Algebra & Number Theory

Volume 7
2013
No. 6

msp

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1281

On the discrete logarithm problem in elliptic curves II

Claus Diem

We continue our study on the elliptic curve discrete logarithm problem over finite extension fields. We show, among others, the following results:

For sequences of prime powers $(q_i)_{i\in\mathbb{N}}$ and natural numbers $(n_i)_{i\in\mathbb{N}}$ with $n_i \to \infty$ and $n_i/\log(q_i)^2 \to 0$ for $i \to \infty$, the discrete logarithm problem in the groups of rational points of elliptic curves over the fields $\mathbb{F}_{q_i^{n_i}}$ can be solved in subexponential expected time $(q_i^{n_i})^{o(1)}$.

Let $a, b > 0$ be fixed. Then the problem over fields $\mathbb{F}_{q^n}$, where q is a prime power and n a natural number with $a \cdot \log(q)^{1/3} \leq n \leq b \cdot \log(q)$, can be solved in an expected time of $e^{\mathcal{O}(\log(q^n)^{3/4})}$.

1. Introduction

In our previous work [Diem 2011b] we have shown that there exist sequences of finite fields over which the elliptic curve discrete logarithm problem can be solved in subexponential expected time in the bit-length of the input.

In this work, we strengthen those results. We show that for larger classes of ground fields the problem can still be solved in subexponential expected time.

Recall that the main result from [Diem 2011b] is as follows.

Theorem 1. *The discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ can be solved in an expected time of*

$$e^{\mathcal{O}(\max(\log(q), n^2))}.$$

Here and in the following, q is always a prime power and n a natural number.

It follows from this theorem that, for any two sequences $(q_i)_{i\in\mathbb{N}}$ and $(n_i)_{i\in\mathbb{N}}$ of prime powers and natural numbers with $n_i \to \infty$ and $n_i/\log(q_i) \to 0$ for $i \to \infty$, the discrete logarithm problem in the groups of rational points of elliptic curves over the fields $\mathbb{F}_{q_i^{n_i}}$ can be solved in an expected time of $(q_i^{n_i})^{o(1)}$.

The main result of this work is the following stronger theorem.

MSC2010: primary 11Y16; secondary 14H52, 11G20.
Keywords: elliptic curves, discrete logarithm problem.

Theorem 2. *The discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ can be solved in an expected time of*

$$e^{\mathcal{O}(\max(\log(q), n\cdot\log(q)^{1/2}, n^{3/2}))}.$$

Note here that

$$\max(\log(q), n\cdot(\log(q))^{1/2}, n^{3/2}) = \begin{cases} \log(q) & \text{for } n \le \log(q)^{1/2}, \\ n\cdot(\log(q))^{1/2} & \text{for } \log(q)^{1/2} \le n \le \log(q), \\ n^{3/2} & \text{for } \log(q) \le n. \end{cases}$$

Theorem 2 gives the following results.

(i) Let sequences of prime powers $(q_i)_{i\in\mathbb{N}}$ and natural numbers $(n_i)_{i\in\mathbb{N}}$ with $q_i \to \infty$ and $n_i/\log(q_i)^2 \to 0$ for $i \to \infty$ be given. Then the discrete logarithm problem in the groups of rational points of elliptic curves over the fields $\mathbb{F}_{q_i^{n_i}}$ can be solved in an expected time of

$$(q_i^{n_i})^{o(1)}.$$

(ii) Let $\beta \in [\frac{1}{2}, 1]$ and $a, b > 0$ be fixed. Let

$$\alpha := \frac{1}{2\beta+1} \quad \text{and} \quad \gamma := 1 - \frac{1}{2}\cdot\frac{1}{\beta+1} = \frac{\beta+\frac{1}{2}}{\beta+1}.$$

Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ with

$$a\cdot\log(q)^{\alpha} \le n \le b\cdot\log(q)^{\beta} \tag{1}$$

can be solved in an expected time of

$$e^{\mathcal{O}((\log(q^n))^{\gamma})}.$$

Note that $\alpha \le \frac{1}{2}$ (with equality if $\beta = \frac{1}{2}$), and γ is maximal if $\alpha = \beta = \frac{1}{2}$, and then it is equal to $\frac{2}{3}$.

As a special case we obtain that for $a, b > 0$ the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ with

$$a\cdot\log(q)^{1/3} \le n \le b\cdot\log(q)$$

can be solved in an expected time of $e^{\mathcal{O}((\log(q^n))^{3/4})}$.

(iii) Let $\beta \in [1, 2)$ and $a, b > 0$ be fixed. Let

$$\alpha := \frac{2-\beta}{3\beta} \quad \text{and} \quad \gamma := \frac{3}{2}\cdot\frac{\beta}{1+\beta}.$$

Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{q^n}$ with

$$a \cdot \log(q)^{\alpha} \leq n \leq b \cdot \log(q)^{\beta}$$

can be solved in an expected time of

$$e^{\mathbb{O}(\log(q^n)^{\gamma})}.$$

The first statement follows immediately from Theorem 2.

The derivation of the second statement from Theorem 2 is as follows:
We have $\beta = (\gamma - \frac{1}{2})/(1-\gamma)$ and $\alpha = 1/\gamma - 1$.
The first inequality in (1) is equivalent to $n \geq a \cdot \log(q)^{1/\gamma - 1}$, and this is equivalent to $(1/a^{\gamma}) \cdot (n \log(q))^{\gamma} \geq \log(q)$.
The second inequality is equivalent to $b^{1-\gamma} \cdot \log(q)^{\gamma - 1/2} \geq n^{1-\gamma}$, and this is equivalent to $b^{1-\gamma} \cdot (n \log(q))^{\gamma} \geq n \cdot \log(q)^{1/2}$.
Additionally, except if $q = 2$, we have $\log(q) \geq \log(q)^{\beta} \geq (1/b) \cdot n$ and thus $n \cdot \log(q)^{1/2} \geq (1/b) \cdot n^{3/2}$.
The results now follow with Theorem 2.

We now show how the third statement follows from Theorem 2. We have $\beta = 2\gamma/(3-2\gamma)$ and — as above — $\alpha = 1/\gamma - 1$.
For the range $a \cdot \log(q)^{\alpha} \leq n \leq \log(q)$, the result follows from the second point, so we consider the range $\log(q) \leq n \leq b \cdot \log(q)^{\beta}$. We have $n \leq b \cdot \log(q)^{2\gamma/(3-2\gamma)}$; that is, $n^{3/2-\gamma} \leq b^{3/2-\gamma} \cdot \log(q)^{\gamma}$. With other words: $n^{3/2} \leq b^{3/2-\gamma} \cdot (n \cdot \log(q))^{\gamma}$.

As an application of Theorem 2 we now consider the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields of a fixed characteristic p. We first remark that Theorem 2 does not give a nontrivial result if q is set to p and n is set to the absolute extension degree of the ground field. We therefore consider a factorization of the absolute extension degree in the form mn; that is, we write the cardinality of the ground field in the form p^{mn}. We can then regard both m and n as the extension degree. One sees that it is advantageous to regard n as the extension degree provided that $n \leq m$ and m as the extension degree otherwise. In this way one obtains:

Theorem 3. *Let p be a fixed prime number. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{p^{mn}}$ can be solved in an expected time of*

$$e^{\mathbb{O}(\max(m,n,\min(m \cdot n^{1/2}, n \cdot m^{1/2})))}.$$

Here we have

$$\max(m, n, \min(m \cdot n^{1/2}, n \cdot m^{1/2})) = \begin{cases} m & \text{for } n \le m^{1/2}, \\ n \cdot m^{1/2} & \text{for } m^{1/2} \le n \le m, \\ m \cdot n^{1/2} & \text{for } n^{1/2} \le m \le n, \\ n & \text{for } m \le n^{1/2}. \end{cases}$$

For any fixed prime number p, Theorem 3 gives the following results:

(iv) Let $(m_i)_{i\in\mathbb{N}}$ and $(n_i)_{i\in\mathbb{N}}$ with $m_i, n_i \to \infty$ for $i \to \infty$. Then the discrete logarithm problem in the groups of rational points of elliptic curves over the finite fields $\mathbb{F}_{p^{m_i n_i}}$ can be solved in an expected time of

$$(p^{m_i n_i})^{o(1)}.$$

(v) Let $\alpha \ge 3$ and $a, b > 0$. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{p^{mn}}$ with

$$m \le a \cdot n^{\alpha} \quad \text{and} \quad n \le b \cdot m^{\alpha}$$

can be solved in an expected time of

$$e^{\mathcal{O}((\log(p^{mn})^{1-1/(1+\alpha)})}.$$

Just as statement (i) above, statement (iv) is again immediate.

So we consider the last statement. Let $\alpha \ge 3$. Note first that $1 - \frac{1}{1+\alpha} = \frac{\alpha}{1+\alpha} = \frac{1}{1+1/\alpha}$. We have $m^{1+1/\alpha} \le a^{1/\alpha} \cdot mn$, so $m \le a^{1/(1+\alpha)} \cdot (mn)^{\alpha/(1+\alpha)}$. Similarly, $n \le a^{1/(1+\alpha)} \cdot (mn)^{\alpha/(1+\alpha)}$. Moreover, $1 - \frac{1}{1+\alpha} \ge \frac{3}{4}$. Thus, if $n \le m$, then $n \cdot m^{1/2} \le (mn)^{3/4} \le (mn)^{\alpha/(1+\alpha)}$. Analogously, if $m \le n$, then $m \cdot n^{1/2} \le (mn)^{\alpha/(1+\alpha)}$.

Some more information on the results. We give here some more information on the precise meaning of the statements above and similar statements throughout this article.

First, we choose some concrete representation of the "abstract input instances" (elliptic curves E over finite fields K and elements $a, b \in E(K)$ with $a \in \langle b \rangle$) by bit-strings. Every "abstract instance" is then given by at least one and finitely many bit-strings. Concretely, we represent elliptic curves by Weierstraß equations, as usual. We also choose some (uniform) randomized model of computation with an appropriate complexity measure, for example, a usual randomized RAM model with logarithmic cost function or a randomized Turing model.

For a function f from some infinite countable set S to $\mathbb{R}_{>0}$, we define the sets $\mathcal{O}(f)$, $\tilde{\mathcal{O}}$, $o(f)$ and $\mathcal{P}oly(f)$ as usual (for the latter see also [Diem 2011b]). We note here that it makes no difference if S is a subset of $\mathbb{N}$ or not.

The assertion in Theorem 1 is then as follows: there exists a machine in the given model and a constant $C > 0$ such that, if the machine is applied to an instance of

the elliptic curve discrete logarithm problem over a field $\mathbb{F}_{q^n}$, the expected running time is bounded by $e^{C\cdot\max(\log(q),n^2)}$. The assertions in Theorem 2 and Theorem 3 are analogous. We stress that the expected value concerns only the internal choices of the computation; there is no averaging over input classes.

Statement (i) means the following: Let $(q_i)_{i\in\mathbb{N}}$ and $(n_i)_{i\in\mathbb{N}}$ be given as indicated. Then there exists a randomized machine and a sequence $(\epsilon_i)_{i\in\mathbb{N}}$ with $\epsilon_i \to 0$ for $i\to\infty$ such that the expected running time of the machine if applied to an instance over $\mathbb{F}_{q_i^{n_i}}$ is bounded by $(q_i^{n_i})^{\epsilon_i}$. Statement (iv) is again analogous.

As usual, throughout this article we use the word "algorithm" instead of "machine". Also as usual, we use the word "algorithm" in an informal way when we outline a computation.

Outline. Just as the algorithm in [Diem 2011b], the algorithm for Theorem 2 is based on the usual index calculus or relation generation and linear method. Again we use multivariate polynomial systems over $\mathbb{F}_q$ to obtain relations. The main conceptual difference between the new algorithm and the previous algorithm is that we enlarge the factor base. This enlargement causes some difficulties in the analysis of the algorithm, and in order to complete the analysis we further modify the definition of the factor base. We also employ a new algorithm to find decompositions. Otherwise the index calculus algorithm in [ibid.] is not changed.

Below we outline a preliminary algorithm, and, on the basis of this algorithm, we discuss under various heuristic assumptions why one should be able to obtain an expected running time of $e^{\mathcal{O}(\max(\log(q),\, n\cdot\log(q)^{1/2}))}$. In the course of this work, we will change the algorithm in various ways. Unfortunately, even with a modified algorithm we cannot prove that one can obtain the expected running time one might expect by heuristic considerations. Indeed, in odd characteristic we can only complete the analysis under the condition that $c^n \le q$ for a suitable constant $c>0$. In even characteristic the situation is more fortunate and we can complete the analysis if $n^c \le q$ for a suitable constant $c>0$. This does however not lead to an improvement over the result in Theorem 3 applied to fields of even characteristic.

The index calculus algorithm we employ has the same overall structure as the one in [ibid.] (see Subsection 2.3 of that work). The changes we perform concern the definition of the factor base (Steps 4 and 5 of that algorithm) and the relation generation (Step 6), where a new decomposition algorithm is employed. Because the overall structure of the algorithm stays the same, we will focus on the parts of the index algorithm which need to be changed.

In the next section, we give the new algorithm for the constructions leading to the definition of the factor base. In Section 3 we formulate a decomposition problem adapted to the new situation and give an algorithm to solve the problem.

In the fourth and last section, we prove that under suitable conditions on n and q the probability that a uniformly randomly distributed point $P \in E(\mathbb{F}_{q^n})$ leads to a relation between P and factor base elements is large enough. In the last part of this section, we indicate how Theorem 2 can be obtained. Additionally, in an appendix we correct two misprints in our previous work [ibid.].

Throughout the article we use the same notation as in our previous work, with the exception that we now denote an affine defining polynomial for the elliptic curve by $f(x, y)$.

The application of the scalar restriction functor, that is, the formation of Weil restrictions, is crucial in this work. Furthermore, many arguments here are based on the consideration of tangent spaces. Background information on these topics is given at the end of this section. The reader should also be familiar with the first two sections of [ibid.]. Additionally, we assume some familiarity with toric geometry and its application to solving polynomial systems as given in [Fulton 1993], [Cox et al. 2005] and in particular in [Rojas 1999].

A preliminary algorithm. The algorithm follows the usual "index calculus" strategy: after some preliminary computations to determine the group structure, we fix a so-called factor base, generate relations and finally solve the discrete logarithm problem via linear algebra.

Just as in [Diem 2011b], the factor base is defined in an algebraic way, and the relations are obtained by solving systems of multivariate polynomial equations over $\mathbb{F}_q$.

Let some instance of the problem with a prime power q, a natural number $n \geq 2$ and an elliptic curve $E/\mathbb{F}_{q^n}$ be given, where E is (as usual) given by an affine Weierstraß equation in x and y with neutral element the point at infinity.

The definition of the factor base and the relation generation are as follows:

Let m be some natural number not exceeding n, which will be optimized later, and let $d := \lceil n/m \rceil$ and $\delta := dm - n$.

We choose some d-dimensional vector subspace U of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$ and define the factor base by

$$\mathcal{F} := \{P \in E(\mathbb{F}_{q^n}) \mid x(P) \in U\}.$$

Furthermore, if n is not divisible by m (that is, $\delta \neq 0$), we choose a $(d-1)$-dimensional vector subspace U' of U and set

$$\mathcal{F}' := \{P \in E(\mathbb{F}_{q^n}) \mid x(P) \in U'\}.$$

Given some element $P \in E(\mathbb{F}_{q^n})$, we want to find a relation

$$P_1 + \cdots + P_m = P$$

with $P_i \in \mathcal{F}'$ for $i = 1, \ldots, \delta$ and $P_i \in \mathcal{F}$ for $i = \delta + 1, \ldots, m$. The key idea is again to find such relations by solving systems of polynomial equations over $\mathbb{F}_q$. One possibility to obtain such a system is via summation polynomials.

Recall that the $(m+1)$-th summation polynomial with respect to the covering $x_{|E} : E \to \mathbb{P}^1_{\mathbb{F}_{q^n}}$ is an irreducible multihomogeneous polynomial $S_{m+1} \in \mathbb{F}_{q^n}[X_1, Y_1, \ldots, X_{m+1}, Y_{m+1}]$ such that, for $P_1, \ldots, P_{m+1} \in E(\overline{\mathbb{F}}_q)$, $P_1 + \cdots + P_{m+1} = 0$ if and only if $s_{m+1}(x_{|E}(P_1), \ldots, x_{|E}(P_{m+1})) = 0$; see Proposition 2.1 and Section 3 of [ibid.]. The $(m+1)$-th affine summation polynomial with respect to $x_{|E}$ is the dehomogenization of this polynomial with respect to $Y_1, \ldots, Y_m$. This is a polynomial $s_{m+1}(x_1, \ldots, x_{m+1}) \in \mathbb{F}_{q^n}[x_1, \ldots, x_{m+1}]$.

We choose a basis of $\mathbb{F}_{q^n}|\mathbb{F}_q$. We expand the variables (or coordinates) $x_1, \ldots, x_m$ over $\mathbb{F}_q$ with respect to the basis. Then for $i = 1, \ldots, \delta$ and $i = \delta + 1, \ldots, m$ we restrict the resulting systems of coordinates to U' and U, respectively. In this way the polynomial $s_{m+1}(x_1, \ldots, x_m, x(P))$ gives rise to a system of n polynomials in n variables. The polynomial $s_{m+1}(x_1, \ldots, x_m, x(P))$ has degree 2^{m-1} in each variable and therefore total degree at most $m \cdot 2^{m-1}$. Therefore each polynomial in the system has degree at most $m \cdot 2^{m-1}$. It follows that "with multiplicities" the system has at most $(m \cdot 2^{m-1})^n = m^n \cdot 2^{(m-1)\cdot n}$ isolated solutions over $\mathbb{F}_q$. Here by an *isolated solution* we mean an isolated point of the scheme defined by the system. (This can be seen by intersection theory in $\mathbb{P}^n_{\mathbb{F}_q}$, similarly to statement a) in Proposition 2.5 of [ibid.].)

Now, with an algorithm by M. Rojas [1999], one can compute a list of solutions of the system over $\mathbb{F}_q$ containing all isolated solutions over $\mathbb{F}_q$ in an expected time of $\mathcal{P}oly(m^n \cdot 2^{n\cdot(m-1)} \cdot \log(q)) = \mathcal{P}oly(e^{mn} \cdot \log(q))$.

Let us assume that, for varying P, most solutions over $\mathbb{F}_q$ of these systems are indeed isolated. It is reasonable to estimate the size of $\mathcal{F}$ as roughly q^d and the size of $\mathcal{F}'$ as roughly q^{d-1}. This indicates that the expected value of relations obtained per try is in $\mathcal{O}(1/m!)$.

Disregarding the possibility that some of the relations generated might be linearly dependent, we need roughly q^d relations. This indicates an expected running time of

$$\mathcal{P}oly\big(m! \cdot e^{nm + \log(q)\cdot d}\big) = \mathcal{P}oly\big(e^{nm + \log(q)\cdot n/m}\big)$$

for the relation generation part.

The expected running time for the linear algebra part is merely $\mathcal{P}oly(e^{\log(q)\cdot d})$.

Now, for $m := \min(\lceil\sqrt{\log(q)}\rceil, n)$, we obtain, again on the basis of the above heuristic arguments, a total expected running time of

$$\mathcal{P}oly\big(e^{\max(\log(q),\, n\cdot\sqrt{\log(q)})}\big).$$

We stress again that we have used various heuristic assumptions. The goal of the rest of this work is to modify the algorithm in such a way that we can indeed prove

the claimed expected running time for large input classes. As already stated, we are however not able to establish the desired expected running time for all instances of the problem.

Weil restrictions and the scalar restriction functor. Let us recall the definition of the scalar restriction functor with respect to a finite field extension.

Let $K|k$ be a finite field extension. Now let X be a quasiprojective K-scheme of finite type. Then a representing object of the contravariant functor $Z \mapsto \mathrm{Hom}_K(Z \times_k K, X)$ from the category of k-schemes to the category of sets is called the Weil restriction of X with respect to $K|k$. We denote the representing k-scheme by $\mathrm{Res}_k^K(X)$; as usual we also fix a corresponding natural transformation. A reformulation of the definition is: The Weil restriction of X with respect to $K|k$ is a k-scheme $\mathrm{Res}_k^K(X)$ together with a morphism $u : \mathrm{Res}_k^K(X)_K = \mathrm{Res}_k^K(X) \times_k K \to X$ satisfying the following universal property: For any k-scheme and any K-morphism $\alpha : Z_K = Z \times_k K \to X$ there exists a unique k-morphism $\beta : Z \to \mathrm{Res}_k^K(X)$ with $\alpha = u \circ \beta_K$. We denote β by $\alpha_\circledcirc$. Now, the formation of the Weil restriction defines a functor from the category of quasiprojective K-schemes to the category of quasiprojective k-schemes; this functor is called the *scalar restriction functor*. Furthermore, if X is a group scheme, so is the Weil restriction in an obvious way.

