exists a density one set of primes* $\mathfrak{p}$ *such that* $\rho_{\mathfrak{p}} = 2$*.*

Notice that for all the above statements, by an abuse of language, being density one means there exists a finite extension of k *such that the primes are of density one with respect to this finite extension.*

Proof. We apply [Mum70, p. 201 Thm. 2 and p.208] (and the remark on p. 203 referring to the work of Shimura) to obtain the list of the rank ρ. When A is geometrically simple, we can only have A of type I, II, and IV (in the sense of the Albert's classification). In the case of Type I, the totally real field may be $\mathbb{Q}$ or quadratic. In this case, the Rosati involution is trivial. This gives case (1)-(a,b). By [Mum70, p. 196], the Rosati involution of Type II is the transpose and its invariants are symmetric 2-by-2 matrices, which proves case (1)-(c). In the case of Type IV, D is a degree 4 CM field. In this case, the Rosati involution is the complex conjugation and this gives case (1)-(d). When A is not geometrically simple, then A is isogenous to the product of two elliptic curves and all these cases are easy.

Notice that after a suitable field extension, there exists a density one set of primes such that A has ordinary reduction (due to Katz, see [Ogu82] Sec. 2). We first pass to such an extension and only focus on primes where A has ordinary reduction. Then $\rho_{\mathfrak{p}} = 2$ if A mod $\mathfrak{p}$ is geometrically simple and $\rho_{\mathfrak{p}} = 4$ if A is not. Since $\rho_{\mathfrak{p}} \geq \rho$, we see that $\rho_{\mathfrak{p}} = 4$ in (1)-(c), (2)-(a,b) for any $\mathfrak{p}$ where A has ordinary reduction. When $\rho = 2$ (case (1)-(b,d), (2)-(c)), the dimension over $\mathbb{Q}$ of the orthogonal complement T of $\mathrm{NS}(\overline{A})$ in the Betti cohomology $\mathrm{H}^2(A, \mathbb{Q})$ is 4. By [Cha14, Thm. 1], if $\rho_{\mathfrak{p}}$ were 4 for a density one set of primes, then the endomorphism algebra E of T as a Hodge structure would have been a totally real field of degree $\rho_{\mathfrak{p}} - \rho = 2$ over $\mathbb{Q}$. Then T would have been of dimension 2 over E, which contradicts the assumption of the second part of Charles' theorem. Now the remaining case is (1)-(a). By [Cha14], for a density one set of $\mathfrak{p}$, the rank $\rho_{\mathfrak{p}}$ only depends on the degree of the endomorphism algebra E of the transcendental part T of the $\mathrm{H}^2(A, \mathbb{Q})$. This degree is the same for all A in case (1)-(a) since $E = \mathrm{End}(T) \subset \mathrm{End}(\mathrm{H}^2(A, \mathbb{Q}))$ is a set of Hodge cycles of $A \times A$ and all A in this case have the same set of Hodge cycles. For more details we refer the reader to [CF16]. Hence we only need to study a generic abelian surface. For a generic abelian surface, its ordinary reduction is a (geometrically) simple CM abelian surface and hence $\rho_{\mathfrak{p}}$ is 2. $\square$

Algorithms to compute the geometric Néron–Severi rank of A

Here we discuss an algorithm provided by Charles in [Cha14]. Charles' algorithm is to compute the geometric Néron–Severi rank of any $K3$ surface X, and his algorithm relies on the Hodge conjecture for codimension 2 cycles in $X \times X$. However, the situation where the Hodge conjecture is needed does not occur for abelian surfaces, so his algorithm is unconditional for abelian surfaces.

Suppose that A is a principally polarized abelian surface and Θ its principal polarization. We run the following algorithms simultaneously:

1. Compute Hilbert schemes of curves on A with respect to Θ for each Hilbert polynomial, and find divisors on A. Compute its intersection matrix using the intersection theory, and determine the rank of lattices generated by divisors one finds. This gives a lower bound η for $\rho = \operatorname{rk} \mathrm{NS}(\overline{A})$.

2. For each finite place $\mathfrak{p}$ of good reduction for A, compute the geometric Néron–Severi rank $\rho_{\mathfrak{p}}$ for $A_{\mathfrak{p}}$ using explicit point counting on the curve C combined with the Weil conjecture and the Tate conjecture. Furthermore compute the square class $\delta(\mathfrak{p})$ of the discriminant of $\mathrm{NS}(A_{\mathfrak{p}})$ in $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$ using the Artin–Tate conjecture:

$$P_2(q^{-s}) \sim_{s \to 1} \left(\frac{\#\,\mathrm{Br}(A_{\mathfrak{p}}) \cdot |\operatorname{disc}(\mathrm{NS}(A_{\mathfrak{p}}))|}{q} (1 - q^{1-s})^{\rho(A_{\mathfrak{p}})} \right),$$

   where P_2 is the characteristic polynomial of the Frobenius endomorphism on

$$\mathrm{H}^2_{\text{ét}}(\overline{A}_{\mathfrak{p}}, \mathbb{Q}_\ell),$$

   and q is the size of the residue field of $\mathfrak{p}$. When the characteristic is not equal to 2, then the Artin-Tate conjecture follows from the Tate conjecture for divisors ([Mil75]), and the Tate conjecture for divisors in abelian varieties is known ([Tat66]). Note that as a result of [LLR05], the size of the Brauer group must be a square. This gives us an upper bound for ρ.

When ρ is even, there exists a prime $\mathfrak{p}$ such that $\rho = \rho_{\mathfrak{p}}$. Thus eventually we obtain $\rho_{\mathfrak{p}} = \eta$ and we compute ρ.

When ρ is odd, it is proved in [Cha14, Prop. 18] that there exist $\mathfrak{p}$ and $\mathfrak{q}$ such that $\rho_{\mathfrak{p}} = \rho_{\mathfrak{q}} = \eta + 1$, but $\delta(\mathfrak{p}) \neq \delta(\mathfrak{q})$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. If this happens, then we can conclude that $\rho = \rho_{\mathfrak{p}} - 1$.

Remark 4.3.3. The algorithm (1) can be conducted explicitly in the following way: Suppose that our curve C of genus 2 is given as a subscheme in the weighted projective space $\mathbb{P}(1,1,3)$. Let $Y = \mathrm{Sym}^2(C)$ be the symmetric product of C. Then we have the following morphism

$$f : C \times C \to Y \to \mathrm{Jac}(C), \quad (P, Q) \mapsto [P + Q - K_C].$$

The first morphism $C \times C \to Y$ is the quotient map of degree 2, and the second morphism is a birational morphism contracting a smooth rational curve R over the identity of $\mathrm{Jac}(C)$. We denote the diagonal of $C \times C$ by Δ and the image of the morphism $C \ni P \mapsto (P, \iota(P)) \in C \times C$ by Δ' where ι is the involution associated to the degree 2 canonical linear system. Then we have

$$f^*\Theta \equiv 5p_1^*\{\mathrm{pt}\} + 5p_2^*\{\mathrm{pt}\} - \Delta.$$

Note that $f^*\Theta$ is big and nef, but not ample. If we have a curve D on $\mathrm{Jac}(C)$, then its pullback f^*D is a connected subscheme of $C \times C$ which is invariant under the symmetric involution and $f^*D.\Delta' = 0$, and vice verse. Hence instead of doing computations on $\mathrm{Jac}(C)$, we can do computations of Hilbert schemes and the intersection theory on $C \times C$. This may be a more effective way to find curves on $\mathrm{Jac}(C)$ and its intersection matrix.

Remark 4.3.4. The algorithm (2) is implemented in the paper [EJ12a].

4.3.2 The computation of the Néron–Severi lattice and its Galois action

Here we discuss an algorithm to compute the Néron–Severi lattice and its Galois structure. We have an algorithm to compute the Néron–Severi rank of $\overline{A}$, so we may assume it to be given. First we record the following algorithm:

Lemma 4.3.5. *Let S be a polarized abelian surface or a polarized K3 surface over k, with an ample divisor H. Suppose that we have computed a* *full rank sublattice* $M \subset \mathrm{NS}(\overline{S})$ *containing the class of* H*, i.e., we know its intersection matrix, the Galois structure on* $M \otimes \mathbb{Q}$*, and we know generators for* M *as divisors in* S*. Then there is an algorithm to compute* $\mathrm{NS}(\overline{S})$ *as a Galois module.*

Proof. We fix a basis $B_1, \cdots, B_r$ for M which are divisors on S. First note that the Néron–Severi lattice $\mathrm{NS}(\overline{S})$ is an overlattice of M. By Nikulin [Nik79, Sec. 1-4], there are only finitely many overlattices, (they correspond to isotropic subgroups in $D(M) = M^\vee/M$), and moreover we can compute all possible overlattices of M explicitly. Let N be an overlattice of M. We can determine whether N is contained in $\mathrm{NS}(\overline{S})$ in the following way:

Let $D_1, \ldots, D_s$ be generators for N/M. The overlattice N is contained in $\mathrm{NS}(\overline{S})$ if and only if the classes D_i are represented by integral divisors. After replacing D_i by $D_i + mH$, we may assume $D_i^2 > 0$ and $(D_i \cdot H) > 0$. If D_i is represented by an integral divisor, then it follows from Riemann–Roch that D_i is actually represented by an effective divisor C_i. We define $k = (D_i \cdot H)$ and $c = -\frac{1}{2}D_i^2$. The Hilbert polynomial of C_i with respect to H is $P_i(t) = kt + c$. Now we compute the Hilbert scheme Hilb^{P_i} associated with $P_i(t)$. For each connected component of Hilb^{P_i}, we take a member E_i of the universal family and compute the intersection numbers $(B_1 \cdot E), \ldots, (B_r \cdot E)$. If these coincide with the intersection numbers of D_i, then that member E_i is an integral effective divisor representing D_i. If we cannot find such an integral effective divisor for any connected component of Hilb^{P_i}, then we conclude that N is not contained in $\mathrm{NS}(\overline{S})$.

In this way we can compute the maximal overlattice $N_{\max}$ all whose classes are represented by integral divisors. This lattice $N_{\max}$ must be $\mathrm{NS}(\overline{S})$. Since M is full rank, the Galois structure on M induces the Galois structure on $\mathrm{NS}(\overline{S})$. □

From now on we focus on the case where $\overline{A}$ is simple and has Néron–Severi rank $\rho = 1$.

Proposition 4.3.6. *Let* A *be a principally polarized abelian surface defined over a number field* k *whose geometric Néron–Severi rank is* 1*. Let* X *be the Kummer surface associated to* A*. Then there is an explicit algorithm that computes* $\mathrm{NS}(\overline{X})$ *as a Galois module and furthermore computes the group* $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$*.*

The abelian surface A is a principally polarized abelian surface, so the lattice $\mathrm{NS}(\overline{A})$ is isomorphic to the lattice $\langle 2\rangle$ with the trivial Galois action. We denote the blow up of 16 2-torsion points on A by $\widetilde{A}$ and the 16 exceptional curves on $\tilde{A}$ by E_i. There is an isometry

$$\mathrm{NS}(\widetilde{A}_{\overline{k}}) \cong \mathrm{NS}(\overline{A}) \oplus \bigoplus_{i=1}^{16} \mathbb{Z}E_i.$$

We want to determine the Galois structure of this lattice. To this end, one needs to understand the Galois action on the set of 2-torsion elements on $\overline{A}$. This can be done explicitly in the following way: Suppose that A is given as a Jacobian of a smooth projective curve C of genus 2. Then C is a hyperelliptic curve whose canonical linear series is a degree 2 morphism. We denote the ramification points (over $\overline{k}$) of this degree 2 map by $p_1, \cdots, p_6$. One can find the Galois action on these ramification points from the polynomial defining C. All non-trivial 2-torsion points of $\overline{A}$ are given by $p_i - p_j$ where $i < j$. Note that $p_i - p_j \sim p_j - p_i$ as classes in $\mathrm{Pic}(C)$. Thus, we can determine the Galois structure on the set of 2-torsion elements of $\overline{A}$.