In this work, we often use Weil restrictions of the affine line $\mathbb{A}^1_K = \mathrm{Spec}(K[x])$. Note here that $\mathrm{Res}_k^K(\mathbb{A}^1_K)(k) \simeq \mathbb{A}^1(K) = K$. One sees easily the following: Let $b_1, \ldots, b_n$ be a k-basis of K. Then $\mathbb{A}^n_k = \mathrm{Spec}(k[x_1, \ldots, x_n])$ together with the universal morphism $\mathbb{A}^n_K \to \mathbb{A}^1_K$, given on Z-valued points for any K-scheme Z by $P \mapsto x_1(P)b_1 + \cdots + x_n(P)b_n$, is a Weil restriction of $\mathbb{A}^1_k$ with respect to $K|k$ (as a group variety). The choice of a k-basis of K of course corresponds to choosing a k-homomorphism $K \approx k^n$.

We would like to have an explicit and canonical description of the Weil restriction of $\mathbb{A}^1_k$ which does not depend on the choice of a basis. For this, let us define for any finite-dimensional k-vector space V the polynomial algebra $k[V]$ in the usual way:

$$k[V] := \bigoplus_{i=0}^{\infty} V^{\overset{\otimes i}{\mathrm{sym}}}.$$

For some finite-dimensional k-vector space V, let

$$\mathbb{A}_k[V] := \mathrm{Spec}(k[V^\vee]),$$

where $V^\vee$ is the dual space of V. Now, for any k-algebra A, we have $\mathbb{A}_k[V](A) \simeq \mathrm{Hom}_k(V^\vee, A) \simeq A \otimes_k V$ in a natural way. Now, $A \otimes_k V$ is a k-vector space and therefore in particular an abelian group. We obtain in this way a commutative group structure on $\mathbb{A}_k[V]$. Clearly, $\mathbb{A}_k[V](k)$ is isomorphic to $(V, +)$ itself. The association $V \mapsto \mathbb{A}_k[V]$ gives rise to a covariant functor from the category of

finite-dimensional vector spaces over k to the category of affine group varieties over k. Here, an injective homomorphism $U \to V$ gives a closed embedding $\mathbb{A}_k[U] \to \mathbb{A}_k[V]$, and in particular, for a vector subspace U of V, $\mathbb{A}_k[U]$ is a group subvariety of $\mathbb{A}_k[V]$.

As a special case of the preceding we have natural isomorphisms $\mathbb{A}_k[K](A) \simeq A \otimes_k K$ for any k-algebra A. Therefore $\mathbb{A}_k[K]$ is in a natural way a Weil restriction of $\mathbb{A}^1_K$ with respect to $K|k$. We remark that the universal morphism $u : \mathbb{A}_k[K] \times_k K \to \mathbb{A}^1_K$ is given as follows: $\mathbb{A}_k[K] \times_k K$ is the affine scheme defined by the K-algebra $k[K^\vee] \otimes_k K \simeq \bigoplus_{i=0}^{\infty} (K^\vee)^{\otimes_{\mathrm{sym}} i} \otimes_k K$, and the universal morphism corresponds to a homogeneous element of degree 1 in the algebra, that is, to an element of $K^\vee \otimes_k K$. This vector space is naturally isomorphic to the vector space of endomorphisms of K as a vector space over k. The universal morphism is the element of $K^\vee \otimes_k K$ corresponding to the identity in this space.

We also use Weil restrictions with respect to flat coverings, that is, finite and flat morphisms. For this and also for other aspects of the scalar restriction functor we refer to Subsection 4.1 of [Diem 2011b].

Tangent spaces and ramification. We make frequent use of homomorphisms between tangent spaces to address whether morphisms of schemes over fields are unramified at rational points. For the convenience of the reader and because we could not find a suitable reference, we make some general remarks here.

Let k be a field.

Let X be a k-scheme of finite type and P a k-rational point of X. Denoting by $\kappa(P)$ the residue field at P, we have a canonical isomorphism $k \simeq \kappa(P)$. We use the latter notation if we regard k as an $\mathbb{O}_{X,P}$-algebra.

The k-vector spaces $\Omega_{X,P} \otimes_{\mathbb{O}_{X,P}} \kappa(P)$ and $\mathfrak{m}_P/\mathfrak{m}_P^2$ are canonically isomorphic; see [Hartshorne 1977, Chapter II, Proposition 8.7]. Either one of these spaces is called the *cotangent space* at P. The *Zariski tangent space* or simply *tangent space* of P in X is $T_P(X) := \mathrm{Hom}_k(\mathfrak{m}_P/\mathfrak{m}_P^2, k)$. The formation of the tangent spaces behaves well under base change via a field extension over k. Let us note here that it is important that P is a k-rational point. A special case which is of importance in this work is: for any finite-dimensional k-vector space V we have a canonical isomorphism $T_0(\mathbb{A}_k[V]) \simeq V$; we identify these spaces.

Let now X be a smooth k-scheme. Then the *tangent sheaf* of X is $\mathcal{T}_X := \Omega_X^\vee = \mathcal{H}om_{\mathbb{O}_X}(\Omega_X, \mathbb{O}_X)$. The canonical homomorphism

$$\begin{aligned} \mathcal{T}_{X,P} &\simeq \mathrm{Hom}_{\mathbb{O}_{X,P}}(\Omega_{X,P}, \mathbb{O}_{X,P}) \to \mathrm{Hom}_{\mathbb{O}_{X,P}}(\Omega_{X,P}, \kappa(P)) \\ &\simeq \mathrm{Hom}_k(\Omega_{X,P} \otimes_{\mathbb{O}_{X,P}} \kappa(P), k) \simeq T_P(X) \end{aligned}$$

induces a homomorphism of k-vector spaces

$$\mathcal{T}_{X,P} \otimes_{\mathcal{O}_{X,P}} \kappa(P) \to T_P(X).$$

As $\Omega_{X,P}$ is (by assumption) a free $\mathcal{O}_{X,P}$-module, this homomorphism is an isomorphism. We denote the image of $t \in \mathcal{T}_{X,P}$ in $T_P(X)$ by $t(P)$.

Now let X and Y be arbitrary k-schemes of finite type, let $f : X \to Y$ be a morphism of k-schemes and let $P \in X$. Then the local ring of P in its fiber over $f(P)$ is $\mathcal{O}_{X,P}/f^{\#}(\mathfrak{m}_{Y,f(P)})\mathcal{O}_{X,P}$, and f is said to be *unramified* at P if this local ring is a finite and separable $\kappa(f(P))$-algebra. If f is unramified at P then it is in particular quasifinite at P; that is, P is isolated in its fiber.

Let now P be a k-rational point of X. Then f is unramified at P if and only if $f^{\#}(\mathfrak{m}_{Y,f(P)})$ generates the maximal ideal of $\mathcal{O}_{X,P}$. By Nakayama's lemma, this is the case if and only if the induced homomorphism between cotangent spaces $f^* : \mathfrak{m}_{f(P)}/\mathfrak{m}_{f(P)}^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$ is surjective. Therefore, f is unramified at P if and only if the induced homomorphism between tangent spaces $f_* : T_P(X) \to T_{f(P)}(Y)$ is injective.

2. The factor base

2A. ***Some general thoughts.*** In [Diem 2011b] we first described the algorithm, which is rather elementary, and later presented the geometric background, involving in particular the role of the Weil restriction of the elliptic curve with respect to $\mathbb{F}_{q^n}|\mathbb{F}_q$.

This approach would also be possible here. However, we now present the geometric background together with the description of the algorithm. The main reason for this is that the conditions required for the definition of the factor base are quite involved but closely related to geometric considerations.

We first make some remarks on the definition of the factor base in [ibid.].

Let an instance with a nontrivial extension of finite fields $\mathbb{F}_{q^n}|\mathbb{F}_q$ and an elliptic curve E over $\mathbb{F}_{q^n}$ be given, where an affine part of E is given by a Weierstraß equation in x and y with degree 2 in x. Let $k := \mathbb{F}_q$ and $K := \mathbb{F}_{q^n}$.

Then, in [ibid.], the factor base is defined as follows:

We fix a covering $\varphi : E \to \mathbb{P}^1_K$ of degree 2 with $\varphi \circ [-1] = \varphi$ satisfying a certain condition (Condition 2.7 in [Diem 2011b]). Then the factor base $\mathcal{F}$ is the set

$$\{P \in E(K) \mid \varphi(P) \in \mathbb{P}^1(k)\}. \tag{2}$$

Now there exists a unique automorphism α of $\mathbb{P}^1_k$ with $\varphi = \alpha \circ x_{|E}$. The factor base is then equal to

$$\{P \in E(K) \mid x_{|E}(P) \in \alpha^{-1}(\mathbb{P}^1(k))\}. \tag{3}$$

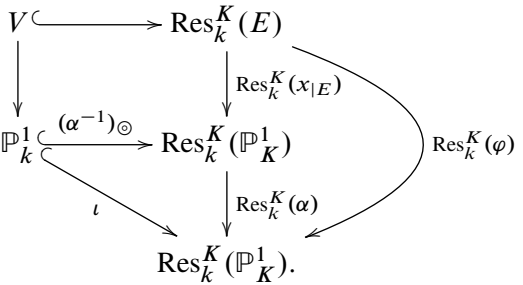
A geometric description of the definition of the factor base in (2) is as follows: Let $\iota = \mathrm{id}_{\circledcirc} : \mathbb{P}^1_k \to \mathrm{Res}^K_k(\mathbb{P}^1_k)$ be the morphism corresponding to the identity on $\mathbb{P}^1_K$ under the universal property of the Weil restriction. This morphism is a closed immersion; it might be called the canonical immersion.

We define V by the diagram

$$\begin{array}{ccc} V & \hookrightarrow & \mathrm{Res}^K_k(E) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}^K_k(\varphi)} \\ \mathbb{P}^1_k & \xrightarrow{\iota} & \mathrm{Res}^K_k(\mathbb{P}^1_k) \end{array} \tag{4}$$

being Cartesian; cf. [ibid., Subsection 4.3]. Then, under the canonical isomorphism $E(K) \simeq \mathrm{Res}^K_k(E)(k)$, the factor base $\mathcal{F}$ corresponds to $V(k)$. Recall here that as the morphism $\varphi : E \to \mathbb{P}^1_K$ is a flat covering of degree 2, the morphism $\mathrm{Res}^K_k(\varphi) : \mathrm{Res}^K_k(E) \to \mathrm{Res}^K_k(\mathbb{P}^1_K)$ and the induced morphism $V \to \mathbb{P}^1_k$ are flat coverings of degree 2^n.

From a geometric point of view, the equivalence of the two descriptions of the factor base via (2) and (3) follows from the commutativity of the diagram



Note here that, by the universal property of the Weil restriction of $\mathbb{P}^1_K$ with respect to $K|k$, the immersions $\mathbb{P}^1_k \hookrightarrow \mathrm{Res}^K_k(\mathbb{P}^1_K)$ correspond exactly to the automorphisms of $\mathbb{P}^1_K$ (via $\alpha \mapsto \alpha_{\circledcirc}$). Thus, instead of varying the covering $\varphi : E \to P^1_K$ in the construction of the factor base, we could also have varied the immersion of $\mathbb{P}^1_k$ into $\mathrm{Res}^K_k(\mathbb{P}^1_K)$.

2B. ***The preliminary definition of the factor base.*** We now give some geometric background on the definition of the factor base in the preliminary algorithm outlined in the introduction. We conclude this subsection with a wish list on the geometric objects related to the definition of the factor base. This then leads to a modification of the construction of the factor base which is described in the next subsection.

Let E_a be the "affine part" of E; that is, $E_a := x_{|E}^{-1}(\mathbb{A}^1_K)$. Furthermore, as already mentioned above, let m be some natural number not exceeding n and let $d := \lceil n/m \rceil$ and $\delta := dm - n$.

In the preliminary algorithm in the introduction we defined the factor base as follows: we fix a d-dimensional k-vector subspace U of K, and we set

$$\mathcal{F} := \{P \in E_a(K) \mid x(P) \in U\}.$$

We now give a geometric description. As mentioned in the introduction, the inclusion $U \hookrightarrow K$ gives rise to a closed immersion $\mathbb{A}_k[U] \to \mathbb{A}_k[K]$, and thus $\mathbb{A}_k[U]$ is a group subvariety of $\mathbb{A}_k[K] = \mathrm{Res}_k^K(\mathbb{A}^1_K)$. Defining $V_a \subseteq \mathrm{Res}_k^K(E)$ by the diagram

$$\begin{array}{ccc} V_a & \hookrightarrow & \mathrm{Res}_k^K(E_a) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}_k^K(x_{|E_a})} \\ \mathbb{A}_k[U] & \hookrightarrow & \mathbb{A}_k[K] \end{array} \tag{5}$$

being Cartesian, the factor base corresponds to $V_a(k)$.

In the preliminary algorithm, we also have a $(d-1)$-dimensional k-vector subspace U' of U, defining a subset $\mathcal{F}'$ of $\mathcal{F}$. We define V'_a analogously to V_a with $\mathbb{A}_k[U]$ being substituted by $\mathbb{A}_k[U']$. Then $\mathcal{F}'$ corresponds to $V'_a(k)$. As the maps $V_a \to A$ and $V'_a \to A'$ are finite flat, every irreducible component of V_a has dimension m and every irreducible component of V'_a has dimension $m-1$; see [Hartshorne 1977, Chapter III, Corollary 9.6].

Now, we would like that the following conditions on V_a and V'_a are satisfied:

(1) The addition morphism $(\mathrm{Res}_k^K(E))^m \to \mathrm{Res}_k^K(E)$ induces a dominant morphism from every irreducible component of $(V'_a)^\delta \times V_a^{m-\delta}$ to $\mathrm{Res}_k^K(E)$.

(2) There exists an (absolute) constant $c > 0$ such that $V_a(k)$ contains at least $c \cdot q^d$ points and $V'_a(k)$ contains at least $c \cdot q^{d-1}$ points.

Note that $\dim((V'_a)^\delta \times V_a^{m-\delta}) = n$ and therefore the statement in the first item implies that the morphism $(V'_a)^\delta \times V_a^{m-\delta} \to \mathrm{Res}_k^K(E)$ is generically finite.

With a randomized algorithm it is straightforward to construct in an efficient way U and U' such that the second item is satisfied.

For $d = 1$, the morphism $(V'_a)^\delta \times V_a^{m-\delta} \to \mathrm{Res}_k^K(E)$ is surjective and therefore, if V'_a and V_a are irreducible, the first item is satisfied; see [Diem 2011b, Remark 4.21]. However, for $d > 1$, we cannot even give an example for which we can prove that the first condition holds. For this reason, we modify the definition of the factor base.

2C. ***The essential modification.*** We now discuss the modification of the construction of the factor base.

We impose the following condition.

Condition 2.1. The point $0 \in \mathbb{P}^1_K$ is not a branch point of $x_{|E} : E \to \mathbb{P}^1_K$ and its preimage in E consists of two K-rational points.

Note that, for $q^n \geq 16$, there exist at least 5 K-rational points on E, so there exists a point in $E(K)$ which is not a ramification point. In the algorithm for the definition of the factor base, we first pass to a projectively equivalent elliptic curve, also given in Weierstraß form with the point at infinity being the neutral element, such that the condition is satisfied. We then fix k-vector subspaces U_i of K of dimension $d-1$ for $i = 1, \ldots, \delta$ and of dimension d for $i = \delta+1, \ldots, m$ such that we have a decomposition

$$K = \bigoplus_{i=1}^{m} U_i \tag{6}$$

and such that some further conditions are satisfied; see Section 2E below. With

$$\mathcal{F}_i := \{P \in E_a(K) \mid x(P) \in U_i - \{0\}\}, \tag{7}$$

we define the factor base as

$$\mathcal{F} := \bigcup_{i=1}^{m} \mathcal{F}_i. \tag{8}$$

Later, for $P \in E(K)$, we search for a relation of the form

$$P_1 + \cdots + P_m = P$$

with $P_i \in \mathcal{F}_i$.

We now apply the geometric considerations of the previous subsection here. Decomposition (6) gives rise to a decomposition

$$\mathbb{A}_k[K] = \bigoplus_{i=1}^{m} \mathbb{A}_k[U_i] \tag{9}$$

in the category of commutative k-group varieties. Decomposition (6) is then obtained from (9) by taking k-valued points.

Similarly to above, we define $V_i \subseteq \mathrm{Res}_k^K(E_a)$ via the diagram

$$\begin{array}{ccc} V_i & \hookrightarrow & \mathrm{Res}_k^K(E_a) \\ \downarrow & & \downarrow \\ \mathbb{A}_k[U_i] & \hookrightarrow & \mathbb{A}_k[K] \end{array}$$

being Cartesian. Note that the morphism $\mathrm{Res}_k^K(E_a) \to \mathbb{A}_k[K]$ is a flat covering of degree 2^n which is unramified at $0 \in \mathbb{A}_k[K]$. As flatness and unramifiedness are

stable under base change, the morphism $V_i \to \mathbb{A}_k[U_i]$ is a flat covering of degree 2^n which is unramified at $0 \in \mathbb{A}_k[U_i]$ too. In particular, V_i has the same dimension as the vector space U_i.

Let

$$a_m : \mathrm{Res}_k^K(E)^m \to \mathrm{Res}_k^K(E) \tag{10}$$

be the m-fold addition morphism and

$$a'_m : V_1 \times \cdots \times V_m \to \mathrm{Res}_k^K(E) \tag{11}$$

be the restriction of a_m to $V_1 \times \cdots \times V_m$. Let P_0 be one of the two points of $E(K)$ which are mapped to 0 by $x_{|E}$.

Note that $\mathrm{Res}_k^K((P_0)_\circledcirc) = 0$. In particular, $(P_0)_\circledcirc$ is a k-rational point of all V_i.

Proposition 2.2. *The morphism a'_m is unramified at $((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)$.*

Remark 2.3. As unramifiedness is an open property, we obtain: a'_m is unramified in an open neighborhood of $((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)$. Every irreducible component of $V_1 \times \cdots \times V_m$ has dimension n (because we have a flat covering of $V_1 \times \cdots \times V_m$ to $\mathbb{A}_k[K]$). Thus the morphism a'_m is dominant. If furthermore $V_1, \ldots, V_m$ are irreducible, a'_m is generically unramified.

Proof of Proposition 2.2. We wish to show that

$$(a'_m)_* : T_{((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)}(V_1 \times \cdots \times V_m) \to T_{m\cdot(P_0)_\circledcirc}\left(\mathrm{Res}_k^K(E)\right)$$

is an isomorphism.

As the morphism $\mathrm{Res}_k^K(x_{|E})$ is unramified at $(P_0)_\circledcirc$, it induces an isomorphism of tangent spaces

$$T_{(P_0)_\circledcirc}\left(\mathrm{Res}_k^K(E_a)\right) \xrightarrow{\sim} T_0(\mathbb{A}_k[K]). \tag{12}$$

Decomposition (9) induces a decomposition of tangent spaces $T_0(\mathbb{A}_k[K]) = \bigoplus_{i=1}^m T_0(\mathbb{A}_k[U_i])$ which is nothing but the original decomposition of vector spaces $K = \bigoplus_{i=1}^m U_i$. Under isomorphism (12), $T_{(P_0)_\circledcirc}(V_i)$ corresponds to $T_0(\mathbb{A}_k[U_i])$. Therefore, we have the decomposition

$$T_{(P_0)_\circledcirc}\left(\mathrm{Res}_k^K(E_a)\right) = \bigoplus_{i=1}^m T_{(P_0)_\circledcirc}(V_i). \tag{13}$$

By the next lemma, we have the following commutative diagram whose vertical maps are isomorphisms:

$$\begin{array}{ccc} T_{((P_0)_\circledcirc,\dots,(P_0)_\circledcirc)}\big(\mathrm{Res}_k^K(E)^m\big) & \xrightarrow{(a_m)_*} & T_{m(P_0)_\circledcirc}\big(\mathrm{Res}_k^K(E)\big) \\ \downarrow{\scriptstyle ((p_1)_*,\dots,(p_m)_*)} & & \uparrow{\scriptstyle (\tau_{(m-1)\cdot(P_0)_\circledcirc})_*} \\ \big(T_{(P_0)_\circledcirc}\big(\mathrm{Res}_k^K(E)\big)\big)^m & \xrightarrow{\sum} & T_{(P_0)_\circledcirc}\big(\mathrm{Res}_k^K(E)\big) \end{array}$$

Here $p_i : \mathrm{Res}_k^K(E)^m \to \mathrm{Res}_k^K(E)$ is the projection to the i-th coordinate and the map $\sum : T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E)) \to T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E))$ is the addition of the k-vector space $T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E))$.

By restriction of the horizontal maps we obtain the commutative diagram

$$\begin{array}{ccc} T_{((P_0)_\circledcirc,\dots,(P_0)_\circledcirc)}(V_1\times\cdots\times V_m) & \xrightarrow{(a_m)_*} & T_{m(P_0)_\circledcirc}\big(\mathrm{Res}_k^K(E)\big) \\ \downarrow & & \uparrow{\scriptstyle (\tau_{(m-1)\cdot(P_0)_\circledcirc})_*} \\ T_{(P_0)_\circledcirc}(V_1)\times\cdots\times T_{(P_0)_\circledcirc}(V_m) & \xrightarrow{\sum} & T_{(P_0)_\circledcirc}\big(\mathrm{Res}_k^K(E)\big) \end{array}$$

Because of decomposition (13), the addition maps $T_{(P_0)_\circledcirc}(V_1)\times\cdots\times T_{(P_0)_\circledcirc}(V_m)$ bijectively to $T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E))$. This gives the desired statement. □

In the following lemma, we use this notation: Let U, V, W be k-vector spaces. If then $\varphi : U \to W$ and $\psi : V \to W$ are k-linear maps, we denote the induced map $U \times V \to W$ by $(\varphi \ \ \psi)$. If $\varphi : W \to U$ and $\psi : W \to V$ are k-linear maps, we denote the induced map $W \to U \times V$ by $\binom{\varphi}{\psi}$.