Let X be the Kummer surface associated to A with the degree 2 finite morphism $\pi : \widetilde{A} \to X$. We take the pushforward of $\mathrm{NS}(\widetilde{A}_{\bar{k}})$ in $\mathrm{NS}(\overline{X})$:

$$\mathrm{NS}(\overline{X}) \supset \pi_* \mathrm{NS}(\widetilde{A}_{\bar{k}}) \cong \pi_* \mathrm{NS}(\overline{A}) \oplus \bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i.$$

This is a full rank sublattice. Thus the Galois representation for $\mathrm{NS}(\widetilde{A}_{\bar{k}})$ tells us the representation for $\mathrm{NS}(\overline{X})$. Hence we need to determine the lattice structure for $\mathrm{NS}(\overline{X})$. This is done in [LP80, Sec. 3]. Let us recall the description of the Néron–Severi lattice for any Kummer surface.

According to [LP80, Prop. 3.4] and [LP80, Prop. 3.5], the sublattice $\pi_* \mathrm{NS}(\widetilde{A}_{\bar{k}})$ is primitive in $\mathrm{NS}(\overline{X})$, and its intersection pairing is twice the intersection pairing of $\mathrm{NS}(\widetilde{A}_{\bar{k}})$. In particular, in our situation, we have $\pi_* \mathrm{NS}(\widetilde{A}_{\bar{k}}) \cong \langle 4\rangle$. Let K be the saturation of the sublattice generated by the $\pi_* E_i$'s. Nodal classes $\pi_* E_i$ have self intersection -2. We have the following inclusions:

$$\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i \subset K \subset K^\vee \subset \left(\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i\right)^\vee = \bigoplus_{i=1}^{16} \frac{1}{2}\mathbb{Z}\pi_* E_i$$

where $L^\vee$ denotes the dual abelian group of a given lattice L. We denote the set of 2-torsion elements of $\overline{A}$ by V. We can consider V as the 4 dimensional affine space over $\mathbb{F}_2$. Then we can interpret $\bigoplus_{i=1}^{16} \frac{1}{2}\mathbb{Z}\pi_* E_i/\mathbb{Z}\pi_* E_i$ as the space of $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued functions on V. [LP80, Prop 3.6] shows that with this identification, the image of K (resp. $K^\vee$) in $\bigoplus_{i=1}^{16} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ consists of polynomial functions $V \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of degree ≤ 1 (resp. ≤ 2.) Hence we have

$$\left[K : \bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i\right] = 2^5, \quad [K^\vee : K] = 2^6.$$

This description allows us to choose an explicit basis for K as well as to find its intersection matrix. The discriminant group of K is isomorphic to $\mathbb{F}_2^6$ whose discriminant form is given by

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This discriminant form is isometric to the discriminant form of $\pi_* H^2(A, \mathbb{Z})$ which is isomorphic to

$$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

Now we have overlattices:

$$\pi_* \operatorname{NS}(\overline{A}) \oplus K \subset \operatorname{NS}(\overline{X}).$$

To identify $\operatorname{NS}(\overline{X})$, we consider the following overlattices:

$$\pi_* \operatorname{H}^2(A, \mathbb{Z}) \oplus K \subset \operatorname{H}^2(X, \mathbb{Z}).$$

One can describe $\operatorname{H}^2(X, \mathbb{Z})$ using techniques in [Nik79, Sec 1.1-1.5]. Since the second cohomology of any $K3$ surface is unimodular, we have the following inclusions:

$$\pi_* \operatorname{H}^2(A, \mathbb{Z}) \oplus K \subset \operatorname{H}^2(X, \mathbb{Z}) = \operatorname{H}^2(X, \mathbb{Z})^\vee \subset (\pi_* \operatorname{H}^2(A, \mathbb{Z}))^\vee \oplus K^\vee$$

This gives us the following isotropic subgroup in the direct sum of the discriminant forms:

$$H = \operatorname{H}^2(X, \mathbb{Z})/\pi_* \operatorname{H}^2(A, \mathbb{Z}) \oplus K \hookrightarrow D(\pi_* \operatorname{H}^2(A, \mathbb{Z})) \oplus D(K)$$

where $D(L)$ denotes the discriminant group of a given lattice L.

Since $\pi_* \mathrm{H}^2(A,\mathbb{Z})$ and K are primitive in $\mathrm{H}^2(X,\mathbb{Z})$, each of the projections $H \to D(\pi_* \mathrm{H}^2(A,\mathbb{Z}))$ and $H \to D(K)$ is injective. Moreover, since $\mathrm{H}^2(X,\mathbb{Z})$ is unimodular, the isotropic subgroup H must be maximal inside $D(\pi_* \mathrm{H}^2(A,\mathbb{Z})) \oplus D(K)$. This implies that both injections are in fact isomorphisms. Thus we determine $\mathrm{H}^2(X,\mathbb{Z})$ as an overlattice corresponding to H in $D(\pi_* \mathrm{H}^2(A,\mathbb{Z})) \oplus D(K)$. Note that we can apply the orthogonal group $O(K)$ to H so that H is unique up to this action. Namely if we fix an identification $q_K = -q_K \cong q_{\pi_* \mathrm{H}^2(A,\mathbb{Z})}$ and $D(K) \cong D(\pi_* \mathrm{H}^2(A,\mathbb{Z}))$, then we can think of H as the diagonal in $D(K) \oplus D(\pi_* \mathrm{H}^2(A,\mathbb{Z}))$.

We succeeded in expressing our embedding $\pi_* H^2(A,\mathbb{Z}) \oplus K \hookrightarrow H^2(X,\mathbb{Z})$, hence we can express $\mathrm{NS}(\overline{X})$ as

$$\mathrm{NS}(\overline{X}) = H^2(X,\mathbb{Z}) \cap (\pi_* \mathrm{NS}(\overline{A}) \oplus K) \otimes \mathbb{Q}.$$

Note that an embedding of $\mathrm{NS}(\overline{A})$ into $H^2(A,\mathbb{Z})$ is unique up to isometries because of [Nik79, Thm 1.1.2[4]], so we can map a generator of $\mathrm{NS}(\overline{A})$ to $e+f$ where e, f is a basis for the hyperbolic plane $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we determine the lattice structure of $\mathrm{NS}(\overline{X})$.

Remark 4.3.7. In §4.5, we will in fact use a somewhat simpler argument in order to describe $\mathrm{NS}(\overline{X})$ as a Galois module. The advantage of the argument given in the current section is that it can be made applicable for higher rank cases.