Lemma 2.4. *Let k be a field.*

(a) *Let X_1, X_2 be two k-schemes, and let $P_1 \in X_1(k)$, $P_2 \in X_2(k)$. Let us assume that X_1 is smooth at P_1 and X_2 is smooth at P_2. The points P_i give rise to closed immersions $\iota_i : X_i \to X_1 \times X_2$. Let $p_i : X_1 \times X_2 \to X_i$ be the canonical projections. Then the maps*

$$((\iota_1)_* \ \ (\iota_2)_*) : T_{P_1}(X_1) \times T_{P_2}(X_2) \to T_{(P_1,P_2)}(X_1 \times X_2)$$

and

$$\binom{(p_1)_*}{(p_2)_*} : T_{(P_1,P_2)}(X_1 \times X_2) \to T_{P_1}(X_1) \times T_{P_2}(X_2)$$

are isomorphisms of k-vector spaces which are inverse with respect to each other.

(b) *Let A be an abelian variety over k with addition morphism $a : A \times A \to A$ and neutral element O. Let $\iota_i : A \to A \times A$ be the two canonical immersions. Then the map $a_* \circ ((\iota_1)_* \ \ (\iota_2)_*) : T_O(A) \times T_O(A) \to T_O(A)$ is the addition on the k-vector space $T_O(A)$.*

(c) *Let A be an abelian variety over k and $P \in A(k)$. Then we have a commutative diagram*

$$\begin{array}{ccc} T_P(A \times A) & \xrightarrow{a_*} & T_{2P}(A) \\ \left(\begin{smallmatrix}(p_1)_* \\ (p_2)_*\end{smallmatrix}\right) \downarrow & & \uparrow (\tau_P)_* \\ T_P(A) \times T_P(A) & \xrightarrow{\sum} & T_P(A), \end{array}$$

where the lower map $\sum : T_P(A) \times T_P(A) \to T_P(A)$ is the addition morphism on the k-vector space $T_P(A)$.

Proof. (a) The k-linear map

$$T_{P_1}(X_1) \times T_{P_2}(X_2) \xrightarrow{\left((\iota_1)_* \ \ (\iota_2)_*\right)} T_{(P_1,P_2)}(X_1 \times X_2) \xrightarrow{\left(\begin{smallmatrix}(p_1)_* \\ (p_2)_*\end{smallmatrix}\right)} T_{P_1}(X_1) \times T_{P_2}(X_2)$$

is obviously the identity. As the dimensions of these k-vector spaces are the same, the two maps in (a) are both isomorphisms.

(b) We only have to check that the k-linear map $a_* \circ ((\iota_1)_* \ \ (\iota_2)_*) : T_O(A) \times T_O(A) \to T_O(A)$ agrees with the addition (which is also k-linear) on the first and second factor. But restricted to factor i, $a_* \circ ((\iota_1)_* \ \ (\iota_2)_*)$ becomes $a_* \circ (\iota_i)_*$, which is the identity, just as is the addition when restricted to one of the factors.

(c) Let us consider A as an abelian variety with P as neutral element, and let a_P be the addition law. Then $a_P = \tau_{-P} \circ a$. The commutativity of the diagram then follows from (b). □

2D. ***Irreducibility.*** If the characteristic is odd, in order to complete the analysis of the relation generation procedure, we need that the V_i are irreducible. In this subsection, we give some theoretical background for the algorithmic construction of the V_i such that they are indeed irreducible.

All the statements in this subsection are valid except in the case that the characteristic is 2 and the j-invariant of E is 0, or, in other words, except if E is a supersingular elliptic curve in characteristic 2. So let us assume that it does not hold that the characteristic is 2 and $j = 0$.

Lemma 2.5. *Let U be a vector subspace of K, and let V_a be defined as in (5). If $\mathbb{A}_k[U]$ contains an irreducible scheme containing 0 whose preimage in V_a is irreducible, then V_a is irreducible. Likewise, if $\mathbb{A}_k[U]$ contains a geometrically irreducible scheme containing 0 whose preimage in V_a is geometrically irreducible, then V_a is geometrically irreducible.*

Proof. Assume that V_a is not irreducible, and let $V_a^{(1)}$ and $V_a^{(2)}$ be two irreducible components of V_a. Let $\mathscr{A} \subseteq \mathbb{A}_k[U]$ be the étale locus of the flat covering $V_a \to \mathbb{A}_k[U]$

and $\mathcal{V}_a$ its preimage on V_a. By Condition 2.1 the covering $E_a \to \mathbb{A}^1_K$ is unramified at 0. Thus so is the covering $\mathrm{Res}^K_k(E_a) \to \mathbb{A}_k[K]$ and the induced covering $V_a \to \mathbb{A}_k[U]$. Thus 0 is contained in $\mathcal{A}$. In particular, $\mathcal{A}$ is nonempty and thus a nonempty open part of $\mathbb{A}_k[U]$.

For $i = 1, 2$, the map $V_a^{(i)} \to \mathbb{A}_k[U]$ is surjective. (As the map $V_a^{(i)} \to \mathbb{A}_k[U]$ is flat and finite, by [Hartshorne 1977, Chapter III, Corollary 9.6], $V_a^{(i)}$ has the same dimension as $\mathbb{A}_k[U]$. The dimension of $V_a^{(i)}$ is equal to the dimension of its image. Thus the dimension of the image is equal to $\mathbb{A}_k[U]$. Therefore the map is dominant. As the map is finite, it is in particular closed, and therefore the image is equal to $\mathbb{A}_k[U]$.) Therefore $V_a^{(i)}$ contains a preimage of 0. Let $\mathcal{V}_a^{(i)}$ be the preimage of $\mathcal{A}$ in $V_a^{(i)}$. Then $\mathcal{V}_a^{(i)}$ is a nonempty open part of $V_a^{(i)}$ which contains a preimage of 0.

As $\mathbb{A}_k[U]$ is smooth, so is $\mathcal{A}$, and, as furthermore $\mathcal{V} \to \mathcal{A}$ is étale, $\mathcal{V}$ is also smooth. It follows that $\mathcal{V}_a^{(1)}$ and $\mathcal{V}_a^{(2)}$ are disjoint.

Let now S be an irreducible subscheme of $\mathbb{A}_k[U]$ as in the first claim of the lemma. As $V_a \to \mathbb{A}_k[U]$ is unramified at 0 and $0 \in S$ by assumption, $S \cap \mathcal{A}$ is a nonempty open part of S. It follows that the preimage of $S \cap \mathcal{A}$ is a nonempty open part of the preimage of S and thus also irreducible. Therefore it is contained in either $\mathcal{V}_a^{(1)}$ or $\mathcal{V}_a^{(2)}$. On the other hand, as it contains all preimages of 0, it has nontrivial intersection with both $\mathcal{V}_a^{(1)}$ and $\mathcal{V}_a^{(2)}$, a contradiction.

The second claim follows via base change to $\bar{k}$. □

In the algorithm, we first search for 1-dimensional k-vector subspaces T_i of K such that the preimages of $\mathbb{A}_k[T_i]$ in $\mathrm{Res}^K_k(E_a)$ with respect to $\mathrm{Res}^K_k(x_{|E_a})$ are geometrically irreducible. Then we search for suitable k-vector subspaces U_i of K containing T_i. The preimages V_i of the corresponding group subvarieties $\mathbb{A}_k[U_i]$ of $\mathbb{A}_k[K]$ then contain $\mathbb{A}_k[T_i]$ and are therefore geometrically irreducible.

To choose the spaces T_i we employ ideas from the first subsection of this section and of our previous work.

Let $\mu \in K^*$, and let us consider the vector subspace $\mu^{-1} \cdot k$ of K and the associated group subvariety $\mathbb{A}[\mu^{-1} \cdot k]$ of $\mathbb{A}_k[K]$. Furthermore, let W_a be the preimage of $\mathbb{A}[\mu^{-1} \cdot k]$ in $\mathrm{Res}^K_k(E_a)$.

Clearly, the group subvariety $\mathbb{A}[\mu^{-1} \cdot k]$ is the image under the closed immersion $\mathbb{A}^1_k \to \mathbb{A}_k[K]$ induced by the injective homomorphism of vector spaces $k \to K$, $a \mapsto \mu^{-1}a$. This morphism can also be given as follows: Let $\alpha_a := \mu x : \mathbb{A}^1_k \to \mathbb{A}^1_k$. Then the morphism $\mathbb{A}^1_k \to \mathbb{A}_k[K]$ is equal to $(\alpha_a^{-1})_\circledcirc$.

We now essentially apply the considerations of Section 2A here, restricting ourselves to the "affine parts". We set $\varphi_a := \alpha_a \circ x_{|E_a}$. Now W_a is the preimage of $\iota(\mathbb{A}^1_k)$ in $\mathrm{Res}^K_k(E_a)$ with respect to the covering $\mathrm{Res}^K_k(\varphi_a)$. This is very closely related to the situation studied in [Diem 2011b, Section 2.2] — the only difference is

that here we use automorphisms of the group variety $\mathbb{A}^1_K$ instead of automorphisms of $\mathbb{P}^1_K$ and we restrict ourselves to the "affine parts".

Lemma 2.6. *There are more than $q^n - 3(n-1)\cdot q^{n/2}$ elements $\mu \in K^*$ such that, with W_a as defined as above, W_a is geometrically irreducible.*

Proof. By assumption on k and E, the covering $x_{|E} : E_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ has two or four branch points, one of which is at infinity. Thus there are exactly one or three branch points not equal to infinity.

Let $\lambda_1, \ldots, \lambda_s \in \mathbb{F}_{q^{6n}} - \{0\}$, with $s \in \{1,3\}$, be the branch points of $x_{|E_a} : (E_a)_{\bar{k}} \to \mathbb{A}^1_{\bar{k}}$. Let $\mu \in K^*$ and let $\alpha := \mu x$. Then the branch points of $\alpha \circ x_{|E_a} : (E_a)_{\bar{k}} \to \mathbb{A}^1_{\bar{k}}$ are $\mu\lambda_1, \ldots, \mu\lambda_s$. Therefore Condition 2.7 from [ibid.] is equivalent to the following condition.

Condition 2.7. There exists an $i = 1, \ldots, s$ such that, for $j = 1, \ldots, n-1$, $(\mu\lambda_i)^{q^j} \notin \{\mu\lambda_1, \ldots, \mu\lambda_s\}$.

As shown in [ibid., Proposition 4.9], if this condition is satisfied, W_a is geometrically irreducible.

We are interested in the probability that, for $j = 1, \ldots, n-1$, $(\mu\lambda_1)^{q^j} \notin \{\mu\lambda_1, \ldots, \mu\lambda_s\}$.

For $j = 1, \ldots, n-1$ and $\ell = 1, \ldots, s$, the condition $(\mu\lambda_1)^{q^j} = \mu\lambda_\ell$ is equivalent to $\mu^{q^j-1} = \lambda_\ell / \lambda_1^{q^j}$. As the cardinality of the kernel of the map $K^* \to \bar{k}^*$, $a \mapsto a^{q^j-1}$ is $q^{\gcd(j,n)} - 1$ (see next lemma), there are either no or exactly $q^{\gcd(j,n)} - 1$ such elements μ.

The situation is now very similar to the situation in [ibid., Lemma 2.10]: in total there are at most $s \cdot \sum_{j=1}^{n-1} (q^{\gcd(j,n)} - 1)$ elements μ for which the condition in the lemma is not satisfied.

Now a crude estimate is that $s \cdot \sum_{j=1}^{n-1} q^{\gcd(j,n)-1} < s \cdot (n-1) \cdot q^{n/2}$. □

Lemma 2.8. *Let q be a prime power and $m, n \in \mathbb{N}$. Then $q^m - 1 \mid q^n - 1$ if and only if $m \mid n$. Moreover* $\gcd(q^m - 1, q^n - 1) = q^{\gcd(m,n)} - 1$.

Proof. If $m \mid n$ then clearly $q^m - 1 \mid q^n - 1$. So assume that $q^m - 1 \mid q^n - 1$. For $a \in \mathbb{F}^*_{q^m}$ we have $a^{q^m-1} = 1$ and by assumption also $a^{q^n-1} = 1$. But this means that $a \in \mathbb{F}^*_{q^n}$. Thus $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ and thus $m \mid n$.

For the second statement, consider the set $G := \{a \in \mathbb{F}_{q^n} \mid a^{q^m-1} = 1\}$. On the one hand, as G is a subgroup of the cyclic group $\mathbb{F}^*_{q^m}$, it has $\gcd(q^m - 1, q^n - 1)$ elements. On the other hand, $G \cup \{0\}$ is a subfield of $\mathbb{F}_{q^n}$, and therefore there exists some $a \mid n$ with $\#G = q^a - 1$. The result now follows with the first statement. □

2E. ***The algorithm for the factor base.*** Let a field extension $K|k$ as above, an elliptic curve E/K, two points $A, B \in E(K)$ with $B \in \langle A \rangle$ as well as $m \in \mathbb{N}$ with $2 \le m \le n$ be given, where $\#K \ge 16$. As always, let $d := \lceil n/m \rceil$ and $\delta := dm - n$.

We first choose — with a randomized algorithm — some point $P_0 \in E_a(K)$ which is not a ramification point of $x_{|E}$ and pass from E to its image under the automorphism of $\mathbb{P}^2_K$ given by $P = (X(P) : Y(P) : Z(P)) \mapsto (X(P) - x(P_0)Z(P) : Y(P) : Z(P))$. Let $\tilde{E}$ be the resulting curve. This is again a curve in Weierstraß form, $x_{|\tilde{E}}$ is unramified above 0 and the preimage of 0 consists of two K-rational points. Clearly, this computation can be performed in an expected time which is polynomially bounded in $\log(q^n)$.

So let us now assume that there exists a K-rational point of E which is unramified under $x_{|E}$ and mapped to 0.

Given an instance as described, we would like to compute a decomposition

$$K = \bigoplus_{i=1}^{m} U_i$$

with $\dim(U_i) = d - 1$ for $i = 1, \ldots, \delta$ and $\dim(U_i) = d$ for $i = \delta + 1, \ldots, m$ such that

- $\#\{P \in E_a(K) \mid x(P) \in U_i - \{0\}\} \geq \frac{1}{4} q^{\dim(U_i)}$;
- if $\mathrm{char}(k)$ is odd: $V_1, \ldots, V_m$ are irreducible.

The factor base is then defined as described in (7) and (8) above.

We now give an algorithm for the task just mentioned under the condition that $m \leq n/2$ and $q \geq 4$. This is sufficient for the algorithm for Theorem 2.

Algorithm to compute a suitable decomposition of K

Input: A field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$ with $q \geq 4$, an elliptic curve $E/\mathbb{F}_{q^n}$ in Weierstraß form with respect to x and y such that there is a K-rational point of E which is unramified under $x_{|E}$ and mapped to 0, two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$ and a natural number m with $2 \leq m \leq n/2$.

Output: A decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{m} U_i$ with $\dim(U_i) = d - 1$ for $i = 1, \ldots, \delta$ and $\dim(U_i) = d$ for $i = \delta + 1, \ldots, m$ such that the conditions mentioned above are satisfied.

(1) If q is not a power of 2
  For $i = 1, \ldots, m$ do
    Repeat
      Choose $\mu_i \in \mathbb{F}^*_{q^n}$ uniformly at random.
    Until μ_i is not contained in $\langle T_1, \ldots, T_{i-1} \rangle$ and μ_i satisfies Condition 2.7.
    Let $T_i \leftarrow \mu_i^{-1} \cdot \mathbb{F}_q < \mathbb{F}_{q^n}$.
  If q is a power of 2, let $T_i \leftarrow \{0\}$ for $i = 1, \ldots, m$.

(2) Let $d \leftarrow \lceil n/m \rceil$ and $\delta \leftarrow dm - n$.
For $i = 1, \ldots, m$ do
If $i \leq \delta$, let $e \leftarrow d - 1$, otherwise let $e \leftarrow d$.
Repeat
Compute an $\mathbb{F}_q$-vector subspace U_i of $\mathbb{F}_{q^n}$ which is uniformly randomly chosen from the set of e-dimensional $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$ containing T_i with intersection $\{0\}$ with $U_1 + \cdots + U_{i-1} + T_{i+1} + \cdots + T_m$.
Until $\{E_a(\mathbb{F}_{q^n}) \mid x(P) \in U_i - \{0\}\}$ contains at least $\frac{1}{4} \cdot q^e$ elements.

(3) Output $U_1, \ldots, U_m$.

Remark 2.9. We represent $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$ by bases over $\mathbb{F}_q$. Therefore the definition of T_i is computationally void; we inserted it only to be able to reason about T_i later.

Note here that, at the end of each iteration of the for-loop in Step 2, we have a direct sum $U_1 \oplus \cdots \oplus U_i \oplus T_{i+1} \oplus \cdots \oplus T_m$ inside K, where, for $j = 1, \ldots, i$, U_j contains T_j, $\dim(U_j) = d - 1$ if $j \leq \delta$ and $\dim(U_j) = d$ if $j > \delta$. The vector space T_i corresponds to a 1-dimensional group subscheme of $\mathbb{A}_k[K]$ whose preimage in $\mathrm{Res}_k^K(E)$ is geometrically irreducible by the arguments in Lemma 2.6. By Lemma 2.5, V_i is then also geometrically irreducible. Therefore an output of the algorithm defines a decomposition $K = \bigoplus_{i=1}^m U_i$ which satisfies the conditions given above.

We remark here that the algorithm itself is much more elementary than the geometric arguments.

The main result of this section is the following proposition.

Proposition 2.10. *For $2 \leq m \leq n/2$ and $q \geq 4$, following the above algorithm, one can compute a decomposition of K with the desired properties in an expected time of $\mathcal{P}oly(n \cdot q^d) = \mathcal{P}oly(n \cdot q^{n/m})$.*

Proof. We only have to consider the expected running time. For this, we discuss the steps of the algorithm.

Step 1. Let q be odd. We consider, for a particular iteration of the for-loop, the expected value of iterations of the repeat-loop.

As $i \leq m$, the space $\langle T_1, \ldots, T_{i-1} \rangle$ contains at most $q^{m-1} \leq q^{n/2}$ elements. By Lemma 2.6, there are at least $q^n - 3(n-1) \cdot q^{n/2} - q^{n/2} \geq q^n - 3n \cdot q^{n/2}$ elements $\mu \in K^*$ which do not lie in $\langle T_1, \ldots, T_{i-1} \rangle$ and which satisfy Condition 2.7. The probability that this is satisfied is therefore at least $1 - 3n/q^{n/2}$. For $n \geq 4$ and $q \geq 4$, which is the case by assumption, this is at least $1 - 3n/2^n \geq 1 - \frac{12}{16} = \frac{1}{4}$. The expected value of iterations of the repeat-loop is therefore at most 4. We can obtain an expected running time which is polynomially bounded in $n \cdot \log(q)$.

Step 2. We always have $e \geq 2$. In the repeat-loop, the space U_i can be computed in an expected time which is polynomially bounded in $n \cdot \log(q)$ by the next lemma. The counting of the set $\{E_a(\mathbb{F}_{q^n}) \mid x(P) \in U_i - \{0\}\}$ can be performed in a time which is polynomially bounded in q^d. The expected number of repetitions of the loop is at most 14 by Lemma 2.12 below. The expected running time of Step 2 is then polynomially bounded in q^d. □

Lemma 2.11. *Let S and T be two $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_q^n$ with $S \cap T = \{0\}$ and $S + T \subsetneq \mathbb{F}_q^n$, and let $e \in \mathbb{N}$ with $\dim(T) \leq e \leq n - \dim(S)$ be given. Then in an expected time which is polynomially bounded in $n \cdot \log(q)$ one can compute an $\mathbb{F}_q$-vector subspace U of $\mathbb{F}_q^n$ which is uniformly randomly chosen from the set of e-dimensional $\mathbb{F}_q$-vector subspaces U of $\mathbb{F}_q$ with $T \subseteq U$ and $S \cap U = \{0\}$.*

Proof. Consider the following algorithm:

Input: Two $\mathbb{F}_q$-vector subspaces S and T of $\mathbb{F}_q^n$ with $S \cap T = \{0\}$, and $e \in \mathbb{N}$ with $\dim(T) \leq e \leq n - \dim(S)$.

Output: An $\mathbb{F}_q$-vector subspace U satisfying the conditions in the lemma.

Let $v_1, \ldots, v_{\dim(T)}$ be the basis of T given with the input.

For $i = \dim(T) + 1, \ldots, e$ do
    Repeat
        Choose $v_i \in \mathbb{F}_q^n$ uniformly at random.
    Until $v_i \notin \langle v_1, \ldots, v_{i-1} \rangle + S$.
Output $\langle v_1, \ldots, v_e \rangle$.