4.4 Effective bounds for the transcendental part of Brauer groups

Let A be a principally polarized abelian surface defined over a number field k. Let $X = \mathrm{Kum}(A)$ be the Kummer surface associated to the abelian surface A. The goal of this section is to prove the following theorem:

Theorem 4.4.1. *There exists an effectively computable constant N_1 depending on the number field k, the Faltings height $h(A)$, and $\mathrm{NS}(\overline{A})$ satisfying*

$$\# \frac{\mathrm{Br}(X)}{\mathrm{Br}_1(X)} \le N_1.$$

[4] attributed to D.G. James

REMARK 4.4.2. In this section we focus on the proof of the method in the general case. In case that A is not geometrically simple, better bounds can be found based on recent work of Newton [New16].

First we use the following important theorem by Skorobogatov and Zarhin:

THEOREM 4.4.3. [SZ12, Prop. 1.3] *Let A be an abelian surface defined over a number field k and $X = \mathrm{Kum}(A)$ the associated Kummer surface. Then there is a natural map*

$$\mathrm{Br}(\overline{X}) \cong \mathrm{Br}(\overline{A})$$

which is an isomorphism of Galois modules.

Hence there is an injection

$$\frac{\mathrm{Br}(X)}{\mathrm{Br}_1(X)} \hookrightarrow \mathrm{Br}(\overline{X})^\Gamma = \mathrm{Br}(\overline{A})^\Gamma,$$

where $\Gamma = \mathrm{Gal}(\bar{k}/k)$. Thus, to bound $\frac{\mathrm{Br}(X)}{\mathrm{Br}_1(X)}$ in terms of k, the Faltings height $h(A)$, and $\delta = \det(\mathrm{NS}(\overline{A}))$, we only need to bound $\mathrm{Br}(\bar{A})^\Gamma$.

Also we would like to recall the following important result about the geometric Brauer groups:

THEOREM 4.4.4. *As abelian groups, we have the following isomorphisms:*

$$\mathrm{Br}(\overline{X}) \cong \mathrm{Br}(\overline{A}) \cong (\mathbb{Q}/\mathbb{Z})^{6-\rho},$$

where $\rho = \rho(\overline{A})$ is the geometric Néron–Severi rank of A.

Proof. This follows from the remark before [SZ12, Lem. 1.1]. □

We discuss several lemmas to prove our main Theorem 4.4.1. Recall that $\widetilde{M}$ is the constant from Theorem 4.2.13.

LEMMA 4.4.5. *Let $N_2 = \max\{\widetilde{M}, \delta\}$ where $\delta = \mathrm{disc}(\mathrm{NS}(\overline{A}))$. Then for any prime number $\ell > N_2$ we have*

$$\mathrm{Br}(\overline{A})^\Gamma_\ell = \{0\},$$

where $\mathrm{Br}(\overline{A})^\Gamma_\ell$ denotes the ℓ-torsion group of $\mathrm{Br}(\overline{A})^\Gamma$.

Proof. This essentially follows from results in [SZ08] combined with Theorem 4.2.13. The following exact sequence occurs as the $n = 1$ case of [SZ08, p. 486 (5)]:

$$\begin{aligned} 0 \to \big(\mathrm{NS}(\overline{A})/\ell\big)^{\Gamma} \xrightarrow{f} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_\ell)^{\Gamma} \to \mathrm{Br}(\overline{A})^{\Gamma}_{\ell} \to \\ \to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell) \xrightarrow{g} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_\ell)). \end{aligned}$$

The discussion in [SZ08, Prop. 2.5 (a)] shows that $\mathrm{NS}(\overline{A}) \otimes \mathbb{Z}_\ell$ is a direct summand of $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1))$ for any prime $\ell \nmid \delta$. For such ℓ, the homomorphism g in the above exact sequence is injective.

Next, Theorem 4.2.13 asserts that there exists an effectively computable integer $\widetilde{M} > 0$ depending on k and $h(A)$ such that for any prime $\ell > \widetilde{M}$, we have an isomorphism:

$$\mathrm{End}_k(A)/\ell \cong \mathrm{End}_\Gamma(A_\ell).$$

The discussion in [SZ08, Lem. 3.5] shows that for such ℓ, the homomorphism f is bijective. Thus our assertion follows. □

Thus, to prove our main theorem, we need to bound $\mathrm{Br}(\overline{A})^{\Gamma}(\ell)$ for each prime number ℓ where $\mathrm{Br}(\overline{A})^{\Gamma}(\ell)$ denotes the ℓ-primary subgroup of elements whose orders are powers of ℓ. To achieve this task, we employ techniques from [HKT13, §7 and 8].

We fix an embedding $k \hookrightarrow \mathbb{C}$ and consider the following lattice:

$$\mathrm{H}^2(A(\mathbb{C}), \mathbb{Z}).$$

It contains $\mathrm{NS}(\overline{A})$ as a primitive sublattice and we denote its orthogonal complement by $T_A = \langle \mathrm{NS}(\overline{A}) \rangle^{\perp}_{\mathrm{H}^2(A(\mathbb{C}),\mathbb{Z})}$ and call it the transcendental lattice of A. The direct sum $\mathrm{NS}(\overline{A}) \oplus T_A$ is a full rank sublattice of $\mathrm{H}^2(A(\mathbb{C}), \mathbb{Z})$ and we can put it into the exact sequence:

$$0 \to \mathrm{NS}(\overline{A}) \oplus T_A \to \mathrm{H}^2(A(\mathbb{C}), \mathbb{Z}) \to K \to 0,$$

where K is a finite abelian group of order $\delta = \mathrm{disc}(\mathrm{NS}(\overline{A}))$. Tensoring with $\mathbb{Z}_\ell$ and using a comparison theorem for the different cohomologies, we have

$$0 \to \mathrm{NS}(\overline{A})_\ell \oplus T_{A,\ell} \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \to K_\ell \to 0,$$

where $\mathrm{NS}(\overline{A})_\ell = \mathrm{NS}(\overline{A}) \otimes \mathbb{Z}_\ell$, $T_{A,\ell} = T_A \otimes \mathbb{Z}_\ell$, and K_ℓ is the ℓ-primary part of K. The second étale cohomology $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1))$ comes with a natural pairing which is compatible with Γ-action, and $T_{S,\ell}$ is the orthogonal complement of $\mathrm{NS}(\overline{A})_\ell$. In particular, $T_{A,\ell}$ has a natural structure as a Galois module.