Obviously the space $\langle v_1, \ldots, v_e \rangle$ is uniformly randomly distributed in the set of e-dimensional subspaces U of $\mathbb{F}_q^n$ with $T \subseteq U$ and $S \cap U = \{0\}$. The claimed expected running time follows from the fact that the probability that v_i is in the $(i - 1 + \dim(S))$-dimensional vector subspace is $q^{(i-1)+\dim(S)-n} \leq 1/q$. □

Lemma 2.12. *For $q \geq 4$ and $n \geq 4$, elliptic curves $E/\mathbb{F}_{q^n}$ in Weierstraß form, proper $\mathbb{F}_q$-vector subspaces S and T of $\mathbb{F}_{q^n}$ with $\dim(S) \leq n-2$, $S \cap T = \{0\}$ and $S + T \subsetneq \mathbb{F}_q^n$ and a natural number e with $\dim(T) < e \leq n - \dim(S)$, the following holds:*

Let U be a uniformly randomly distributed vector subspace of $\mathbb{F}_q^n$ of dimension e with $T \subseteq U$ and $S \cap U = \{0\}$. Then, with a probability of at least $\frac{1}{14}$, $\#\{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U - \{0\}\} \geq \frac{1}{4} \cdot q^e$.

Proof. Let first U be a uniformly randomly distributed e-dimensional $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^n}$. Then, as each point of $\mathbb{F}_{q^n} - \{0\}$ has the same probability of appearing in U, each point of $\mathbb{F}_{q^n} - \{0\}$ has a probability of

$$\frac{q^e - 1}{q^n - 1}$$

to appear in U.

Likewise, if S, T and e are as in the lemma and U is a uniformly randomly distributed e-dimensional vector subspace of $\mathbb{F}_{q^n}$ with $T \subseteq U$ and $U \cap S = \{0\}$, each point of $\mathbb{F}_{q^n} - (S \cap T)$ has a probability of

$$\frac{q^e - q^{\dim(T)}}{q^n - q^{\dim(S)}} \geq \frac{1}{2} \cdot q^{e-n}$$

to appear in U.

Let

$$\mathcal{S} := \{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in S\}, \quad \mathcal{T} := \{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in T - \{0\}\},$$
$$N := \#\{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U - \{0\}\}.$$

The expected value of N, $\mathbb{E}[N]$, can be expressed as follows:

$$\begin{aligned}\mathbb{E}[N] &= \#(E_a(\mathbb{F}_{q^n}) - (\mathcal{S} \cup \mathcal{T})) \cdot \frac{q^e - q^{\dim(T)}}{q^n - q^{\dim(S)}} + \#\mathcal{T} \\ &\geq (\#E_a(\mathbb{F}_{q^n}) - \#\mathcal{S}) \cdot \frac{q^e - q^{\dim(T)}}{q^n - q^{\dim(S)}} \geq (q^n - 2 \cdot q^{n/2} - 2 \cdot q^{\dim(S)}) \cdot \tfrac{1}{2} \cdot q^{e-n},\end{aligned}$$

the last inequality by the Hasse–Weil bound.

As $q \geq 4$ and $n \geq 4$, $2 \cdot q^{n/2} \leq \frac{1}{8} \cdot q^n$. As $q \geq 4$ and $\dim(S) \leq n-2$, $2 \cdot q^{\dim(S)} \leq 2 \cdot q^{n-2} \leq \frac{1}{8} \cdot q^n$. We obtain

$$\mathbb{E}[N] \geq \tfrac{3}{8} \cdot q^e.$$

On the other hand, $N \leq 2 \cdot q^e$. The claimed bound on the probability that $N \geq \frac{1}{4} \cdot q^e$ now follows by the following elementary probability theoretic argument. We have

$$\tfrac{3}{8} \cdot q^e \leq \mathbb{E}[N] \leq \mathbb{P}\big[N < \tfrac{1}{4} \cdot q^e\big] \cdot \tfrac{1}{4} \cdot q^e + \mathbb{P}\big[N \geq \tfrac{1}{4} \cdot q^e\big] \cdot 2 \cdot q^e$$

and thus

$$\tfrac{3}{8} \leq \big(1 - \mathbb{P}\big[N \geq \tfrac{1}{4} \cdot q^e\big]\big) \cdot \tfrac{1}{4} + \mathbb{P}\big[N \geq \tfrac{1}{4} \cdot q^e\big] \cdot 2 = \tfrac{1}{4} + \tfrac{7}{4} \cdot \mathbb{P}\big[N \geq \tfrac{1}{4} \cdot q^e\big].$$

In other words,

$$\mathbb{P}\big[N \geq \tfrac{1}{4} \cdot q^e\big] \geq \tfrac{1}{14}. \qquad \square$$

After suitable k-vector subspaces U_i of K have been computed, the sets $\mathcal{F}_i := \{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U_i - \{0\}\}$ are enumerated and sorted for the elements in $\mathcal{F}_i$ (such that given an element of $\mathcal{F}_i$ one can easily find its number). The factor base is then $\mathcal{F} := \bigcup_{i=1}^{m} \mathcal{F}_i$.

The total expected running time for all these computations is polynomially bounded in $n \cdot q^d$.

3. The new decomposition algorithm

Just as in the predecessor [Diem 2011b] to this work, the relation generation relies on an algorithm to compute "decompositions", and this algorithm is again based on solving systems of multivariate polynomials over $\mathbb{F}_q$. The definition of a "decomposition" is however different in this work from the previous one. Moreover, we do not use summation polynomials anymore, and, more generally, we do not use the projection to a product of projective lines. The reason for this is that, by avoiding the projection to projective lines, we can significantly improve the lower bound on the success probability of the relation generation algorithm. This improvement is crucial for the derivation of Theorem 2.

We start with some definitions.

As in the previous section, let q be a prime power, n a natural number at least 2, and let us set $k := \mathbb{F}_q$ and $K := \mathbb{F}_{q^n}$. Let E be an elliptic curve in Weierstraß form in x and y over K (with zero point at infinity), and let $f(x, y) \in K[x, y]$ be the defining polynomial of the affine part E_a. (The notation for the defining polynomial is different from the one in [ibid.].) Let us fix a direct sum decomposition $K = \bigoplus_{i=1}^{m} U_i$ with $m \geq 2$ into k-vector subspaces. (In this whole section, we do not impose any conditions on $x_{|E}$ or the direct sum decomposition of K, except that the decomposition be nontrivial.) Let $\mathcal{F}_i$ be defined as above. Finally, let $P \in E(K)$.

Definition 3.1. A tuple $(P_1, \ldots, P_m) \in \mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ with $P_1 + \cdots + P_m = P$ is called a *decomposition* of P with respect to the direct sum decomposition of K.

Let now V_i be defined as in the previous section. Then, under the isomorphism $E(K) \simeq \mathrm{Res}_k^K(E)(k)$, the set of decompositions of P corresponds to the set of tuples $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$ with $\sum_i P_i = P_\infty$ and $\mathrm{Res}_k^K(x)(P_i) \neq 0$. This is nothing but the set of k-rational points $(P_1, \ldots, P_m)$ of the fiber at P_∞ of the morphism

$$V_1 \times \cdots \times V_m \to \mathrm{Res}_k^K(E)$$

induced by the addition morphism on $\mathrm{Res}_k^K(E)$ with $\mathrm{Res}_k^K(x)(P_i) \neq 0$ for all i.

This leads to the next definition.

Definition 3.2. A decomposition $(P_1, \ldots, P_m)$ of P is called *isolated* if it corresponds to an isolated (k-rational) point of the fiber $(V_1 \times \cdots \times V_m)_{P_\infty}$ just considered.

The "new decomposition problem" is now the computational problem with the following specification: The input consists of a prime power q, a natural number n, an elliptic curve $E \subseteq \mathbb{P}^2_{\mathbb{F}_{q^n}}$ in Weierstraß form with respect to x and y and point at infinity as zero point, a direct sum decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{m} U_i$ of $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$-vector subspaces with $m \geq 2$ and a point $P \in E(\mathbb{F}_{q^n})$. The output consists of a list of decompositions of P with respect to the direct sum decomposition of $\mathbb{F}_{q^n}$, containing all isolated decompositions.

For the relation generation, the first crucial result is the following proposition. Furthermore, we need a nontrivial lower bound on the probability that a uniformly randomly distributed point in $E(\mathbb{F}_{q^n})$ has an isolated decomposition with respect to the chosen decomposition of K, given that certain conditions are satisfied. Such bounds are established in the next section.

Proposition 3.3. (a) *There exists an absolute constant $C > 0$ such that the number of isolated decompositions of some point $P \in E(\mathbb{F}_{q^n})$ is at most $e^{C \cdot mn}$.*

(b) *The "new decomposition problem" can be solved in an expected running time which is polynomially bounded in $e^{mn} \cdot \log(q)$.*

The rest of this section is devoted to the proof of this proposition.

We now give some background information on the idea of the algorithm and address claim (a). Computational aspects will be discussed later.

Let us fix an instance as specified in (b), and, as above, let $K|k$ be the extension of finite fields under consideration.

We first make the following assumption:

$$x(P) \notin \bigcup_{i=1}^{m} U_i.$$

At the end of the section we will discuss an easy modification of the following arguments and the algorithm for the case that $x(P) \in \bigcup_{i=1}^{m} U_i$.

The main idea is to use the isomorphism $E(K) \simeq \mathrm{Cl}^0(E)$. Let us use the following notation (cf. [Silverman 1986]): For $P \in E(K)$, the prime divisor defined by P is denoted by (P).

For points $P_1, \ldots, P_m \in E(K)$, we have $\sum_i P_i = P$ if and only if there exists a function $g \in K(E)^*$ with $(g) = (P_1) + \cdots + (P_m) + (-P) - (m+1) \cdot (O)$. Moreover, g is uniquely determined "up to a constant" by the points.

Let us assume that $P \neq O$. (For the case $P = O$, the following considerations can easily be modified.) Let $p_1 := 1$, $p_{2i} = x^i$, $p_{2i+1} := x^{i-1} y$ for $i \in \mathbb{N}$. Note that, for $\ell \in \mathbb{N}$, $(p_1)_{|E}, \ldots, (p_\ell)_{|E}$ is a basis of $L(\ell O)$. Let $L_\ell := \langle p_1, \ldots, p_\ell \rangle \cap \{ f \in k[x, y] \mid f(-P) = 0 \}$, and let $g_1, \ldots, g_m$ be a basis of L_{m+1} such that $g_1, \ldots g_{m-1}$ is a basis of L_m. Then $(g_1)_{|E}, \ldots, (g_m)_{|E}$ is a basis of $L((m+1) \cdot (O) - (-P))$ and $(g_m)_{|E} \notin L(m \cdot O - (-P))$. Now $(P_1, \ldots, P_m)$ is a decomposition of P if and only if there exists a tuple $(\alpha_1, \ldots, \alpha_{m-1}) \in K^{m-1}$ with

$$(g_m + \alpha_{m-1} g_{m-1} + \cdots + \alpha_1 g_1) = (P_1) + \cdots + (P_m) + (-P) - (m+1) \cdot (O). \quad (14)$$

Furthermore, there exists at most one such tuple $(\alpha_1, \ldots, \alpha_{m-1})$ in $\bar{k}^{m-1}$. The set of decompositions of P is thus in canonical bijection to the set of tuples $(\alpha_1, \ldots, \alpha_{m-1}, P_1, \ldots, P_m) \in K^{m-1} \times E_a^m(K)$ with $x(P_i) \in U_i - \{0\}$ such that (14)

holds. Note that in any such tuple the points $P_1, \ldots, P_m, P$ are distinct. (Recall that $x(P) \notin \bigcup_{i=1}^{m} U_i$ by assumption).

Let us recall that the defining polynomial of E_a is denoted by f. Let now

$$f_{(i)} := f(x_i, y_i) \in K[x_1, y_1, \ldots, x_m, y_m]$$

for all $i = 1, \ldots, m$; the scheme $V(f_{(1)}, \ldots, f_{(m)})$ is therefore equal to E_a^m in $\mathrm{Spec}(K[x_1, y_1, \ldots, x_m, y_m])$.

Let

$$h := g_m + a_{m-1} g_{m-1} + \cdots a_1 g_1 \in K[x, y, a_1, \ldots, a_{m-1}]$$

and let

$$h_{(i)} := g_m(x_i, y_i) + a_{m-1} g_{m-1}(x_i, y_i) + \cdots + a_1 g_1(x_i, y_i) \in K[a_1, \ldots, a_{m-1}, x_1, y_1 \ldots, x_m, y_m]$$

for all $i = 1, \ldots, m$.

The set of decompositions of P is then in canonical bijection to the set of K-rational points $(\alpha_1, \ldots, \alpha_{m-1}, P_1, \ldots, P_m)$ of the scheme $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$ in $\mathrm{Spec}(K[a_1, \ldots, a_{m-1}, x_1, y_1, \ldots, x_m, y_m])$ with $x(P_i) \in U_i - \{0\}$ for all i. Note that we have the canonical projection

$$V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)}) \to V(f_{(1)}, \ldots, f_{(m)}) = E_a^m,$$

given on Z-valued points for any k-scheme Z by

$$(\alpha_1, \ldots, \alpha_{m-1}, P_1, \ldots, P_m) \mapsto (P_1, \ldots, P_m).$$

It is natural to pass to the Weil restriction of $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$ here. Let us first fix some notations: Let W be defined by the diagram

$$\begin{array}{ccc} W & \hookrightarrow & \mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})) \\ \downarrow & & \downarrow \\ V_1 \times \cdots \times V_m & \hookrightarrow & (\mathrm{Res}_k^K(E_a))^m \\ \downarrow & & \downarrow \\ \mathbb{A}_k[U_1] \times \cdots \times \mathbb{A}_k[U_m] & \hookrightarrow & \mathbb{A}_k[K] \end{array}$$

being Cartesian. Now the k-rational points of W correspond exactly to the K-rational points $(\alpha_1, \ldots, \alpha_{m-1}, P_1, \ldots, P_m)$ of $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$ with $P_i \in U_i$.

We now give an explicit description of W via a polynomial system. This description will serve as a basis for the algorithm.

Let $b_1, \ldots, b_n$ be a k-basis of K. (In the algorithm, such a basis is given with the input.) With this basis, we now identify K with k^n and also $\mathbb{A}_k[K]$ with $\mathbb{A}_k^n$. Moreover, for $i = 1, \ldots, m$, let $b_{i,1}, \ldots, b_{i,\dim(U_i)}$ be a basis of U_i. The scheme $W \subseteq \mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)}))$ can be described explicitly as follows: Let the polynomials $h_{(i),j}$ and $f_{(i),j}$ for $i = 1, \ldots, m$, $j = 1, \ldots, n$ in $k[(a_{\ell,j'})_{\ell=1,\ldots,m-1,\, j'=1,\ldots,n}, ((x_{i',j'})_{j'=1,\ldots,\dim(U_i)}, (y_{i',j'})_{j'=1,\ldots,n})_{i'=1,\ldots,m}]$ be defined by

$$h_{(i)}\left(\left(\sum_{j'=1}^{n} a_{\ell,j'}b_{j'}\right)_{\ell=1,\ldots,m-1}, \sum_{j'=1}^{\dim(U_i)} x_{i,j'}b_{j'}, \sum_{j'=1}^{n} y_{i,j'}b_{j'}\right) = \sum_{j=1}^{n} h_{(i),j}b_j,$$

$$f_{(i)}\left(\sum_{j'=1}^{\dim(U_i)} x_{i,j'}b_{i,j'}, \sum_{j'=1}^{n} y_{i,j'}b_{j'}\right) = \sum_{j'=1}^{n} f_{(i),j}b_j.$$

We have isomorphisms

$$V_i \simeq V((f_{(i),j})_{j=1,\ldots,n}) \subseteq \mathrm{Spec}(k[x_{i,1}, \ldots, x_{i,\dim(U_i)}, y_{i,1}, \ldots, y_{i,n}])$$

and

$$W \simeq V\big((f_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n}, (h_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n}\big)$$

(which are canonical for the chosen basis).

The k-rational points of $V((f_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n}, (h_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n})$ correspond in an obvious way to the K-rational points $(a_1, \ldots, a_{m-1}, P_1, \ldots, P_m)$ of $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$ with $x(P_i) \in U_i$. Such points with $x(P_i) \in U_i - \{0\}$ then correspond to the decompositions of P.

We have a polynomial system in $2mn$ variables and $2mn$ equations.

We want to obtain a suitable polytope which contains the exponents in the support of the system.

Let us first consider the total degrees of $h_{(i),j}$ and $f_{(i),j}$ with respect to the three systems of variables $(a_{\ell,j'})_{\ell,j'}$, $(x_{i',j'})_{i',j'}$ and $(y_{i,j'})_{i,j'}$. Concerning the $h_{(i),j}$ we have: the total degree with respect to the $a_{\ell,j'}$ is at most 1; the total degree with respect to the $x_{i',j'}$ is at most $\lfloor m/2 \rfloor$; the total degree with respect to the $y_{i',j'}$ is at most 1. Concerning the $f_{(i),j}$ we have: the total degree with respect to the $x_{i',j'}$ is at most 3; the total degree with respect to the $y_{i',j'}$ is at most 2.

We now consider the $a_{\ell,j'}$ and the $y_{i',j'}$ as one system of variables and the $x_{i',j'}$ as another system of variables. So we have $2 \cdot (m-1) \cdot n$ variables in the first system and the total degrees of all polynomials under consideration with respect to this system are at most 2. Furthermore, we have n variables in the second system and the total degrees with respect to this system are at most $\max(3, \lfloor m/2 \rfloor)$.

Let $\Delta_\ell := \{\underline{x} \in \mathbb{R}^\ell_{\geq 0} \mid \sum_i x_i \leq 1\}$. With a suitable numeration, the exponents are contained in the polytope

$$\boldsymbol{P} := 2 \cdot \Delta_{(2m-1)\cdot n} \times \max\left(3, \left\lfloor \frac{m}{2} \right\rfloor\right) \cdot \Delta_n.$$

The toric variety $\mathcal{T}(\boldsymbol{P})$ defined by this polytope is $\mathbb{P}_k^{(2m-1)\cdot n} \times \mathbb{P}_k^n$. The volume of the polytope is $2^{(2m-1)\cdot n}/((2m-1)\cdot n)! \cdot \max(3, \lfloor m/2 \rfloor)^n / n!$. The system of equations defines a system of sections of a line bundle on $\mathcal{T}(\boldsymbol{P})$, and the degree of the 0-cycle in the Chow ring of $\mathcal{T}(\boldsymbol{P})$ defined by this system is $(2mn)!$ times the volume of the polytope; that is,

$$2^{(2m-1)\cdot n} \cdot \max\left(3, \left\lfloor \frac{m}{2} \right\rfloor\right)^n \cdot \binom{2mn}{n} < 2^{(2m-1)\cdot n} \cdot \max\left(3, \left\lfloor \frac{m}{2} \right\rfloor\right)^n \cdot 2^{2mn} < 2^{4mn} \cdot \max\left(3, \frac{m}{2}\right)^n.$$

Therefore the scheme defined by the sections on $\mathcal{T}(\boldsymbol{P})$ associated to the equations has at most $2^{4mn} \cdot \max(3, m/2)^n$ isolated $\bar{k}$-rational points. We have a natural embedding of $\mathbb{A}_k^{2mn}$ into $\mathcal{T}(\boldsymbol{P})$, and the sections restrict to the equations under this embedding. Thus the scheme $V((f_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n}, (h_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n})$ has at most $2^{4mn} \cdot \max(3, m/2)^n \in e^{\mathcal{O}(mn)}$ isolated $\bar{k}$-rational points.

Let us now turn to algorithmic aspects: It is straightforward to compute a system $(f_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n}$, $(h_{(i),j})_{i=1,\ldots,m,\, j=1,\ldots,n}$ as above. We then use Rojas' algorithm [1999] for sparse polynomial systems to determine all isolated k-rational solutions. The input and output structure as well as the running time of the algorithm are given in [ibid., Main Theorem 2.1]; all the following statements on the algorithm refer to this theorem.

We apply the algorithm with the system of equations and the polytope $\boldsymbol{P}$ defined above. The output of the algorithm is a system of univariate polynomials $h, h_1, \ldots, h_{2mn}$, the degrees of which are all bounded by the degree of the 0-cycle defined by the given system of sections in the Chow ring of $\mathcal{T}(\boldsymbol{P})$ and thus by $2^{4mn} \cdot \max(3, m/2)^n$. By factoring h and applying the system $h_1, \ldots, h_{2mn}$ to the rational roots, we obtain a list of points in k^{2mn}. This list consists of solutions to the system and contains all isolated k-rational solutions of the system on $\mathbb{A}_k^{2mn}$.

The running time of Rojas' algorithm is polynomially bounded in $e^{m\cdot n} \cdot \log(q)$, and in an expected time which is also polynomially bounded in $e^{m\cdot n} \cdot \log(q)$ we can factor the univariate polynomial h. Explicitly, the running time of Rojas' algorithm depends on mixed volumes of various systems of polytopes, all of which are contained in the polytope $\boldsymbol{P}$. Therefore these mixed volumes are also bounded by $2^{4mn} \cdot \max(3, m/2)^n$.