LEMMA 4.4.6. *Fix a prime number ℓ. Let $N_{3,\ell} = (6-\rho)\log_\ell \widetilde{M}$. Then for each integer $n \geq 1$ the bound*

$$\#(T_A/\ell^n)^\Gamma \leq \ell^{N_{3,\ell}}$$

is satisfied.

Proof. Since A is principally polarized, we have a natural isomorphism of Galois modules:

$$\mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \cong (\mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)))^* \cong T_\ell(A),$$

where $T_\ell(A)$ is the Tate module of A. Hence we have

$$\begin{aligned} T_{A,\ell} \hookrightarrow \mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) &= \textstyle\bigwedge^2 \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \\ &\hookrightarrow \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \otimes \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \cong \mathrm{End}(T_\ell(A)). \end{aligned}$$

Thus we have

$$(T_A/\ell^n) = (T_{A,\ell}/\ell^n) \hookrightarrow \mathrm{End}(T_\ell(A))/\ell^n = \mathrm{End}(\overline{A}[\ell^n]).$$

Hence we obtain a homomorphism

$$\Phi : (T_A/\ell^n)^\Gamma \hookrightarrow \mathrm{End}_\Gamma(\overline{A}[\ell^n]) \to \mathrm{End}_\Gamma(\overline{A}[\ell^n])/\mathrm{End}(A).$$

This composite homomorphism Φ must be injective because T_A is the transcendental lattice which does not meet the algebraic part $\mathrm{End}(A)$. The order of this quotient is bounded by Theorem 4.2.13. □

Taking a finite extension of k only increases the size of $\mathrm{Br}(\overline{A})^{\mathrm{Gal}(\bar{k}/k')}$, so from now on we assume that the Galois action on the Néron–Severi space $\mathrm{NS}(\overline{A})$ is trivial. This is automatically true when the geometric Néron–Severi rank of A is 1.

LEMMA 4.4.7. *Suppose that the Galois action on* $\mathrm{NS}(\overline{A})$ *is trivial. Write*

$$N_{4,\ell} = (2v_\ell(\delta) + 10\log_\ell \widetilde{M})(6-\rho)$$

where v_ℓ is the valuation at ℓ. Then for each prime ℓ, we have

$$\#\,\mathrm{Br}(\overline{A})^\Gamma(\ell) \leq \ell^{N_{4,\ell}}.$$

Proof. Recall the exact sequence of [SZ08, p. 486 (5)]:

$$0 \to \left(\mathrm{NS}(\overline{A})/\ell^n\right)^\Gamma \xrightarrow{f_n} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma \to \mathrm{Br}(\overline{A})^\Gamma_{\ell^n} \to$$
$$\to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \xrightarrow{g_n} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})),$$

so we need to bound the cokernel of f_n and the kernel of g_n independent of n. By Theorem 4.4.4, it is enough to bound the orders of elements in $\mathrm{coker}(f_n)$ as well as $\ker(g_n)$ independently of n.

Let ℓ^m be the order of K_ℓ and we assume that $n \geq m$. We have the following exact sequence:

$$0 \to \mathrm{NS}(\overline{A})_\ell \oplus T_{A,\ell} \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \to K_\ell \to 0.$$

Tensoring by $\mathbb{Z}/\ell^n\mathbb{Z}$ (as $\mathbb{Z}_\ell$-modules) and using Tor functors, we obtain a four term exact sequence:

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus T_A/\ell^n \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \to K_\ell \to 0, \qquad (4.4.1)$$

where we've used that the middle term $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1))$ is a free (and hence flat) $\mathbb{Z}_\ell$-module.

Note that the projection

$$K_\ell \to \mathrm{NS}(\overline{A})/\ell^n$$

is injective because $T_A/\ell^n \to \mathrm{H}^2(\overline{A}, \mu_{\ell^n})$ is injective. In particular, the Galois action on K_ℓ is trivial. We split the exact sequence (4.4.1) as

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus T_A/\ell^n \to D \to 0,$$

and

$$0 \to D \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \to K_\ell \to 0.$$

These gives us the long exact sequences

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus (T_A/\ell^n)^\Gamma \to D^\Gamma \to$$
$$\to \mathrm{Hom}(\Gamma, K_\ell) \to \mathrm{Hom}(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \oplus \mathrm{H}^1(\Gamma, T_A/\ell^n),$$

and

$$0 \to D^\Gamma \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma \to K_\ell \to \mathrm{H}^1(\Gamma, D) \to \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})).$$

The map $\mathrm{Hom}(\Gamma, K_\ell) \to \mathrm{Hom}(\Gamma, \mathrm{NS}(\overline{A})/\ell^n)$ is injective, so the sequence

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus (T_A/\ell^n)^\Gamma \to D^\Gamma \to 0,$$

is exact. We conclude that

$$\#\operatorname{coker}(f_n) = \frac{\#\,\mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma}{\#\,\mathrm{NS}(\overline{A})/\ell^n} \le \frac{\#K_\ell \cdot \#D^\Gamma}{\#\,\mathrm{NS}(\overline{A})/\ell^n} = \#(T_A/\ell^n)^\Gamma$$

is bounded independent of n by application of Lemma 4.4.6.

Next we discuss a uniform bound on the maximum order of elements in $\ker(g_n)$. The homomorphism g_n is a composition of two homomorphisms:

$$\mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \to \mathrm{H}^1(\Gamma, D) \to \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})).$$

The kernel of $\mathrm{H}^1(\Gamma, D) \to \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}))$ is bounded by K_ℓ. We have the exact sequence

$$0 \to \mathrm{NS}(\overline{A})/\ell^n \to D \to D/\mathrm{NS}(\overline{A}) \to 0,$$

which gives the long exact sequence

$$0 \to \mathrm{NS}(\overline{A})/\ell^n \to D^\Gamma \to (D/\mathrm{NS}(\overline{A}))^\Gamma \to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \to \mathrm{H}^1(\Gamma, D).$$

Thus to finish the proof we need to find an uniform bound for the maximum order of elements in $(D/\mathrm{NS}(\overline{A}))^\Gamma$. To obtain this, we look at the exact sequence

$$0 \to K_\ell \to T_A/\ell^n \to D/\mathrm{NS}(\overline{A}) \to 0.$$

This gives us the long exact sequence

$$0 \to K_\ell \to (T_A/\ell^n)^\Gamma \to (D/\mathrm{NS}(\overline{A}))^\Gamma \to \mathrm{Hom}(\Gamma, K_\ell).$$

Note that the group $\mathrm{Hom}(\Gamma, K_\ell)$ is killed by $\#K_\ell$. Finally, $\#(T_A/\ell^n)^\Gamma$ is uniformly bounded by the result of Lemma 4.4.6. Therefore the maximum order of elements in $(D/\mathrm{NS}(\overline{A}))^\Gamma$ is uniformly bounded and our assertion follows. □

Proof of Theorem 4.4.1. It follows from Lemma 4.4.5 and 4.4.7 that we can take N_1 as

$$\delta^{10} \prod_{\ell \le N_2} \widetilde{M}^{50}.$$

□

4.5 Computations on rank 17

In this section we discuss some computations in order to determine the group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ through $\mathrm{H}^1(k, \mathrm{NS}(\overline{X}))$ using MAGMA, where the geometric Néron–Severi rank of X is 17.[5] Recall that the Néron–Severi lattice of a Kummer surface is determined by the sixteen 2-torsion points on the associated abelian surface and its Néron–Severi lattice. A principally polarized abelian surface is the Jacobian of a genus 2 curve C and its 2-torsion points correspond to the classes $p_i - p_j$ of differences of the six ramification points of $C \to \mathbb{P}^1$.

First we need to fix some ordering. Let $\{p_1, \ldots, p_6\}$ be the ramification points of C. Then on $\mathrm{Jac}(C)[2] = \{0, p_i - p_j : i < j\}$ the following additive rule holds

$$p_i - p_j = p_k - p_l + p_n - p_m$$

where $\{i, j\}$ and $\{k, l, m, n\}$ are two complementary subsets of $\{1, \ldots, 6\}$.

LEMMA 4.5.1. *The set*

$$\{p_1 - p_2 =: v_1, p_1 - p_3 =: v_2, p_1 - p_4 =: v_3, p_1 - p_5 =: v_4\}$$

forms a basis of $\mathrm{Jac}(C)[2] \cong \mathbb{F}_2^4$.

Proof. In order to write 0 as a linear combination of these elements (over $\mathbb{F}_2$), we need to use an even number. Since any two of these are different, this may only be done using all four of them. However, the sum of these four elements is $p_2 - p_3 + p_4 - p_5 = p_1 - p_6 \neq 0$. □

We order the 2-torsion elements in terms of $p_i - p_j$ and in terms of v_i in Table 4.1.

The Galois action is defined by a subgroup of S_6, acting on the six ramification points p_i and hence on the set of e_i. This action defines S_6 as a subgroup of S_{16}. We know that S_6 is generated by the two elements $(1, 2)$ and $(1, 2, 3, 4, 5, 6)$, so to determine the map $S_6 \to S_{16}$ we need only specify the images of $(1, 2)$ and $(1, 2, 3, 4, 5, 6)$.

[5] In the published paper there is a typo: this rank is said to be assumed to be 1 instead. In the case we are considering, this does hold for the associated abelian surface.

Lemma 4.5.2. *Let $\rho\colon S_6 \to S_{16}$ be the map that represents the action of S_6 on the sixteen 2-torsion points e_i. Then*

$$\rho((1,2)) = (3,4)(5,6)(9,10)(15,16)$$

and

$$\rho((1,2,3,4,5,6)) = (2,4,7,13,8,16)(3,6,11,12,9,15)(5,10,14)$$

hold.

Proof. Direct computation on the elements in Table 4.1, e.g. $\rho((1,2))$ maps $e_3 = p_1 - p_3$ to $p_2 - p_3 = e_4$. □

$e_1 = 0$	$e_9 = p_1 - p_5 = v_4$
$e_2 = p_1 - p_2 = v_1$	$e_{10} = p_2 - p_5 = v_1 + v_4$
$e_3 = p_1 - p_3 = v_2$	$e_{11} = p_3 - p_5 = v_2 + v_4$
$e_4 = p_2 - p_3 = v_1 + v_2$	$e_{12} = p_4 - p_6 = v_1 + v_2 + v_4$
$e_5 = p_1 - p_4 = v_3$	$e_{13} = p_4 - p_5 = v_3 + v_4$
$e_6 = p_2 - p_4 = v_1 + v_3$	$e_{14} = p_3 - p_6 = v_1 + v_3 + v_4$
$e_7 = p_3 - p_4 = v_2 + v_3$	$e_{15} = p_2 - p_6 = v_2 + v_2 + v_4$
$e_8 = p_5 - p_6 = v_1 + v_2 + v_3$	$e_{16} = p_1 - p_6 = v_1 + v_2 + v_3 + v_4$

Table 4.1: Chosen ordering of 2-torsion elements in both descriptions.

Using the description from [LP80, Prop. 3.4 and 3.5] as explained in §4.3.2, the lattice K is generated by $\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i$ together with lifts from polynomials in four variables with values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of degree at most 1. These are generated as an abelian group by $x_1, x_2, x_3, x_4, 1$, where the set of x_i's is dual to the set of v_j's in the sense $x_i(v_j) = \delta_{ij}$. We identify the set of exceptional curves with the set of 2-torsion points in the natural way by identifying E_i and e_i for each $i = 1, \dots, 16$.

From a theoretical perspective, one could use the approach as laid out in §4.3.2 in order to calculate $\mathrm{NS}(X)$, but for the case $\operatorname{rk} \mathrm{NS}(\overline{A}) = 1$, it turns out that there is an easier approach which involves knowing the index of $\pi_* \mathrm{NS}(A) \oplus K$ in $\mathrm{NS}(X)$.