We obtain the following intermediate result:

Lemma 3.4.

(a) *A system* $(f_{(i),j})_{i=1,\ldots,m,\,j=1,\ldots,n}$, $(h_{(i),j})_{i=1,\ldots,m,\,j=1,\ldots,n}$ *as above has* $e^{\mathcal{O}(mn)}$ *isolated* k*-rational solutions.*

(b) *Given an instance of the "new decomposition problem", one can compute a system* $(f_{(i),j})_{i=1,\ldots,m,\,j=1,\ldots,n}$, $(h_{(i),j})_{i=1,\ldots,m,\,j=1,\ldots,n}$ *as above and a list of* k*-rational solutions, containing all isolated* k*-rational solutions, in an expected time which is polynomially bounded in* $e^{mn} \cdot \log(q)$.

This is however not yet the statement we want to prove. Indeed, we still have to show that in this way we can obtain a list of decompositions of P which contains all isolated decompositions.

Let $P \in E_a(K)$.

We first study the geometric fibers of the morphism

$$V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)}) \to V(f_{(1)}, \ldots, f_{(m)}) = E_a^m.$$

Let $(P_1, \ldots, P_m) \in E_a^m(\bar{k})$ such that the points $P_1, \ldots, P_m, P_\oplus$ are distinct. Then there is at most one tuple $(\alpha_1, \ldots, \alpha_{m-1}) \in \bar{k}^m$ such that (14) holds, depending on whether $\sum_i P_i = P_\oplus$ or not.

Let now D be the closed subscheme of E_a^m given on Z-valued points for any k-scheme Z by

$$D(Z) = \{(P_1, \ldots, P_m) \in E_a^m(Z) \mid \exists i \neq i' : P_i = P_{i'} \text{ or } \exists i : P_i = P\}.$$

Let $T := E_a^m - D$ and let S be the preimage of T in $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$. Now the morphism $S \to T$ induces an injection on the sets of geometric points and its image consists of those points $(P_1, \ldots, P_m) \in E_a^m(\bar{k})$ with $\sum_i P_i = P_\oplus$.

We consider the restriction of the m-fold addition morphism $E^m \to E$ to T. Following the usual notation, let T_P be the fiber of this morphism at P. This is an open subscheme of a scheme isomorphic to E^{m-1}.

The morphism $S \to T$ induces a bijection $S(\bar{k}) \to T_P(\bar{k})$. As T_P is reduced, we have an induced morphism $S \to T_P$.

We now pass to Weil restrictions. Note first that we again have the addition $\mathrm{Res}_k^K(E)^m \to \mathrm{Res}_k^K(E)$ and the fiber $(\mathrm{Res}_k^K(E)^m)_{P_\oplus}$.

We have a canonical open embedding

$$\mathrm{Res}_k^K(T) \subseteq \mathrm{Res}_k^K(E_a^m) \simeq \left(\mathrm{Res}_k^K(E_a)\right)^m.$$

Note that, under the canonical isomorphism $\mathrm{Res}_k^K(E_a)^m(k) \simeq E_a^m(K)$, the points of $\mathrm{Res}_k^K(T)(k)$ correspond to the points $(P_1, \ldots, P_m) \in E^m(K)$ which are contained in $T(K)$, that is, to points $(P_1, \ldots, P_m) \in E^m(K)$ such that the points $P_1, \ldots, P_m, P$ are distinct.

Let

$$V^* := (V_1 \times \cdots \times V_m) \cap \mathrm{Res}_k^K(T) \subseteq \left(\mathrm{Res}_k^K(E_a)\right)^m$$

and let $V^*_{P_\circledcirc}$ be the fiber of $P_\circledcirc$ under the restriction of the addition morphism $\mathrm{Res}_k^K(E)^m \to \mathrm{Res}_k^K(E)$ to V^*. We have

$$V^*_{P_\circledcirc} = V^* \cap \left(\mathrm{Res}_k^K(E_a)^m\right)_{P_\circledcirc} = V^* \cap \mathrm{Res}(T)_{P_\circledcirc}. \tag{15}$$

Let now $P \notin \bigcup_{i=1}^m U_i$. The set of k-rational points of V^* contains all k-rational points of $\mathrm{Res}_k^K(E_a)^m$ corresponding to decompositions of P. (There might be more points in $V^*(k)$ because there might be k-rational points $(P_1, \ldots, P_m)$ of V^* with $x_i(P) = 0$ for some $i \in \{1, \ldots, m\}$.) As $\mathrm{Res}_k^K(T)$ is open in $\mathrm{Res}_k^K(E_a)^m$, a k-rational point of $V_1^* \times \cdots \times V_m^*$ is open in $V_1^* \times \cdots \times V_m^*$ if and only if it is open in $V_1 \times \cdots \times V_m$. Therefore, the set of isolated k-rational points of V^* contains all k-rational points of $\mathrm{Res}_k^K(E_a)^m$ corresponding to isolated decompositions of P.

Let W^* be the preimage of V^* in $\mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)}))$. Our goal is to show that the preimages of the isolated k-rational points of V^* are isolated k-rational points of W^*.

We have the Cartesian diagram

$$\begin{array}{ccc} \mathrm{Res}_k^K(S) & \hookrightarrow & \mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})) \\ \downarrow & & \downarrow \\ \mathrm{Res}_k^K(T) & \hookrightarrow & \mathrm{Res}_k^K(E_a^m) \simeq \mathrm{Res}_k^K(E_a)^m. \end{array}$$

Moreover, as the morphism $S \to T$ factors through the fiber T_P, by functoriality, the morphism $\mathrm{Res}_k^K(S) \to \mathrm{Res}_k^k(T)$ factors through the fiber $\mathrm{Res}_k^K(T)_{P_\circledcirc}$. We claim that we have an induced bijection between $\mathrm{Res}_k^K(S)(\bar{k})$ and $\mathrm{Res}_k^K(T)_{P_\circledcirc}(\bar{k})$. For this, we can (obviously) apply the base change to $\bar{k}|k$. But over $\bar{k}$, the two Weil restrictions become products of Galois twists of S and T, respectively, and we have already shown the claim for the factors of the product. The claim thus follows. By considering the Galois operation, we obtain that, for every algebraic field extension $\lambda|k$, we have a bijection between $\mathrm{Res}_k^K(S)(\lambda)$ and $(\mathrm{Res}_k^k(T))_{P_\circledcirc}(\lambda)$. We are going to use this for $\lambda = k$.

As V^* is contained in $\mathrm{Res}_k^K(T)$, W^* is contained in $\mathrm{Res}_k^K(S)$, and we have a Cartesian diagram

$$\begin{array}{ccc} W^* & \hookrightarrow & \mathrm{Res}_k^K(S) \\ \downarrow & & \downarrow \\ V^* & \hookrightarrow & \mathrm{Res}_k^K(T). \end{array}$$

The composition $W^* \to \mathrm{Res}_k^K(T)$ (obviously) factors through V^* and — as we have just seen — it factors through $(\mathrm{Res}_k^K(T))_{P_\infty}$. By (15) it factors through $V^*_{P_\infty}$. The morphism

$$W^* \to V^*_{P_\infty}$$

again induces a bijection

$$W^*(k) \to V^*_{P_\infty}(k).$$

Let now $(P_1, \ldots, P_m)$ be an isolated k-rational point of V^*. This is a k-rational point of V^* which is open in V^*. Then the fiber over $(P_1, \ldots, P_m)$ in W^* is open in W^*, and it is a k-rational point. Therefore it is an isolated k-rational point of W^* and also of W.

We note again that for any isolated decomposition of P the corresponding point in $(V_1 \times \cdots \times V_m)(k)$ lies in $V^*(k)$ and is isolated. Therefore every isolated decomposition of P defines an isolated k-rational point of W.

This finishes the proof of Proposition 3.3 under the assumption $x(P) \notin \bigcup_{i=1}^m U_i$.

Modification for $x(P) \in \bigcup_{i=1}^m U_i$. We now discuss the modification for the case that $x(P) \in \bigcup_{i=1}^m U_i$. Except for finitely many instances, there exists a point $R \in E_a(K)$ with $x(R) \notin \bigcup_{i=1}^m U_i$ and $x(P-R) \notin \bigcup_{i=1}^m U_i$.

Let us fix such a point R and let $S := P - R$. Let $\tilde{L}_\ell := \langle p_1, \ldots, p_\ell \rangle \cap \{f \in k[x,y] \mid f(-R) = 0, f(-S) = 0\}$. Let $\tilde{g}_1, \ldots, \tilde{g}_m$ be a basis of $\tilde{L}_{m+2}$ such that $\tilde{g}_1, \ldots, \tilde{g}_{m-1}$ is a basis of L_{m+1}. Now a tuple $(P_1, \ldots, P_m) \in \mathfrak{F}_1 \times \cdots \times \mathfrak{F}_m$ is a decomposition of P if and only if there exists a tuple $(\alpha_1, \ldots, \alpha_{m-1}) \in K^{m-1}$ with

$$(\tilde{g}_m + \alpha_{m-1}\tilde{g}_{m-1} + \cdots + \alpha_1 \tilde{g}_1) = (P_1) + \cdots + (P_m) + (-R) + (-S) - (m+1)\cdot(O).$$

Moreover, if such a tuple exists, it is unique. With this modifications, we obtain again the desired bound on the number of isolated decompositions. Moreover, by choosing a point $R \in E_a(K)$ uniformly randomly, we also obtain the algorithmic result. Note here that, if P is in the factor base, we immediately have a relation, so we do not need to apply the decomposition algorithm. The bound on the number of isolated decompositions will however be used later.

4. Analysis and the final result

Let $K|k$ and E/K be as above and $m \in \mathbb{N}$ with $2 \le m \le n/2$. We assume that Condition 2.1 is satisfied. Furthermore, let a decomposition $K = \bigoplus_{i=1}^m U_i$ be given which satisfies the conditions in Section 2E. Moreover, let $\mathfrak{F}_i$ and V_i be as above.

As in Section 2C, let $P_0 \in E(K)$ be one of the two points in $E(K)$ lying over 0.

We want to obtain a lower bound on the number of points $P \in E(K)$ which have isolated decompositions. For this goal, we first want to derive an upper bound

on the number of tuples $(P_1, \dots, P_m) \in \mathscr{F}_1 \times \cdots \times \mathscr{F}_m$ which define nonisolated decompositions.

Let $a_m : \mathrm{Res}_k^K(A) \to \mathrm{Res}_k^K(E)$ be the m-fold addition morphism and $a'_m : V_1 \times \cdots \times V_m \to \mathrm{Res}_k^K(E)$ the restriction of a_m to $V_1 \times \cdots \times V_m$.

We now consider a point $(P_1, \dots, P_m) \in E^m(K)$ with $x(P_i) \in U_i$ and let $P := \sum_{i=1}^m P_i$.

The morphism $a'_m : V_1 \times \cdots \times V_m \to \mathrm{Res}_k^K(E)$ is unramified at $((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)$ if and only if $((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)$ is an isolated reduced point of the fiber at $P_\circledcirc$. We ask ourselves for which tuples $(P_1, \dots, P_m)$ as above the morphism is ramified at $((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)$. As already pointed out in the proof of Proposition 2.2 the morphism $a'_m : V_1 \times \cdots \times V_m \to \mathrm{Res}_k^K(E)$ is unramified at $((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)$ if and only if the induced map on tangent spaces

$$(a'_m)_* : T_{((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)}(V_1 \times \cdots \times V_m) \to T_{P_\circledcirc}(V_1 \times \cdots \times V_m)$$

is injective.

We now consider points $(P_1, \dots, P_m) \in E(K)^m$ with $x(P_i) \in U_i$ for all i which satisfy the following condition.

Condition 4.1. The flat covering $x_{|E}$ is unramified at $P_1, \dots, P_m$.

This condition is equivalent to the condition that, for every i, the flat covering $\mathrm{Res}_k^K(E_a) \to \mathrm{Res}_k^K(\mathbb{A}_k^1)$ is unramified at $(P_i)_\circledcirc$. By base change, this implies that, for every i, $V_i \to \mathbb{A}_k[U_i]$ is unramified (and thus étale) at $(P_i)_\circledcirc$. Therefore, V_i is smooth at $(P_i)_\circledcirc$ and we have an isomorphism of tangent spaces $T_{(P_i)_\circledcirc}(V_i) \to T_{(x(P_i))_\circledcirc}(\mathbb{A}_k[U_i])$.

Let such a point $(P_1, \dots, P_m)$ be given and let again $P := \sum_{i=1}^m P_i$. By Lemma 2.4 we have a commutative diagram

$$\begin{array}{ccc}
T_{((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)}(V_1 \times \cdots \times V_m) & \xrightarrow{(a'_m)_*} & T_{P_\circledcirc}\big(\mathrm{Res}_k^K(E)\big) \\
\downarrow{\scriptstyle (\tau_{(P_0-P_1)_\circledcirc, \dots, (P_0-P_m)_\circledcirc})_*} & & \downarrow{\scriptstyle (\tau_{m\cdot(P_0-P)_\circledcirc})_*} \\
T_{((P_0)_\circledcirc, \dots, (P_0)_\circledcirc)}(V_1 \times \cdots \times V_m) & \xrightarrow{(a'_m)_*} & T_{m(P_0)_\circledcirc}\big(\mathrm{Res}_k^K(E)\big) \\
\downarrow & & \uparrow{\scriptstyle (\tau_{(m-1)\cdot(P_0)_\circledcirc})_*} \\
T_{(P_0)_\circledcirc}(V_1) \times \cdots \times T_{(P_0)_\circledcirc}(V_m) & \longrightarrow & T_{(P_0)_\circledcirc}\big(\mathrm{Res}_k^k(E)\big)
\end{array}$$

where the lower map is the addition on tangent spaces. Moreover, by the proof of Proposition 2.2, the two lower vertical homomorphisms are isomorphisms. Under the isomorphism $T_{(P_1)_\circledcirc}(V_1) \times \cdots \times T_{(P_m)_\circledcirc}(V_m) \simeq T_{((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)}(V_1 \times \cdots \times V_m)$,

the horizontal map on the left-hand side is

$$(\tau_{(P_0-P_1)_\circledcirc})_* \times \cdots \times (\tau_{(P_0-P_m)_\circledcirc})_* : \\ T_{(P_1)_\circledcirc}(V_1) \times \cdots \times T_{(P_m)_\circledcirc}(V_m) \to T_{(P_0)_\circledcirc}(V_1) \times \cdots \times T_{(P_0)_\circledcirc}(V_m).$$

So the morphism $(a'_m)_*$ is unramified at $((P_1)_\circledcirc, \ldots, (P_m)_\circledcirc)$ if and only if we have a direct sum decomposition

$$T_{(P_0)_\circledcirc}\left(\mathrm{Res}_k^K(E)\right) = \bigoplus_{i=1}^{m} (\tau_{(P_0-P_i)_\circledcirc})_*(T_{(P_i)_\circledcirc}(V_i)). \tag{16}$$

We want to derive a condition under which we do have such a decomposition. For this, we distinguish between three cases: q odd; q even and $j \neq 0$; and q even and $j = 0$.

The case that q is odd. We need some facts on tangent vectors of the projective line and the elliptic curve E. Here and in the following we assume that the defining polynomial f of E_a is of the form $y^2 - v(x)$ (with v monic of degree 3).

Following our usual notation, let $\mathbb{P}^1_K := \mathrm{Proj}(K[X, Y])$. We set $x_{\mathbb{P}^1} := X/Y \in K(\mathbb{P}^1)$ (such that $K(\mathbb{P}^1) = K(x_{\mathbb{P}^1})$).

On $\mathbb{P}^1_K$, we have the meromorphic cotangent vector field $dx_{\mathbb{P}^1}$ with divisor -2∞. Under duality, this corresponds to a tangent vector field which we denote by $t_{\mathbb{P}^1} \in \Gamma(\mathbb{P}^1_k, \mathcal{T}_{\mathbb{P}^1_k})$ and which has divisor 2∞.

Let R be the ramification divisor of the covering $x_{|E}$. Then the meromorphic cotangent vector field $dx_{|E}$ has divisor $-4(O) + R$, and we have the holomorphic cotangent vector field $dx_{|E}/y_{|E}$. This field is invariant under translation; that is, for every translation τ of E we have $\tau^*(dx_{|E}/y_{|E}) = dx_{|E}/y_{|E}$.

Again under duality, $dx_{|E}$ corresponds to a meromorphic tangent vector field; we denote this by t_E. It has divisor $4(O) - R$. So we have the holomorphic tangent vector field $y_E t_E$, which corresponds to $dx_{|E}/y_{|E}$ under duality. Moreover, the field $y_E t_E$ is also invariant under translation; that is, for every translation τ of E, $\tau_*(y_{|E} t_E) = y_{|E} t_E$.

Following the notation fixed in the introduction, for some point $P \in E(K)$, we denote the tangent vector in $T_P(E)$ induced by t_E by $t_E(P)$.

Let two K-rational points P_0 and P_1 of E which are not ramification points under $x_{|E}$ be given and let us consider the homomorphism $(\tau_{P_0-P_1})_* : T_{P_1}(E) \to T_{P_0}(E)$. This homomorphism is given by $y(P_1)t_E(P_1) \mapsto y(P_0)t_E(P_0)$; that is,

$$t_E(P_1) \mapsto \frac{y(P_0)}{y(P_1)} t_E(P_0). \tag{17}$$

As in the previous section, Let us fix a basis $(b_j)_j$ of K over k and bases $(b_{i,j})_j$ of the U_i. Let us denote the corresponding dual bases by $(x_j)_j$ and $(x_{i,j})_j$. The

bases $(b_j)_j$ and $(b_{i,j})_j$ define bases of the spaces $\Gamma(\mathbb{A}_k[K], \mathcal{T})$ and $\Gamma(\mathbb{A}_k[U_i], \mathcal{T})$. We denote these bases by $(t_j)_{j=1,\dots,n}$ for $\mathbb{A}_k[K]$ and $(t_{i,j})_{j=1,\dots,\dim(U_i)}$ for $\mathbb{A}_k[U_i]$.

Let $P \in E(K)$ such that $x_{|E}$ is unramified at P. Then $\mathrm{Res}_k^K(x_{|E_a})$ defines an isomorphism of tangent spaces $(\mathrm{Res}_k^K(x_{|E_a}))_* : T_{P_\circledcirc}(\mathrm{Res}_k^K(x_{|E_a})) \to T_{x(P)_\circledcirc}(\mathbb{A}[K])$. Now, for $t \in \Gamma(\mathbb{A}[K], \mathcal{T})$, we define $t(P_\circledcirc) := ((\mathrm{Res}_k^K(x_{|E_a}))_*)^{-1}(t(x(P)_\circledcirc))$. The isomorphism of tangent vector spaces restricts to an isomorphism of tangent vector spaces $T_{P_\circledcirc}(V_i) \to T_{x(P)_\circledcirc}(\mathbb{A}[U_i])$. Thus $t(P_\circledcirc)$ is in $T_{P_\circledcirc}(V_i)$ if and only if $t(x(P)_\circledcirc)$ is in $T_{x(P)_\circledcirc}(\mathbb{A}[U_i])$.

Just as the bases $(t_j(x(P)_\circledcirc))_j$ and $(d(x_j)(x(P)_\circledcirc))_j$ are dual to each other, so are the bases $(t_j(P_\circledcirc))_j$ and $(d(x_j)_{|\mathrm{Res}_k^K(E_a)}(P_\circledcirc))_j$.

Let A_i be the coordinate matrix of $(b_{i,j})_j$ with respect to $(b_j)_j$. Then this is also the coordinate matrix of $(t_{i,j})_j$ with respect to $(t_j)_j$, and, for any $P \in E(K)$ as above, it is also the coordinate matrix of $(t_{i,j}(P_\circledcirc))_j$ with respect to $(t_j(P_\circledcirc))_j$. For the following, it is important that the matrix does not depend on P.

Let now $(P_1, \dots, P_m) \in E^m(K)$ with $x(P_i) \in U_i$ for all i satisfy Condition 4.1. Then, for each $i = 1, \dots, m$, the system $(t_{i,j}((P_i)_\circledcirc))_j$ is a basis of the k-vector space $T_{(P_i)_\circledcirc}(V_i)$. We have a direct sum decomposition of $T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E))$ as in (16) if and only if the elements $(t_{(P_0-P_i)_\circledcirc})_*(t_{i,j}((P_i)_\circledcirc))$ for $i = 1, \dots, m$, $j = 1, \dots, \dim(U_i)$ form a k-basis of $T_{P_\circledcirc}(\mathrm{Res}_k^K(E))$.

Let, for $j = 0, \dots, n-1$, $f_j \in k[x_1, \dots, x_n, y_1, \dots, y_n]$ be defined by $f = \sum_{j=1}^n b_j \cdot f_j$. Let $u : (\mathrm{Res}_k^K(E_a))_K \to E_a$ be the universal morphism. We have the isomorphism

$$(u, \sigma(u), \dots, \sigma^{n-1}(u)) : \left(\mathrm{Res}_k^K(E_a)\right)_K \xrightarrow{\sim} \prod_{s=0}^{n-1} \sigma^s_{K|k}(E_a) \tag{18}$$

corresponding to the isomorphism of K-algebras

$$\bigotimes_{s=0}^{n-1} K[x^{(s)}, y^{(s)}]/\left(\sigma^s_{K|k}(f)(x^{(s)}, y^{(s)})\right) \xrightarrow{\sim} K[x_1, \dots, x_n, y_1, \dots, y_n]/(f_1, \dots, f_n),$$

$$x^{(s)} \mapsto \sum_{j=1}^n \sigma^s_{K|k}(b_j) \cdot x_j, \quad y^{(s)} \mapsto \sum_{j=1}^n \sigma^s_{K|k}(b_j) \cdot y_j.$$

Note that, for $P \in E(K)$, under isomorphism (18) the point $P_\circledcirc \in \mathrm{Res}_k^k(E)(k) \subseteq \mathrm{Res}_k^K(E)(K)$ corresponds to the point $(\sigma^s(P))_{s=0,\dots,n-1} \in \prod_{s=0}^{n-1} \sigma^s_{K|k}(E_a)(K)$.

We have an induced isomorphism $\Gamma(\mathrm{Res}_k^K(E_a)_K, \Omega) \simeq \bigoplus_{s=0}^{n-1} \Gamma(\sigma^s(E_a), \Omega)$ under which $d(x^{(s)})_{|\sigma^s(E_a)}$ corresponds to $\sum_{j=1}^n \sigma^s_{K|k}(b_j) \cdot d(x_j)_{|\mathrm{Res}_k^K(E_a)}$. This isomorphism induces an isomorphism between the cotangent spaces at $P_\circledcirc$ and $(\sigma^s(P))_{s=0,\dots,n-1}$. Let again $x_{|E}$ be unramified at P. If we then apply the duality between cotangent and tangent spaces, we obtain that $t_j(P_\circledcirc)$ corresponds to

$\left(\sigma^s_{K|k}(b_j)\cdot t_{\sigma^s(E_a)}(\sigma^s(P))\right)_{s=0,\dots,n-1}$ under the induced isomorphism of tangent spaces at $P_\odot$ and $(\sigma^s(P))_{s=0,\dots,n-1}$.

On each of the factors of the product $\prod_{s=0}^{n-1}\sigma^s_{K|k}(E_a)$, we can apply the considerations above. We obtain that $(\tau_{(P_0-P_i)_\odot})_*(t_j((P_i)_\odot))$ corresponds to

$$\begin{aligned}&\left((\tau_{(\sigma(P_0)-\sigma(P_i))})_*(\sigma^s_{K|k}(b_j)\cdot t_{\sigma^s(E_a)}(\sigma^s(P_0)))\right)_{s=0,\dots,n-1}\\ &\quad=\left(\sigma^s_{K|k}(b_j)\cdot\frac{y^{(s)}(\sigma(P_0))}{y^{(s)}(\sigma(P_i))}\cdot t_{\sigma^s(E_a)}(\sigma^s(P_0))\right)_{s=0,\dots,n-1}\\ &\quad=\left(\sigma^s_{K|k}(b_j)\cdot\frac{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_\ell((P_0)_\odot)}{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_\ell((P_i)_\odot)}\cdot t_{\sigma^s(E_a)}(\sigma^s(P_0))\right)_{s=0,\dots,n-1}.\end{aligned}$$

This vector is of course invariant under the Galois operation of $K|k$. Let C be the inverse of the matrix $((\sigma^s(b_j)))_{s=0,\dots,n-1,\,j=1,\dots,n}$; this is a matrix of the form $((\sigma^s(c_u)))_{u=1,\dots,n,\,s=0,\dots,n-1}$. Going back, we have

$$\begin{aligned}&(\tau_{(P_0-P_i)_\odot})_*(t_j((P_i)_\odot))\\ &\quad=\sum_{s=0}^{n-1}\sigma^s_{K|k}(b_j)\cdot\frac{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_\ell((P_0)_\odot)}{\sum_{\ell=1}^s\sigma^s_{K|k}(b_\ell)\cdot y_\ell((P_i)_\odot)}\cdot\left(\sum_{u=1}^n\sigma^s(c_u)(t_u((P_0)_\odot))\right)\\ &\quad=\sum_{u=1}^n\sum_{s=0}^{n-1}\sigma^s_{K|k}\left(b_j\cdot\frac{\sum_{\ell=1}^n b_\ell\cdot y_\ell((P_0)_\odot)}{\sum_{\ell=1}^s b_\ell\cdot y_\ell((P_i)_\odot)}\cdot c_u\right)\cdot(t_u(P_0)_\odot).\end{aligned}$$

Let $c_{j,u}:=b_jc_u\cdot\left(\sum_{\ell=1}^n b_\ell\cdot y_\ell(P_0)_\odot\right)\in K$. (These constants are independent of $P_1,\dots,P_m$.) Then

$$(\tau_{(P_0-P_i)_\odot})_*(t_j((P_i)_\odot))=\sum_{u=1}^n\sum_{s=0}^{n-1}\sigma^s_{K|k}\left(\frac{c_{j,u}}{\sum_{\ell=1}^n b_\ell\cdot y_\ell((P_i)_\odot)}\right)\cdot t_u((P_0)_\odot).$$

Let $\iota_i:V_i\hookrightarrow\mathrm{Res}^K_k(E)$ be the immersions. It follows that there are constants $c_{i,j,u}\in K$ (again independent of $P_1,\dots,P_m$) with

$$\begin{aligned}&\left((\tau_{(P_0-P_i)_\odot})_*\circ(\iota_i)_*\right)t_{i,j}((P_i)_\odot)\\ &\qquad=\sum_{u=1}^n\sum_{s=0}^{n-1}\sigma^s_{K|k}\left(\frac{c_{i,j,u}}{\sum_{\ell=1}^n b_\ell\cdot y_{i,\ell}((P_i)_\odot)}\right)\cdot t_u((P_0)_\odot)\\ &\qquad=\sum_{u=1}^n\sum_{s=0}^{n-1}\left(\frac{\sigma^s_{K|k}(c_{i,j,u})}{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_{i,\ell}((P_i)_\odot)}\right)\cdot t_u((P_0)_\odot).\end{aligned}$$

Let

$$M_0 := \left(\left(\sum_{s=0}^{n-1} \frac{\sigma_{K|k}^s(c_{i,j,u})}{\sum_{\ell=1}^n \sigma_{K|k}^s(b_\ell)\cdot y_{i,\ell}}\right)\right)_{u=1,\dots,n,\,(i=1,\dots,m,\,j=1,\dots,\dim(U_i))}$$
$$\in k((y_{i',j'})_{i'=1,\dots,m,\,j'=1,\dots,n})^{\{1,\dots,n\}\times\bigcup_{i=1}^m\bigcup_{j=1}^{\dim(U_i)}\{(i,j)\}}.$$

Note here that as indicated M_0 is a matrix over $k((y_{i',j'})_{i'=1,\dots,m,\,j'=1,\dots,n}$ because the entries are invariant under the Galois operation. The matrix has the size $n\times n$. It is however more convenient to use the indicated indices for the columns. Note further that, for no $(P_1,\dots,P_m)\in E^m(K)$ with $x(P_i)\in U_i$ for all i satisfying Condition 4.1 and for no i,s, $\sum_{\ell=1}^n \sigma^s(b_\ell)\cdot y_{i,\ell}$ vanishes at $((P_1)_\circledcirc,\dots,(P_n)_\circledcirc)$.

We have a direct sum decomposition of $T_0(\mathrm{Res}_k^K(E))$ as in (16) if and only if the matrix $M_0((P_1)_\circledcirc,\dots,(P_n)_\circledcirc)$ is nonsingular.

By Proposition 2.2 we know that this matrix is nonsingular for $(P_1,\dots,P_n)=(P_0,\dots,P_0)$. In particular, the matrix M_0 itself is nonsingular.

We now multiply the columns of M by polynomials such that the entries of the resulting matrix are polynomials. Concretely, we multiply all columns with column index (i,j) with the polynomial $\prod_{t=0}^{n-1}\left(\sum_{\ell=1}^n \sigma_{K|k}^t(b_\ell)\cdot y_{i,\ell}\right)$. The resulting matrix is

$$M = \left(\left(\sum_{s=0}^{n-1}\sigma_{K|k}^s(c_{i,j,u})\cdot\prod_{\substack{t=0\\t\neq s}}^{n-1}\left(\sum_{\ell=1}^n \sigma_{K|k}^t(b_\ell)\cdot y_{i,\ell}\right)\right)\right)_{\substack{u=1,\dots,n,\\(i=1,\dots,m,\,j=1,\dots,\dim(U_i))}}$$
$$\in k[(y_{i',j'})_{i'=1,\dots,m,\,j'=1,\dots,n}]^{\{1,\dots,n\}\times\bigcup_{i=1}^m\bigcup_{j=1}^{\dim(U_i)}\{(i,j)\}}.$$

Let $\boldsymbol{d} := \det(M)\in k[(y_{i',j'})_{i',j'}]$. Again for $(P_1,\dots,P_m)$ as above, $\boldsymbol{d}$ vanishes at $((P_1)_\circledcirc,\dots,(P_m)_\circledcirc)$ if and only if the homomorphism a'_m is unramified at $((P_1)_\circledcirc,\dots,(P_m)_\circledcirc)$. Furthermore $\boldsymbol{d}$ does not vanish identically on $V_1\times\cdots\times V_m$ because it does not vanish at $((P_0)_\circledcirc,\dots,(P_0)_\circledcirc)$.

We want to study the vanishing locus of $\boldsymbol{d}$ on $V_1\times\cdots\times V_m$ and derive an upper bound on the number of k-rational points in the locus.

An entry of M with column index (i,j) is a homogeneous polynomial in the variables $y_{i,1},\dots,y_{i,n}$ of degree $n-1$. Therefore $\boldsymbol{d}$ is multihomogeneous with respect to the sets of variables $(y_{i,1},\dots,y_{i,n})_{i=1,\dots,m}$ of multidegree $(\dim(U_1)\cdot(n-1),\dots,\dim(U_m)\cdot(n-1))$. The total degree is therefore n^2-n. We want to prove:

Proposition 4.2. *The number of k-rational points in the locus of $\boldsymbol{d}$ on $V_1\times\cdots\times V_m$ is at most $n^5\cdot 4^n\cdot q^{n-1}$.*

Proof. Let us first mention the following general fact.

Lemma 4.3. *Let f be a nontrivial polynomial in $\mathbb{F}_q[x_1,\dots,x_n]$ of total degree d. Then $V(f)$ contains at most $d\cdot q^{n-1}$ $\mathbb{F}_q$-rational points.*

Proof. As $\mathbb{F}_q[x_1, \ldots, x_n]$ is factorial, we are immediately reduced to the case that f is irreducible. If now $f = x_n - a$ for some $a \in \mathbb{F}_q$, we are done. Let us assume that this is not the case and let $a \in \mathbb{F}_q$. Now f is not divisible by $x_n - a$. This means that not every coefficient of f as a polynomial in $\mathbb{F}_q[x_n][x_1, \ldots, x_{n-1}]$ is divisible by $x_n - a$; in other words, the polynomial $f(x_1, \ldots, x_{n-1}, a)$ is nontrivial. The result now follows by induction on n. □

We will use resultants to eliminate the "y-variables". Let us consider the polynomials f, f_j and $f_{(i),j}$ as polynomials in the "y-variables". Now let

$$F := Z^2 \cdot f\left(x, \frac{Y}{Z}\right) \in K[x][Y, Z],$$

$$F_j := Z^2 \cdot f_j\left(x_1, \ldots, x_n, \frac{Y_1}{Z}, \ldots, \frac{Y_n}{Z}\right) \in k[x_1, \ldots, x_n][Y_1, \ldots, Y_n, Z],$$

$$F_{(i),j} := Z^2 \cdot f_{(i),j}\left(x_{i,1}, \ldots, x_{i,\dim(U_i)}, \frac{Y_{i,1}}{Z}, \ldots, \frac{Y_{i,n}}{Z}\right) \in k[x_{i,1}, \ldots, x_{i,\dim(U_i)}][Y_{i,1}, \ldots, Y_{i,n}, Z]$$

be the homogeneous polynomials of degree 2 obtained by "homogenizing with respect to the y-variables to a homogeneous degree-2 polynomial". Let us consider $k[x][Y, Z]$, $k[x_1, \ldots x_n][Y_1, \ldots, Y_n, Z]$, $k[x_{i,1}, \ldots, x_{i,\dim(U_i)}][Y_{i,1}, \ldots, Y_{i,n}, Z]$ as graded rings in the second set of variables. Let $\overline{V}_i$ be the scheme defined by $(F_{(i),j})_{j=1,\ldots,n}$ in $\mathrm{Proj}(k[x_{i,1}, \ldots, x_{i,\dim(U_i)}][Y_{i,1}, \ldots, Y_{i,n}, Z]) \simeq \mathbb{A}_k^{\dim(U_i)} \times \mathbb{P}_k^n$. We have a commutative diagram of canonical embeddings

$$\begin{array}{ccc} V_i & \hookrightarrow & \overline{V}_i \\ \downarrow & & \downarrow \\ \mathrm{Res}_k^K(E) = V(f_1, \ldots, f_n) & \hookrightarrow & V(F_1, \ldots, F_n). \end{array}$$

Lemma 4.4. *For each i, the embedding $V_i \hookrightarrow \overline{V}_i$ is an isomorphism.*

Proof. We have to show that $\overline{V}_i$ has no points "at infinity"; that is, the intersection $V(Z) \cap \overline{V}_i$ is trivial. We show in fact the stronger statement that $V(Z) \cap V(F_1, \ldots, F_n)$ is trivial.

Let $f^{(s)} := \sigma_{K|k}^s(f)(x^{(s)}, y^{(s)})$ and $F^{(s)} := F(x^{(s)}, Y^{(s)}, Z)$ for $s = 0, \ldots, n-1$.

Let us consider the isomorphism of graded K-algebras

$$K[x_1, \ldots, x_n][Y_1, \ldots, Y_n, Z] \to K[x^{(1)}, \ldots, x^{(n)}][Y^{(1)}, \ldots, Y^{(n)}, Z],$$

$$x^{(s)} \mapsto \sum_{j=1}^{n} \sigma_{K|k}^s(b_j) \cdot x_j, \quad Y^{(s)} \mapsto \sum_{j=1}^{n} \sigma_{K|k}^s(b_j) \cdot Y_j, \quad Z \mapsto Z.$$

We have the following commutative diagram over K:

$$\begin{array}{ccc}
\begin{array}{c}\mathrm{Spec}(K[x_1,\ldots,x_n])\\ \times\\ \mathrm{Spec}(K[y_1,\ldots,y_n])\end{array} & \longrightarrow & \begin{array}{c}\mathrm{Spec}(K[x^{(1)},\ldots,x^{(n)}])\\ \times\\ \mathrm{Spec}(K[y^{(1)},\ldots,y^{(n)}])\end{array}\\
\big\uparrow & & \big\uparrow\\
\mathrm{Res}_k^K(E) = V(f_1,\ldots,f_n)_K & \longrightarrow & V(f^{(1)},\ldots,f^{(n)}) = \prod_{s=0}^{n-1}\sigma_{K|k}^s(E_a)\\
\big\downarrow & & \big\downarrow\\
V(F_1,\ldots,F_n)_K & \longrightarrow & V(F^{(1)},\ldots,F^{(n)})\\
\big\downarrow & & \big\downarrow\\
\begin{array}{c}\mathrm{Spec}(K[x_1,\ldots,x_n])\\ \times\\ \mathrm{Proj}(K[Y_1,\ldots,Y_n,Z])\end{array} & \longrightarrow & \begin{array}{c}\mathrm{Spec}(K[x^{(1)},\ldots,x^{(n)}])\\ \times\\ \mathrm{Proj}(K[Y^{(1)},\ldots,Y^{(n)},Z])\end{array}
\end{array}$$

Here the horizontal maps are induced by the isomorphism mentioned above. They are clearly isomorphisms. One can easily see that the middle morphism on the right is an isomorphism: we have $F(x^{(s)}, Y^{(s)}, 0) = (Y^{(s)})^2$, and the scheme $V((Y^{(1)})^2,\ldots,(Y^{(n)})^2, Z)$ is trivial. Therefore the middle morphism on the left is an isomorphism too. □

We fix the following notation: for $b \in \mathbb{N}_0$, $(P_0)_\circledcirc^b$ is the point $((P_0)_\circledcirc,\ldots,(P_0)_\circledcirc)$ with b entries. Let now for $\ell = 0,\ldots,m$ the k-scheme $\mathcal{V}_\ell$ be the following subscheme of $V_1 \times\cdots\times V_m$:

$$\mathcal{V}_\ell := V_1 \times\cdots\times V_\ell \times (P_0)_\circledcirc^{m-\ell}.$$

Furthermore, let $\boldsymbol{d}_\ell \in k[(y_{i',j'})_{i'=1,\ldots,\ell,\ j'=1,\ldots,n}]$ be the polynomial obtained from $\boldsymbol{d}$ by evaluating $y_{i',j'}$ for $i' = \ell+1,\ldots,m$ and $j' = 1,\ldots,n$ at $(P_0)_\circledcirc$. Note that $\boldsymbol{d}_\ell$ does not vanish identically on $\mathcal{V}_\ell$ because it does not vanish at $(P_0)_\circledcirc^\ell$.

We want to show by induction on ℓ:

$$\#(\mathcal{V}_\ell \cap V(\boldsymbol{d}))(k) \le \ell \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell}\dim(U_i))-1}.$$

Recall here that $\dim(U_i) = \dim(V_i)$.

The induction base is $\ell = 0$. As $\boldsymbol{d}$ does not vanish at $(P_0)_\circledcirc^\ell$, the set $\mathcal{V}_0 \cap V(\boldsymbol{d})$ is empty. Therefore the claim holds.

So let $\ell \le m$ be given and let us assume that the claim holds for $\ell - 1$.

The set $(\mathcal{V}_\ell \cap V(\boldsymbol{d}))(k)$ can be divided into two disjoint parts: The first part consists of the points $(P_1, \ldots, P_\ell)$ with $\boldsymbol{d}_{\ell-1}(P_1, \ldots, P_{\ell-1}) = 0$. The second part consists of the points $(P_1, \ldots, P_\ell)$ with $\boldsymbol{d}_{\ell-1}(P_1, \ldots, P_{\ell-1}) \neq 0$.

We first consider points in the first part. As over each point of $\mathbb{A}^1(K)$ there lie at most 2 points of $E_a(K)$, over each point $\mathbb{A}^n(k)$ lie at most two points of $\mathrm{Res}_k^K(E_a)(k)$. In particular, over each point of $\mathbb{A}_k[U_\ell](k)$ lie at most 2 points of $V_\ell(k)$. Because of this and because of the induction hypothesis, there are at most

$$(2q)^{\dim(U_\ell)} \cdot (\ell-1) \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell-1} \dim(U_i))-1} = (\ell-1) \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell} \dim(U_i))-1}$$

points in the first part.

We now consider points in the second part.

Let $(P_1, \ldots, P_{\ell-1}) \in V_1(k) \times \cdots \times V_{\ell-1}(k)$ with $\boldsymbol{d}_{\ell-1}(P_1, \ldots, P_{\ell-1}) \neq 0$; that is, $\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}, (P_0)_\circledcirc) \neq 0$.

The polynomial

$$\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}) \in k[y_{\ell,1}, \ldots, y_{\ell,n}] \subseteq k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}, y_{\ell,1}, \ldots, y_{\ell,n}]$$

is now nontrivial on V_ℓ. Since — by the conditions we have imposed — V_ℓ is irreducible, $V_\ell \cap V(\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}))$ is of codimension 1 in V_ℓ by Krull's Hauptidealsatz; with other words, it is of dimension $\dim(U_\ell) - 1$.

The polynomial $\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1})$ is already homogeneous with respect to $y_{\ell,1}, \ldots, y_{\ell,n}$; let $\bar{\boldsymbol{d}} \in k[Y_{\ell,1}, \ldots, Y_{\ell,n}, Z] \subseteq k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}][Y_{\ell,1}, \ldots, Y_{\ell,n}, Z]$ be the polynomial obtained by substituting $Y_{\ell,n}$ for $y_{\ell,n}$. This is a homogeneous polynomial of degree $\dim(U_\ell) \cdot (n-1)$ with respect to $Y_{\ell,1}, \ldots, Y_{\ell,n}, Z$. As $V_\ell = \overline{V}_\ell$ (Lemma 4.4), we have

$$\begin{aligned} V_\ell \cap V(\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1})) = \overline{V}_\ell \cap V(\bar{\boldsymbol{d}}) = V(F_{(\ell),1}, \ldots, F_{(\ell),n}, \bar{\boldsymbol{d}}) \\ \subseteq \mathrm{Spec}(k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}]) \times \mathrm{Proj}(k[Y_{\ell,1}, \ldots, Y_{\ell,n}, Z]). \end{aligned}$$

Let $\mathrm{Res} = \mathrm{Res}(G_1, \ldots, G_{n+1})$ be the dense multivariate resultant for $n+1$ homogeneous variables and polynomials of (homogeneous) degrees $2, \ldots, 2, \dim(U_i) \cdot (n-1)$. Here, the $G_1, \ldots, G_{n+1}$ are independent generic polynomials, that is, polynomials with algebraically independent coefficients. (As in [Diem 2011b], the similarity between the notation for the Weil restriction and the resultant is accidental.)