Lemma 4.5.3. *Let A be an abelian surface of Néron–Severi rank ρ, write $X = \mathrm{Kum}(A)$ and let K be the saturation of $\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i$ inside $\mathrm{NS}(X)$. Then the index of $\pi_* \mathrm{NS}(A) \oplus K$ inside $\mathrm{NS}(X)$ is 2^ρ.*

Proof. Write $t = |\operatorname{disc} \mathrm{NS}(A)|$, then also $t = |\operatorname{disc} T(A)|$ holds, where $T(A)$ is the transcendental lattice of A, since $\mathrm{H}^2(A, \mathbb{Z})$ is unimodular. We have equality of ranks

$$\operatorname{rk} T(X) = \operatorname{rk} T(A) = 6 - \rho,$$

and hence $|\operatorname{disc} T(X)| = t \cdot 2^{6-\rho}$ from which follows $|\operatorname{disc} \mathrm{NS}(X)| = t \cdot 2^{6-\rho}$ since $\mathrm{H}^2(X, \mathbb{Z})$ is unimodular.

Let $L = \pi_* \mathrm{NS}(A)$. Then $\operatorname{rk} L = \rho$ and $|\operatorname{disc} L| = 2^\rho t$ hold.

We use the chain of inclusions

$$L \oplus K \subset \mathrm{NS}(X) \subset \mathrm{NS}(X)^\vee \subset L^\vee \oplus K^\vee$$

The index of $L \oplus K \subset L^\vee \oplus K^\vee$ is $2^\rho t \cdot 2^6$ (see §4.3.2 for the discriminant of K) and combining with the discriminants above, we find the statement of the lemma. □

From now on, assume $\rho = 1$, i.e. the geometric Néron–Severi rank of X is 17. Let l be the push-forward of the theta-divisor on A. Then $l^2 = 4$ and by Lemma 4.5.3, the index of $\Lambda := \langle l \rangle \oplus K$ in $\mathrm{NS}(\overline{X})$ is 2. It therefore suffices to find a single element $D \in \mathrm{NS}(\overline{X})$ such that $2D$ is an element of Λ but D itself is not. Then Λ and D together span $\mathrm{NS}(\overline{X})$.

LEMMA 4.5.4. *Up to isomorphism there is only one index 2 even overlattice of* Λ.

Proof. Even overlattices of index 2 correspond to isotropic subgroups of the discriminant group $D(\Lambda) = D(\pi_* \mathrm{NS}(\overline{A})) \oplus D(K)$ of order 2. Since K is saturated, a generating element of such a subgroup projects to an element of $D(\pi_* \mathrm{NS}(\overline{A}))$ which has order exactly 2. Since $D(\pi_* \mathrm{NS}(\overline{A}))$ is isomorphic to $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$, there is only one such element, which has square $1 \pmod 2$. We therefore need to consider order 2 elements of square $1 \pmod 2$ in $D(K)$. Since we remember the intersection form on $D(K)$ from section 4.3.2, we easily see that there are four such elements, with coordinates $(1,0,0,0,0,1)$, $(0,1,0,0,1,0)$, $(0,0,1,1,0,0)$ and $(1,1,1,1,1,1)$. By calculating the centralizer of the intersection matrix of $D(K)$ inside $\mathrm{GL}_6(\mathbb{F}_2)$, that is $\mathcal{O}(D(K))$, it is easily found that each of these lie in the same orbit under the action of $\mathcal{O}(D(K))$. □

It is worthwhile to remark that the Galois action on the 2-torsion points of A induces an action on $D(K)$ and only one of the four elements in the previous proof is invariant under the action of the full symmetric group S_6, which in our chosen basis is $(1,1,1,1,1,1)$.

LEMMA 4.5.5. *The element*

$$D = \frac{1}{2}(\pi_* E_1 + \pi_* E_8 + \pi_* E_{12} + \pi_* E_{14} + \pi_* E_{15} + \pi_* E_{16} + l)$$

together with Λ *spans* $\mathrm{NS}(\overline{X})$.

Proof. We already know that the coefficient of l is non-zero since K is saturated in $\mathrm{NS}(\overline{X})$, and by adding a suitable element of 2Λ to D, we can write $D = \frac{1}{2}l + \frac{1}{2}\sum_{i=1}^{16} a_i \pi_* E_i$, where for each i we take $a_i \in \{0, \frac{1}{2}, 1, \frac{3}{2}\}$.

By intersecting D with any of the $\pi_* E_i$, we find $a_i \in \{0,1\}$ since the intersection needs to be integral. From $D^2 \in 2\mathbb{Z}$ we deduce the congruence $\sum_{i=1}^{16} a_i \equiv 2 \pmod 4$. Furthermore, the projection of D to $D(K)$ needs to be one of the four elements from the proof of Lemma 4.5.4. In order to ensure that the lattice we generate is a Galois module for any subgroup of S_6, the element D from the statement is chosen so that it projects to the unique S_6-invariant one. □

Now that we have computed $\mathrm{NS}(\overline{X})$, we can have MAGMA take Galois cohomology by applying the action from Lemma 4.5.2 and we find

$$\mathrm{H}^1(k, \mathrm{NS}(\overline{X})) = 1.$$

We can furthermore consider the case where the Galois group is not the full S_6. The MAGMA computations also yield the following:

PROPOSITION 4.5.6. *Up to conjugation there are only three subgroups* H *of* S_6 *for which* $\mathrm{H}^1(H, \mathrm{NS}(\overline{X}))$ *is non-trivial: one of order 4 (isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*), one of order 12 (isomorphic to* A_4*) and one of order 60 (isomorphic to* A_5*). In each of these cases we find* $\mathrm{H}^1(H, \mathrm{NS}(\overline{X})) \cong \mathbb{Z}/2\mathbb{Z}$.

4.6 An example

In this section we compute a concrete bound as stated in Theorem 4.2.13. Let us consider the genus 2 curve defined over $\mathbb{Q}$ by:

$$C : y^2 = x^6 + x^3 + x + 1.$$

Let A denote the Jacobian of C. Thanks to the algorithm provided by Elsenhans and Jahnel in [EJ12a] we compute the Néron–Severi rank of A and we obtain that its geometric Néron–Severi rank is 1. By Theorem 4.3.2 we know $\mathrm{End}(A) = \mathbb{Z}$.