Taking the resultant of $F_{(\ell),1}, \ldots, F_{(\ell),n}, \bar{\boldsymbol{d}}$ with respect to $Y_{\ell,1}, \ldots, Y_{\ell,n}, Z$, we obtain $\mathrm{Res}(F_{(\ell),1}, \ldots, F_{(\ell),n}, \bar{\boldsymbol{d}})$, a nontrivial polynomial in $k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}]$. For some point $Q \in \mathbb{A}^n(\bar{k})$, the resultant $\mathrm{Res}(F_{(\ell),1}, \ldots, F_{(\ell),n}, \bar{\boldsymbol{d}})$ vanishes at Q if and only if there is a $\bar{k}$-rational point in $\overline{V}_\ell \cap V(\bar{\boldsymbol{d}}) = V_\ell \cap V(\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}))$ over Q.

We want to determine the multidegree of this polynomial. First we consider the degrees of Res as a polynomial on the coefficients of the G_j. By [Gelfand

et al. 1994, Subsection 3.3A] we have: for $j = 1, \dots, n$, Res is a homogeneous polynomial of degree $\dim(U_j)\cdot(n-1)\cdot 2^{n-1} < n^2\cdot 2^{n-2}$ in the coefficients of the G_j. The inequality is obtained as follows: As $m \geq 2$, $\dim(U_j) \leq \lceil n/2 \rceil \leq (n+1)/2$. Furthermore, Res is a homogeneous polynomial of degree 2^n in the coefficients of G_{n+1}. Moreover, $F_{(\ell),j}$ has degree at most 3 in the $x_{\ell,j'}$ ($j' = 1, \dots, \dim(U_i)$) and $\bar{\boldsymbol{d}}$ obviously has degree 0 in the $x_{\ell,j'}$.

Therefore, $\mathrm{Res}(F_{\ell,1}, \dots, F_{\ell,n}, \bar{\boldsymbol{d}})$ has degree at most $n\cdot 3\cdot n^2\cdot 2^{n-2}$ in each of the variables $x_{\ell,j'}$. Its total degree is thus at most $3n^4\cdot 2^{n-2}$. By Lemma 4.3, the locus the resultant contains at most $3n^4\cdot 2^{n-2}\cdot q^{\dim(U_\ell)-1}$ k-rational points. As over each of these points lie at most two k-rational points of $V_\ell \cap V(\boldsymbol{d}(P_1, \dots, P_{\ell-1}))$, this set contains at most $6n^4\cdot 2^{n-2}\cdot q^{\dim(U_\ell)-1}$ points. We now let $P_1, \dots, P_{\ell-1}$ vary, and we obtain that there are at most

$$\begin{aligned} &6n^4\cdot 2^{n-2}\cdot q^{\dim(U_\ell)-1}\cdot(2q)^{\sum_{i=1}^{\ell-1}\dim(U_i)} \\ &\quad = 6n^4\cdot 2^{n-1}\cdot 2^{\sum_{i=1}^{\ell-1}\dim(U_i)-1}\cdot q^{\sum_{i=1}^{\ell}\dim(U_i)-1} < n^4\cdot 2^n\cdot(2q)^{(\sum_{i=1}^{\ell}\dim(U_i))-1} \end{aligned}$$

points in the second part of the set $(\mathcal{V}_a \cap V(\boldsymbol{d}))(k)$. (We use that $\dim(U_\ell) \geq 2$ as $m \leq n/2$.)

Altogether, there are $< \ell\cdot n^4\cdot 2^n\cdot(2q)^{(\sum_{i=1}^{\ell}\dim(U_i))-1}$ points in $(\mathcal{V}_\ell \cap V(\boldsymbol{d}))(k)$.

This concludes the proof of Proposition 4.2. □

There are at most 3 K-rational ramification points in E_a under $x_{|E_a}$. Therefore, there are at most $3\cdot 2^{m-1}\cdot q^{n-1} < 2^n\cdot q^{n-1}$ tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which do not satisfy Condition 4.1. Proposition 4.2 gives therefore:

Proposition 4.5. *The number of tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which do not define isolated decompositions is at most $(n^5\cdot 4^n + 2^n)\cdot q^{n-1}$.*

The case that q is even and $j \neq 0$. Let $a \in K$ be the ramification point of E_a over $\mathbb{A}^1_K$. Then $dx_{|E}/(x_{|E} - a)$ is a holomorphic differential on E.

As above, we obtain a nontrivial polynomial $\boldsymbol{d} \in k[(x_{i,j})_{i=1,\dots,m,\, j=1,\dots,\dim(U_i)}]$ of total degree $n^2 - n$ such that, for points $(P_1, \dots, P_m) \in E(K)^m$ with $x(P_i) \in U_i$ satisfying Condition 4.1, $((P_1)_\circledcirc, \dots, (P_m)_\circledcirc)$ is an isolated reduced point in its fiber if and only if $\boldsymbol{d}((P_1)_\circledcirc, \dots, (P_m)_\circledcirc) = 0$.

There are at most $(n^2 - n)\cdot q^{n-1}$ points in the locus of $\boldsymbol{d}$ on $\mathbb{A}^n_k$. Moreover, over each point of $\mathbb{A}^1(K)$ are at most two points of $E(K)$. The number of points $(P_1, \dots, P_m) \in V_1(k) \times \cdots \times V_m(k)$ satisfying Condition 4.1 which are not isolated reduced points in their fiber is thus at most $2^m\cdot(n^2 - n)\cdot q^{n-1}$. Therefore:

Proposition 4.6. *The number of tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which do not define isolated decompositions is at most $2^m\cdot n^2\cdot q^{n-1}$.*

The case that q is even and $j = 0$. In this case, $dx_{|E}$ itself is a holomorphic differential on E. It follows that $(\tau_{(P_0 - P_i)_\circledcirc})_*(t_{i,j}((P_i)_\circledcirc)) = (t_{i,j}((P_0)_\circledcirc))$ for

any $P \in E_a(K)$. Therefore, the morphism $a'_m : V_1 \times \cdots \times V_m \to \mathrm{Res}_k^K(E)$ is unramified everywhere and we obtain:

Proposition 4.7. *Every decomposition is isolated.*

The final result of the analysis. All in all, we have:

Proposition 4.8. *For*

- $2^{5n} \leq q$, *or*
- q *even*, $n^3 \leq q$ *and* $m \leq \lceil\sqrt{\log_2(q)}\rceil$,

the following holds: *The probability that a uniformly randomly distributed point of* $E(K)$ *has an isolated decomposition is in*

$$\frac{1}{e^{\mathcal{O}(mn)}} = \left(\frac{1}{e^{mn}}\right)^{\Omega(1)}.$$

We remark here that the condition $m \leq \lceil\sqrt{\log_2(q)}\rceil$ is satisfied for m in the preliminary algorithm presented in the introduction.

Proof. Let first q be odd and the first condition satisfied. By the conditions in Section 2E, we have $\#\mathcal{F}_i \geq \frac{1}{4} \cdot q^{\dim(U_i)}$ for all i and therefore $\#(\mathcal{F}_1 \times \cdots \times \mathcal{F}_m) \geq (1/4^m) \cdot q^n \geq (1/4^n) \cdot q^n$. By Proposition 4.5, at most $(n^5 \cdot 4^n + 2^n) \cdot q^{n-1}$ of these tuples do not define isolated decompositions. So if $n^5 \cdot 4^n + 2^n \leq \frac{1}{2} \cdot (1/4^n) \cdot q$, we have at least $\frac{1}{2} \cdot (1/4^n) \cdot q^n$ tuples which do define isolated decompositions. This is for example the case if $2^{5n} \leq q$ and n is large enough, and for every fixed n it holds if q is large enough. By Proposition 3.3(a) the image of the set of tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which define isolated decompositions has a size of $(1/e^{\mathcal{O}(mn)}) \cdot q^n$. The probability that a uniformly randomly distributed point in $E(\mathbb{F}_{q^n})$ has an isolated decomposition is therefore in $1/e^{\mathcal{O}(mn)}$.

We now consider the case that q is even. The proof is similar to the previous one, only that we now apply Propositions 4.6 and 4.7. We now want that the condition $2^m \cdot n^2 \leq \frac{1}{2} \cdot (1/4^m) \cdot q$ is satisfied; that is, $2 \cdot 2^{3m} \cdot n^2 \leq q$. This is always satisfied under the first condition; that is, $2^{5n} \leq q$. Furthermore, under the condition that $m \leq \lceil\sqrt{\log_2(q)}\rceil$ the desired condition is in particular satisfied if $2n^2 \leq 2^{\log_2(q) - 3\lceil\sqrt{\log_2(q)}\rceil}$. This condition is for example satisfied if $n^3 \leq q$ and n is large enough, and it holds for every fixed n if q is large enough. □

Derivation of Theorem 2. Finally, we show how Theorem 2 follows. In addition we show that in characteristic 2 one can obtain a result which on first sight seems to be an improvement over Theorem 2 but is in fact further improved upon by Theorem 3 which relies solely on Theorem 2.

As already mentioned in the outline in the introduction, the basic structure of the index calculus algorithm is the same as that in [Diem 2011b]. So we only

discuss the constructions surrounding the definition of the factor base and briefly the relation generation and the linear algebra part, using the results proved above. For an overview over the complete algorithm, we refer to Subsection 2.3 of our previous work.

The input to the index calculus algorithm consists of a field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_{q^n}$ and points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A\rangle$ such that $2^{5n} \leq q$ or q is even and $n^3 \leq q$. The following considerations hold for q and n *large enough*. An algorithm for all instances under consideration running in the claimed expected time can be obtained by running the index calculus algorithm "in parallel" with a brute force computation.

Similarly to the "preliminary algorithm", we set $m := \min\{\lceil\sqrt{\log_2(q)}\rceil, \lfloor n/2\rfloor\}$. (We need $m \leq n/2$ in order to be able to apply the algorithm for the construction of a decomposition of K in Section 2E.) So $d = \lceil n/m\rceil \leq \max(n/\sqrt{\log_2(q)} + 1, 3)$ and thus $\mathcal{P}oly(q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n\cdot\sqrt{\log(q)}))}$.

The expected running time of the construction of the decomposition of K and the definition of the factor base is in $\mathcal{P}oly(n\cdot q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n\cdot\sqrt{\log(q)}))}$ (see Proposition 2.10). We have an algorithm for the "new decomposition problem" with an expected running time of $\mathcal{P}oly(e^{mn}\cdot\log(q)) \subseteq e^{\mathcal{O}(n\cdot\sqrt{\log(q)})}$ and a success probability of $1/e^{\mathcal{O}(mn)}$ (see Propositions 3.3 and 4.8). Therefore the expected running time of the relation generation part is in $\mathcal{P}oly(e^{n\cdot\sqrt{\log(q)}}\cdot m\cdot q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n\cdot\sqrt{\log(q)}))}$. The linear algebra part has an expected running time of $\mathcal{P}oly(m\cdot q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n\cdot\sqrt{\log(q)}))}$.

In total, we obtain an expected running time of

$$e^{\mathcal{O}(\max(\log(q), n\cdot\sqrt{\log(q)}))}.$$

We recall again that we have only considered instances with $2^{5n} \leq q$ or q even and $n^3 \leq q$ so far. The derivation of Theorem 2 is now analogous to the derivation of Theorem 1 from [ibid., Proposition 2.11].

We make the following case distinction: If $2^{5n} \leq q$, we apply the index calculus algorithm directly. If $2^{5n} > q$, we set $a := \lceil 5n/\log_2(q)\rceil$ and apply the index calculus algorithm to the curve $E_{\mathbb{F}_{q^{an}}}$, the field extension $\mathbb{F}_{q^{an}}|\mathbb{F}_{q^a}$ and A, B. Now $2^{5n} \leq q^a$; thus we can conclude that the index calculus algorithm runs in an expected running time of $e^{\mathcal{O}(\max(\log(q^a), n\cdot\sqrt{\log(q^a)}))} = e^{\mathcal{O}(n^{3/2})}$.

This gives Theorem 2 except that in the theorem the field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$ is not given with the input data. As already pointed out in [ibid.], one can apply the above algorithm with all possible field extensions "in parallel" to obtain the desired result.

In addition to the derivation of Theorem 2 we now consider only instances in characteristic 2. Under this condition, we can proceed as follows: For $n^3 \leq q$ we apply the index calculus algorithm directly. For $n^3 > q$, we set $a := \lceil 3\log_2(n)/\log_2(q)\rceil$

and proceed as above. We obtain an expected running time of $e^{\mathbb{O}(n\cdot\sqrt{\log(n)})}$. In total, we obtain an expected running time of

$$e^{\mathbb{O}(\max(\log(q),\, n\cdot\log(q)^{1/2},\, n\cdot\log(n)^{1/2}))}; \tag{19}$$

with $q = 2^m$ this is

$$e^{\mathbb{O}(\max(m,\, n\cdot m^{1/2},\, n\cdot\log(n)^{1/2}))}. \tag{20}$$

We note however that for the derivation of Theorem 3 we only apply Theorem 2 under the condition that $n \leq m$. Under this condition, we do not have an improvement upon the expected time given in Theorem 2, and in fact Theorem 3 improves upon the expected time given by (20) if $m \in o(n)$.

Acknowledgment

I thank the anonymous referee for carefully reading this work and for suggestions. I thank Tian Song for pointing out the misprints in [Diem 2011b] I mention in the appendix.

Appendix: Misprints in the previous work

I would like to take the opportunity to correct two misprints in [Diem 2011b].

- In Subsection 4.2 the following situation is considered: Let k be a field, let $n_1 > n_2$, and let $p : (\mathbb{P}^1_k)^{n_1} = \prod_{i=1}^{n_1} \mathrm{Proj}(k[X_i, Y_i]) \to (\mathbb{P}^1_k)^{n_2} = \prod_{i=1}^{n_2} \mathrm{Proj}(k[X_i, Y_i])$ be the projection to the first n_2 factors. Let h_i be the class of $V(X_i)$ in any of the two Chow rings. Lemma 4.6 is on the push-forward map $p_* : \mathrm{CH}((\mathbb{P}^1_k)^{n_1}) \to \mathrm{CH}((\mathbb{P}^1_k)^{n_2})$, which is a group homomorphism. There is a misprint in the lemma. The correct statement is:

  Let $\underline{e} \in \{0,1\}^{n_1}$. *Then* $p_*(h_1^{e_1}\cdots h_{n_1}^{e_1}) = h_1^{e_1}\cdots h_{n_2}^{e_2}$ (*rather than being* 1) *if* $e_{n_2+1} = \cdots = e_{n_1} = 1$ *and* $p_*(h_1^{e_1}\cdots h_{n_1}^{e_1}) = 0$ *otherwise.*

  Computations with the push-forward map are used only once in the analysis of the algorithm, namely in equalities (6) in Subsection 4.5. Here, the correct statement is applied.

- In Proposition 4.28 a subset M of $\{(P_1,\ldots,P_n) \in E(K)^n \mid \forall i = 1,\ldots,n : \varphi(P_i) \in \mathbb{P}^1(k)\}$ is fixed and a lower bound on the number of elements $P \in E(K)$ such that there exists a φ-isolated decomposition $(P_1,\ldots,P_n)$ of P or $-P$ with $P_1,\ldots,P_n \in M$ is given. This lower bound is a difference, and in the subtrahend a factor of $n!$ is missing. The correct lower bound is

$$\frac{\#M - n^3\cdot n!\cdot 2^{2n^2-n}\cdot(q+1)^{n-1}}{n!\cdot 2^{n^2}}.$$

In a similar way, the next lower bound is also incorrect. All following bounds are correct again and no further changes have to be performed for the proof of Proposition 4.29. Proposition 4.28 is also cited for Proposition 5.9 in [Diem 2011a], which is concerned with an application for fixed n. This proposition is not at all affected by the cited misprint.

References

[Cox et al. 2005] D. A. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, 2nd ed., Graduate Texts in Mathematics **185**, Springer, New York, 2005. MR 2005i:13037 Zbl 1079.13017

[Diem 2011a] C. Diem, "On the discrete logarithm problem in class groups of curves", *Math. Comp.* **80**:273 (2011), 443–475. MR 2011j:11242 Zbl 1231.11142

[Diem 2011b] C. Diem, "On the discrete logarithm problem in elliptic curves", *Compos. Math.* **147**:1 (2011), 75–104. MR 2012b:11198 Zbl 1213.11200

[Fulton 1993] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies **131**, Princeton University Press, 1993. MR 94g:14028 Zbl 0813.14039

[Gelfand et al. 1994] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Mathematics: Theory & Applications, Birkhäuser, Boston, MA, 1994. MR 95e:14045 Zbl 0827.14036

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977. MR 57 #3116 Zbl 0367.14001

[Rojas 1999] J. M. Rojas, "Solving degenerate sparse polynomial systems faster", *J. Symbolic Comput.* **28**:1-2 (1999), 155–186. MR 2000g:65050 Zbl 0943.65060

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

Communicated by Bjorn Poonen
Received 2011-07-28 Revised 2012-06-12 Accepted 2012-07-15

diem@math.uni-leipzig.de *Mathematical Institute, University of Leipzig, Augustusplatz 10, D-04109 Leipzig, Germany*

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1325

Identifying Frobenius elements in Galois groups

Tim Dokchitser and Vladimir Dokchitser

We present a method to determine Frobenius elements in arbitrary Galois extensions of global fields, which may be seen as a generalisation of Euler's criterion. It is a part of the general question how to compare splitting fields and identify conjugacy classes in Galois groups, which we will discuss as well.

1. Introduction

Take a Galois extension $L/\mathbb{Q}$. Associated to each (unramified) prime p is a Frobenius element Frob_p, an element of the Galois group that reduces to $x \mapsto x^p$ modulo a prime above p. In the setting when L is the splitting field of a polynomial f, this element is intimately connected to the factorisation of f mod p: Viewed as a permutation of the roots, Frob_p is a product of disjoint cycles whose lengths are the degrees of the irreducible factors.

In this paper, we address the question of how to determine Frob_p. Generally, we study the problem of how to compare splitting fields and identify conjugacy classes in Galois groups; see Sections 2–4. Our motivation was computing L-series of Artin representations for arbitrary Galois groups, which requires the knowledge of Frobenius elements at all primes; see Remark 5.8 and Example 7.7. Obtaining

MSC2010: primary 11R32; secondary 11R42, 12F10.
Keywords: Frobenius elements, Artin representations, Galois groups.

them directly from the definition is impractical unless L either has small degree or is particularly simple to work with.

Let us briefly illustrate the various standard techniques for computing Frobenius elements. As before, L is the splitting field of a polynomial $f \in \mathbb{Z}[x]$, and we write $G = \mathrm{Gal}(L/\mathbb{Q})$.

Quadratic fields. Suppose $f(x) = x^2 - d$, so $L = \mathbb{Q}(\sqrt{d})$. For a prime $p \nmid 2d$, the Frobenius element is given by the Legendre symbol:

$$\mathrm{Frob}_p = \mathrm{id} \quad \Longleftrightarrow \quad f(x) \bmod p \text{ is reducible} \quad \Longleftrightarrow \quad \left(\frac{d}{p}\right) = 1.$$

There are two essentially different methods to compute it:

(A) Euler's criterion $\left(\frac{d}{p}\right) \equiv d^{(p-1)/2} \bmod p$.

(B) Quadratic reciprocity.