Since $x^6 + x^3 + x + 1 = (x + 1)(x^2 + 1)(x^3 - x^2 + 1)$, the splitting field F of $x^6 + x^3 + x + 1$ is the composite field of $\mathbb{Q}(\sqrt{-1})$ and the splitting field F_1 of $x^3 - x^2 + 1$. The Galois group $\mathrm{Gal}(F/\mathbb{Q})$ has 12 elements and two normal subgroups: $\mathbb{Z}/2\mathbb{Z}$ and S_3. By Proposition 4.5.6, the only exceptional subgroup with 12 elements is A_4. Since the only nontrivial normal subgroup of A_4 has 4 elements, $\mathrm{Gal}(F/\mathbb{Q})$ cannot be one of the exceptional subgroups of S_6. Therefore the algebraic Brauer group is trivial.

To compute the bound of Theorem 4.2.13 we need to compute the Faltings height of the abelian surface A. By Proposition 4.2.1, $h(A)$ is bounded above by

$$\begin{aligned} -\log(2\pi^2) + \tfrac{1}{10}\log\left(2^{-12}\,\mathrm{Disc}_6\left(4(x^6 + x^3 + x + 1)\right)\right) \\ - \log\left(2^{-1/5}|J_{10}|^{1/10}\det(\Im\tau)^{1/2}\right), \end{aligned}$$

with $2^{-12}\,\mathrm{Disc}_6\left(4(x^6 + x^3 + x + 1)\right) = 2^{12}\cdot 25\cdot 23$, $|J_{10}| = 0.001921635$ and

$$\tau = \begin{pmatrix} -1.49097 + 1.64505i & -0.50000 + 0.98058i \\ -0.50000 + 0.98058i & -1.50903 + 1.64505i \end{pmatrix}.$$

Hence $h(A) \leq -0.79581$. In our situation we have $k = \mathbb{Q}$, so we can bound M by plugging these into

$$\begin{aligned} M \leq 2^{4664} c_1^{16} c_2(k)^{256}\Big(2h(A) + \tfrac{8}{17}\log[k:\mathbb{Q}] + 8\log c_1 \\ + 128\log c_2(k) + 1503\Big)^{512} \end{aligned}$$

with $c_1 = 4^{11}\cdot 9^{12}$ and $c_2(k) = 7.5\cdot 10^{47}[k:\mathbb{Q}]$.

Using MAGMA we get

$$M \leq \widetilde{M} = 8.7\times 10^{16100}.$$

Let $X = \mathrm{Kum}(A)$. We may apply Theorem 4.4.1 directly to obtain an explicit bound. However, since the curve C is defined over $\mathbb{Q}$, we will combine our bound in Lemma 4.4.7 with the results of Dieulefait and Skorobogatov–Zarhin to obtain a sharper bound as pointed out by one of the referees.

PROPOSITION 4.6.1 (Dieulefait[6].). *For* $\ell \geq 3$*, the image of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *in* $\mathrm{Aut}(A[\ell])$ *is* $\mathrm{GSp}_4(\mathbb{F}_\ell)$*.*

Proof. Note that C is isomorphic to the curve defined by $y^2 = x^6 - x^3 - x + 1$ and hence by [Die02, Thm. 4.2], the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell \neq 2, 3, 5, 23$. By [BLR90, Ex.9.2.8][7], one finds that [Die02 Prop 5.4] applies. The order of the component group of the Néron-model is $\mathrm{ord}_p(n)$ where n is the resultant of $f(x)$ and $f'(x)$. For $p = 5$ (resp. $p = 23$) this order is 2 (resp. 1). Now we apply [Die02, Thm. 5.4] and we use MAGMA to compute characteristic polynomials of Frobenii for hyperelliptic curves over $\mathbb{Q}$. We first take $p = 5$ and $q = 11$ (resp. $q = 19$). Since the characteristic polynomial of $Frob_q$ is irreducible modulo 3 (resp. 23), we conclude that the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell = 3, 23$. We then take $p = 23$ and $q = 29$ to conclude that the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell = 5$. □

PROPOSITION 4.6.2 (Skorobogatov–Zarhin). *For* $\ell \geq 3$*, we have*

$$\mathrm{Br}(\overline{A})^\Gamma(\ell) = 0.$$

Proof. It suffices to show that the assumptions of [Sko17, Prop. 4.2] are satisfied when image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$. This follows from $\mathrm{PSp}_4(\mathbb{F}_\ell)$ being a simple non-abelian group of order $> \ell$ as in the argument in Example 1 in *loc. cit.*. □

COROLLARY 4.6.3. *For the Kummer surface* $X = \mathrm{Kum}(\mathrm{Jac}(C))$ *with* C *defined by* $y^2 = x^6 + x^3 + x + 1$*, we have*

$$|\operatorname{Br}(X)/\operatorname{Br}_0(X)| < 2^{10} \cdot 10^{805050}.$$

Proof. By Propositions 4.6.1 and 4.6.2, we have $|\operatorname{Br}(\overline{X})^\Gamma| = |\operatorname{Br}(\overline{A})^\Gamma(2)|$. By Lemma 4.4.7, we have

$$|\operatorname{Br}(\overline{A})^\Gamma(2)| < \prod \ell^{10 v_\ell(\delta)} \cdot (8.7 \times 10^{16100})^{50} < 2^{10} \cdot 10^{805050}.$$

Since $\operatorname{Br}_1(X)/\operatorname{Br}_0(X) = 0$, we conclude that

$$|\operatorname{Br}(X)/\operatorname{Br}_0(X)| \leq |\operatorname{Br}(\overline{X})^\Gamma| < 2^{10} \cdot 10^{805050}.$$

□

[6]The results in [Die02] are stated as conditional upon Serre's modularity conjecture, which is now proved by Khare and Wintenberger [KW09a, KW09b]

[7]Alternatively one may use the SAGE function *genus2reduction*.

Remark 4.6.4. The above algorithm works for any genus 2 (hyperelliptic) curve over $\mathbb{Q}$. More precisely, we may use Dieulefait's algorithm in [Die02] to find a finite set S such that for any $\ell \notin S$, the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(\mathrm{Jac}(C)[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and hence by [Sko17, Prop. 4.2], we conclude that $\mathrm{Br}(\overline{A})^\Gamma(\ell) = 0$ for $\ell \notin S$. Then by Lemma 4.4.7, we have

$$|\,\mathrm{Br}(X)/\,\mathrm{Br}_1(X)| < \delta^{2(6-\rho)} \cdot \widetilde{M}^{10(6-\rho)|S|}.$$