Kummer extensions. Suppose $f(x) = x^3 - 2$, so $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ and $G = \mathrm{S}_3$. For $p \neq 2, 3$ the number of cube roots of 2 mod p determines whether Frob_p is trivial, a 3-cycle or a transposition. It is easy to see that the last case is equivalent to $p \equiv 2 \bmod 3$. There are analogues of both (A) and (B) to distinguish between the first two cases:

(A) Euler's criterion: Since $\mathbb{F}_p^\times$ is cyclic,

$$\begin{aligned} 2 \text{ is a cube mod } p \quad &\Longleftrightarrow \quad 2^{(p-1)/3} \equiv 1 \bmod p. \\ 2 \text{ not a cube mod } p \quad &\Longleftrightarrow \quad 2^{(p-1)/3} \text{ is another third root of unity } z \in \mathbb{F}_p. \end{aligned}$$

To link this criterion to our main theorem below, let us rephrase it: Let

$$M = \left(\begin{smallmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}_3(\mathbb{F}_p), \quad \text{so that } M^3 = \left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{smallmatrix}\right) \quad \text{and} \quad f(M) = 0.$$

Then

$$\begin{aligned} \mathrm{Frob}_p = \mathrm{id} &\iff M^{p-1} = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \iff \tfrac{1}{3}\operatorname{Tr} M^{p-1} = 1, \\ \mathrm{Frob}_p \in [(123)] &\iff M^{p-1} = \left(\begin{smallmatrix} z & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & z \end{smallmatrix}\right) \iff \tfrac{1}{3}\operatorname{Tr} M^{p-1} \text{ satisfies } t^2+t+1 = 0, \\ \mathrm{Frob}_p \in [(12)] &\iff M^{p-1} = \left(\begin{smallmatrix} 0 & 0 & * \\ * & 0 & 0 \\ 0 & * & 0 \end{smallmatrix}\right) \iff \tfrac{1}{3}\operatorname{Tr} M^{p-1} = 0. \end{aligned}$$

(B) Class field theory over $\mathbb{Q}(\zeta_3)$:

Factorise $p = (a + b\zeta_3)(a + b\bar{\zeta}_3)$. Then 2 is a cube mod p if and only if the ideal $(a + b\zeta_3)$ splits in L, and class field theory says that this is a congruence condition on a and b. In fact, it is easy to verify that

$$2 \text{ is a cube mod } p \quad \Longleftrightarrow \quad a + b\zeta_3 \equiv \pm 1, \pm\zeta_3 \text{ or } \pm\zeta_3^2 \bmod 6.$$

Modular forms. See [Zagier 2008, §4.3]. Suppose $f(x) = x^3 - x - 1$, so $G = S_3$ and L is the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$. Let ρ be the 2-dimensional irreducible representation of G. It has an associated Artin L-series

$$L(\rho, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

whose coefficient a_p for a prime $p \neq 23$ is $2, -1$ or 0 depending on whether Frob_p is trivial, a 3-cycle or a transposition. The theory of modular forms tells us that

$$\sum_{n=1}^{\infty} a_n q^n = q \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{23n}),$$

and is a cusp form of weight 1, level 23 and character $\left(\frac{\cdot}{23}\right)$. Moreover, for all integers n not divisible by 23,

$$a_n = \tfrac{1}{2}\big(\#\{x, y \in \mathbb{Z} \mid n = x^2 + xy + 6y^2\} - \#\{x, y \in \mathbb{Z} \mid n = 2x^2 + xy + 3y^2\}\big).$$

Let us remark that in an arbitrary Galois group G, the L-series of the irreducible representations of G also pin down the Frobenius elements. The global Langlands conjecture predicts that, as in this example, all such L-series come from automorphic forms. This is a massive conjectural generalisation of "method (B)". Moreover, like quadratic reciprocity and class field theory, this approach gives expressions for the L-series coefficients a_n that do not depend on n being prime. This is crucial for theoretical applications such as analytic continuation of L-functions. (Note, however, that formulas such as the one above are not practical for numerically computing Frobenius elements.)

The purpose of this paper is to extend "method (A)" to arbitrary Galois groups. Here is an illustration for cubic polynomials of the type of criterion that we obtain. Note its similarity to the Kummer case.

General cubic. Suppose $f(x) = x^3 + bx + c$. Pick a prime $p \nmid 3b\Delta$, where $\Delta = -4b^3 - 27c^2$ is the discriminant of f. Let

$$M = \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p).$$

Then

$$\begin{aligned} f(x) \text{ has 3 roots mod } p &\iff \operatorname{Tr} M^{p+1} = -2b, \\ f(x) \text{ has 1 root mod } p &\iff \operatorname{Tr} M^{p+1} \text{ satisfies } (t + 2b)(t - b)^2 = -\Delta, \\ f(x) \text{ is irreducible mod } p &\iff \operatorname{Tr} M^{p+1} = b. \end{aligned}$$

This can be easily checked by hand; alternatively, see Theorem 7.2.

Our main result for Frobenius elements is the following generalisation of Euler's criterion. Note that taking the class of x in $\mathbb{F}_q[x]/f(x)$ is the same as taking a matrix M with characteristic polynomial $f(x)$, like in the examples above.

Theorem 1.1. *Let K be a global field and $f(x) \in K[x]$ a separable polynomial with Galois group G. There is a polynomial $h(x) \in K[x]$ and polynomials $\Gamma_C \in K[X]$ indexed by the conjugacy classes C of G such that*

$$\mathrm{Frob}_{\mathfrak{p}} \in C \quad \Longleftrightarrow \quad \Gamma_C\big(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q)\big) = 0 \mod \mathfrak{p}$$

for almost all primes $\mathfrak{p}$ of K; here $\mathbb{F}_q$ is the residue field at $\mathfrak{p}$.

This is proved in Section 5; see Theorem 5.3. Usually one can take $h(x) = x^2$ (see below); in particular $\mathrm{Tr}(x^{q+2})$ then determines the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$. In Section 6 we explain how the theorem recovers classical formulas for Frobenius elements in cyclotomic and Kummer extensions. In Section 7 we give explicit examples for nonabelian Galois groups, including general cubics, general quartics and quintics with Galois group D_{10}.

The polynomials Γ_C are explicitly given by

$$\Gamma_C(X) = \prod_{\sigma \in C} \big(X - \sum_{j=1}^{n} h(a_j)\sigma(a_j)\big),$$

where $a_1, \ldots, a_n$ are the roots of f in some splitting field. The "almost all primes" in the theorem are those not dividing the denominators of the coefficients of f, its leading coefficient and the resultants $\mathrm{Res}(\Gamma_C, \Gamma_{C'})$ for $C \neq C'$; the latter simply says that the $\Gamma_C \bmod \mathfrak{p}$ are pairwise coprime. (This condition always fails for ramified primes; see Remark 5.6.) Finally, the only constraint on the polynomial h is that the resulting Γ_C are coprime over K. This holds for almost all h, in the sense that the admissible ones of degree at most $n-1$ form a Zariski dense open subset of K^n. Also, a fixed h with $1 < \deg h < n$ (for instance $h(x) = x^2$) will work for almost all f that define the same field; see Section 8.

Remark 1.2. The method of using polynomials in the roots of f to recognise conjugacy classes is also used in "Serre's trick" for alternating groups. For example, $G = A_5$ has 5 conjugacy classes and all but the two classes of 5-cycles have their own cycle type. (Recall that the cycle type of Frobenius can be recovered from the degrees of the factors of the defining quintic $f \bmod p$; in practice, these are readily determined by computing $\gcd(x^{p^d} - x, f(x))$ for $d = 1, 2$.) It was pointed out by Serre (see Buhler [1978, p. 53]) that the classes of 5-cycles can be distinguished by evaluating the square root of the discriminant of f modulo p; see Example 3.9. This has been generalised by Roberts [2004] to all alternating groups, and was used for instance by Booker [2005] in his work on L-series for icosahedral representations.

Finally, let us illustrate our approach to Frobenius elements with a simple case:

Example 1.3. The polynomial $f(x) = x^5 + 2x^4 - 3x^3 + 1$ has Galois group $G = \mathrm{D}_{10}$ over $K = \mathbb{Q}$. If we number its complex roots by

$$a_1 \approx -3.01, \quad a_2 \approx -0.35 - 0.53i, \quad a_3 \approx 0.85 - 0.31i, \quad a_4 = \overline{a_3}, \quad a_5 = \overline{a_2},$$

then G is generated by the 5-cycle (12345) and complex conjugation (25)(34). It is easy to see that $f(x)$ is irreducible over $\mathbb{F}_2$, so $\mathrm{Frob}_2 \in G$ is in one of the two conjugacy classes of 5-cycles, either $[(12345)]$ or $[(12345)^2]$. How can we check which one it is?

Consider the expressions

$$n_1 = a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_1,$$
$$n_2 = a_1a_3 + a_2a_4 + a_3a_5 + a_4a_1 + a_5a_2.$$

If we think of G as the group of symmetries of a pentagon, the sums are taken over all edges and over all diagonals, respectively. Therefore they are clearly G-invariant, and hence rational numbers. Also, as a_i are algebraic integers, n_1 and n_2 are in fact integers, readily recognised from their complex approximations as being 2 and -5.

Now suppose b_1 is a root of $f(x)$ in $\mathbb{F}_{2^5}$, and $b_i = b_{i-1}^2$ for $i = 2, 3, 4, 5$ are its other roots ordered by the action of the Frobenius automorphism. Then

$$N = b_1b_2 + b_2b_3 + b_3b_4 + b_4b_5 + b_5b_1$$

is in $\mathbb{F}_2$. By considering the reduction modulo a prime $\mathfrak{q}$ above 2 in the splitting field, we see that if $\mathrm{Frob}_\mathfrak{q}$ is (12345) or $(12345)^{-1}$, then $n_1 \equiv N \bmod 2$. Similarly, if $\mathrm{Frob}_\mathfrak{q}$ is $(12345)^2$ or $(12345)^3$, then $n_2 \equiv N \bmod 2$. Computing in $\mathbb{F}_2^5$ (or noting that $N = \mathrm{Tr}_{\mathbb{F}_2[x]/f(x)}(x^3)$) we find that $N = 0$, so Frob_2 must be in $[(12345)]$.

In the language of Theorem 1.1, we took $h(x) = x$ and proved that

$$\Gamma_{[(12345)]} = (X-2)^2 \quad \text{and} \quad \Gamma_{[(12345)^2]} = (X+5)^2$$

distinguish between the two conjugacy classes of 5-cycles: If $f(x)$ is irreducible mod p (and $p \neq 7$, so that $2 \not\equiv -5$), then

$$\mathrm{Frob}_p \in C \quad \Longleftrightarrow \quad \Gamma_C(\mathrm{Tr}_{\mathbb{F}_p[x]/f(x)}(x^{p+1})) = 0 \bmod p.$$

This choice of $h(x)$ was in some sense deceptively simple, because the roots n_i of the Γ_C were integers. (We used that the conjugacy classes of 5-cycles are self-inverse in D_{10}.) Generally, these roots would be algebraic integers of degree $|C|$. For example, $h(x) = x^2$ leads to

$$\Gamma_{[(12345)]} = X^2 + 5X + 18 \quad \text{and} \quad \Gamma_{[(12345)^2]} = X^2 - 11X + 42,$$

and $\mathrm{Tr}(x^{p+2})$ is a root of one of them whenever $f(x) \bmod p$ is irreducible.

Notation. Throughout the paper we use the following notation:

K	ground field
$f(x)$	separable polynomial in $K[x]$ of degree n
L	some extension of K where f splits completely
$\boldsymbol{a} = [a_1, \dots, a_n]$	ordered roots of f in L
$K(\boldsymbol{a})$	field generated by the a_i over K (a splitting field of f)
$G_{\boldsymbol{a}}$	Galois group of f, considered as a subgroup of S_n via its permutation action on $[a_1, \dots, a_n]$.
$[\Psi]$	conjugacy class of $\Psi \in G_{\boldsymbol{a}}$.
$\mathfrak{p}$	prime of K, when K is a global field
$\mathbb{F}_q$	residue field at $\mathfrak{p}$
$\mathrm{Frob}_{\mathfrak{p}}$	any (arithmetic) Frobenius element at $\mathfrak{p}$ in $G_{\boldsymbol{a}}$
$e^F_{\boldsymbol{a}}$, Γ, $M^F_{\boldsymbol{a},\Psi}$	see Definitions 2.2, 2.7, 3.4 and 4.3.

Recall that a global field is a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_p(T)$. The Frobenius element in $\mathrm{Gal}(L/K)$ at $\mathfrak{p}$ is characterised by $\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^q \bmod \mathfrak{q}$ for all $x \in L$ that are integral at some fixed prime $\mathfrak{q}$ of L above $\mathfrak{p}$. The element $\mathrm{Frob}_{\mathfrak{p}}$ is well-defined modulo inertia and up to conjugation. In particular, its conjugacy class is well-defined if $\mathfrak{p}$ is unramified in L/K.

The symmetric group S_n acts on n-tuples by $[c_1, \dots, c_n]^\sigma = [c_{\sigma^{-1}(1)}, \dots, c_{\sigma^{-1}(n)}]$. It acts on the ring of polynomials in n variables $K[x_1, \dots, x_n]$ by $\sigma(x_i) = x_{\sigma(i)}$; thus, for a polynomial $F \in K[x_1, \dots, x_n]$,

$$F^\sigma([c_1, \dots, c_n]) = F([c_1, \dots, c_n]^{\sigma^{-1}}),$$

where $F([\,\cdot\,])$ is the evaluation of F on the n-tuple. Note that all our actions are left actions.

2. Isomorphisms of splitting fields

In this section we introduce our main tools. The reader who is only interested in applications to Frobenius elements may skip to Section 5 and prove Theorem 5.3 directly (at the expense of not seeing the origins of Γ_C).

As a motivation, consider the following general question:

Problem 2.1. Suppose a given separable polynomial $f(x) \in K[x]$ of degree n splits completely in $L \supset K$ and $L' \supset K$. Given the roots $a_1, \dots, a_n$ and $b_1, \dots, b_n$ of f in L and L', find a bijection between them that comes from an isomorphism of splitting fields of f inside L and L'.

We assume that we know the Galois group of f over K as a permutation group on the roots in L, but we do not want to construct the splitting fields explicitly. Instead,

we will evaluate polynomials in $K[x_1, \ldots, x_n]$ on the roots in L and L' taken in various orders and try to extract information out of the values (as in Example 1.3).

Definition 2.2. For $F \in K[x_1, \ldots, x_n]$ define the *evaluation map* $S_n \to K(\boldsymbol{a})$ by

$$e^F_{\boldsymbol{a}}(\sigma) = F([a_1, \ldots, a_n]^\sigma).$$

Definition 2.3. Let T be a subgroup of S_n. A *T-invariant* F is an element of $K[x_1, \ldots, x_n]$ whose stabiliser is precisely T.

Remark 2.4. Any $F \in K[x_1, \ldots, x_n]$ is evidently T-invariant if we take for T its stabiliser in S_n. Also, any subgroup $T < S_n$ has a T-invariant, for example,

$$F = \sum_{t \in T} m^t, \quad \text{where } m = x_1^{n-1} x_2^{n-2} \cdots x_{n-1},$$

since clearly the stabiliser of m in S_n is $\{1\}$.

Lemma 2.5. *Let F be a T-invariant and $\sigma, \tau \in S_n$.*

(1) $e^F_{\boldsymbol{a}^\tau}(\sigma) = e^F_{\boldsymbol{a}}(\sigma\tau)$.

(2) $g(e^F_{\boldsymbol{a}}(\sigma)) = e^F_{\boldsymbol{a}}(\sigma g^{-1})$ *for* $g \in G_{\boldsymbol{a}}$.

(3) *The map* $e^F_{\boldsymbol{a}} : S_n \to K(\boldsymbol{a})$ *is constant on the right cosets* $T\sigma$.

Proof. (1) $e^F_{\boldsymbol{a}^\tau}(\sigma) = F((\boldsymbol{a}^\tau)^\sigma) = F(\boldsymbol{a}^{\sigma\tau}) = e^F_{\boldsymbol{a}}(\sigma\tau)$.

(2) For $g \in G_{\boldsymbol{a}}$,

$$\begin{aligned} g(e^F_{\boldsymbol{a}}(\sigma)) &= g(F([a_1, \ldots, a_n]^\sigma)) = F([g(a_1), \ldots, g(a_n)]^\sigma) \\ &= F(([a_1, \ldots, a_n]^{g^{-1}})^\sigma) = F([a_1, \ldots, a_n]^{\sigma g^{-1}}) \quad = e^F_{\boldsymbol{a}}(\sigma g^{-1}). \end{aligned}$$

(3) For $\tau \in T$,

$$\begin{aligned} e^F_{\boldsymbol{a}}(\tau\sigma) &= F([a_1, \ldots, a_n]^{\tau\sigma}) = F(([a_1, \ldots, a_n]^\sigma)^\tau) \\ &= F^{\tau^{-1}}([a_1, \ldots, a_n]^\sigma) = F([a_1, \ldots, a_n]^\sigma) \quad = e^F_{\boldsymbol{a}}(\sigma). \end{aligned}$$

□

Remark 2.6. Part (3) of the lemma says that the values of F on the various permutations $\boldsymbol{a}^\sigma$ of the roots are essentially the right cosets of T in S_n. It may accidentally happen that the same value occurs on two right cosets, but it is always possible to adjust the original polynomial f to prevent this (see Lemma 8.1c). Part (2) of Lemma 2.5 says that the action of the Galois group $\mathrm{Gal}(K(\boldsymbol{a})/K)$ on these values translates into right multiplication by $G_{\boldsymbol{a}}$. This motivates the following:

Definition 2.7. For a double coset $D = T\sigma_0 G_{\boldsymbol{a}}$ in S_n, define the corresponding "minimal polynomial"

$$\Gamma^F_{\boldsymbol{a},\sigma_0} = \Gamma^F_{\boldsymbol{a},D}(X) = \prod_{\sigma \in T\backslash D} (X - e^F_{\boldsymbol{a}}(\sigma)) \in K[X].$$

By Lemma 2.5(3), this is well-defined.

Remark 2.8. Note that by Lemma 2.5(2), $G_{\boldsymbol{a}}$ permutes the linear factors of $\Gamma^F_{\boldsymbol{a},D}$ transitively, so it is a power of an irreducible polynomial in $K[X]$. If $e^F_{\boldsymbol{a}} : T\backslash \mathrm{S}_n \to K(\boldsymbol{a})$ is injective, then $\Gamma^F_{\boldsymbol{a},D}(X)$ is irreducible, and hence the minimal polynomial of $e^F_{\boldsymbol{a}}(\sigma_0)$.

Remark 2.9. The point is that the $\Gamma^F_{\boldsymbol{a},D}(X)$ are K-rational objects, and they can be used to compare different splitting fields:

Proposition 2.10. *Let $\boldsymbol{a}, \boldsymbol{b}$ be orderings of roots of f in two splitting fields of f, and let $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$ be an isomorphism. If $e^F_{\boldsymbol{a}} : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective, then for every double coset $D \in T\backslash \mathrm{S}_n / G_{\boldsymbol{a}}$,*

$$\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0 \quad \Longleftrightarrow \quad \boldsymbol{b} = [\phi(a_1), \dots, \phi(a_n)]^\sigma \quad \text{for some } \sigma \in D.$$

Proof. We have that $\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0$ if and only if $F(\boldsymbol{b}) = \phi(x)$ for some root x of $\Gamma^F_{\boldsymbol{a},D}$ in $K(\boldsymbol{a})$. Such roots are $e^F_{\boldsymbol{a}}(\sigma)$ for some $\sigma \in D$, so

$$\begin{aligned}
\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0 \quad &\Longleftrightarrow \quad F(\boldsymbol{b}) = \phi(e^F_{\boldsymbol{a}}(\sigma)) && \text{for some } \sigma \in D \\
&\Longleftrightarrow \quad F(\phi^{-1}(\boldsymbol{b})) = e^F_{\boldsymbol{a}}(\sigma) = F(\boldsymbol{a}^\sigma) \\
&\Longleftrightarrow \quad \phi^{-1}(\boldsymbol{b}) = (\boldsymbol{a}^\sigma)^\tau = \boldsymbol{a}^{\tau\sigma} && \text{for some } \tau \in T \\
&\Longleftrightarrow \quad \boldsymbol{b} = \phi(\boldsymbol{a}^{\sigma'}) = \phi(\boldsymbol{a})^{\sigma'} && \text{for some } \sigma' \in D. \qquad \square
\end{aligned}$$

Theorem 2.11. *Let F be a $G_{\boldsymbol{a}}$-invariant with $e^F_{\boldsymbol{a}} : G_{\boldsymbol{a}}\backslash \mathrm{S}_n \to K(\boldsymbol{a})$ injective. If $F(\boldsymbol{b}) = F(\boldsymbol{a}) \in K$, then $a_i \mapsto b_i$ defines an isomorphism $K(\boldsymbol{a}) \to K(\boldsymbol{b})$.*

Proof. Take $T = G_{\boldsymbol{a}}$ and D the principal double coset $G_{\boldsymbol{a}} 1 G_{\boldsymbol{a}}$, and apply the proposition. Since $\Gamma^F_{\boldsymbol{a},D}(X) = X - F(\boldsymbol{a})$, we have $\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0$, so $\boldsymbol{b} = \phi(\boldsymbol{a})^\sigma$ for some $\sigma \in G_{\boldsymbol{a}}$ and some isomorphism $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$. Then $\phi \circ \sigma$ is the required isomorphism. $\square$

Remark 2.12. This gives a solution to Problem 2.1:

Pick a $G_{\boldsymbol{a}}$-invariant F, for instance using Remark 2.4. Adjusting f if necessary, we may assume that $e^F_{\boldsymbol{a}} : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective (Lemma 8.1c). In L', keep permuting the roots of f until $F(\boldsymbol{b})$ becomes $F(\boldsymbol{a}) \in K$. When this happens, $a_i \mapsto b_i$ defines an isomorphism of the two splitting fields.

Note however, that in the worst case we are evaluating a polynomial with $|G|$ terms on $|G\backslash \mathrm{S}_n / G|$ permutations. So the complexity is about $n!$ operations, which is impractical for large n.

Example 2.13 (D_{10}-extensions). Suppose $f(x) \in K[x]$ has degree 5, and $G_{\boldsymbol{a}} = \mathrm{Gal}(f/K)$ is the dihedral group D_{10}, generated by (12345) and (25)(34). Take

$$F(x_1, \dots, x_5) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1.$$

This is a T-invariant with $T = G_{\boldsymbol{a}}$: It is clearly invariant under D_{10}, and on the other hand a permutation preserving F is determined by $x_1 \mapsto x_i$, $x_2 \mapsto x_{i\pm1}$, so there are at most 10 choices. In particular, $F(a_1, \dots, a_5)$ is invariant under the Galois group, and so lies in K. Substituting the a_i into F in all possible orders gives the values

$$e_{\boldsymbol{a}}^F(\sigma^{-1}) = a_{\sigma(1)}a_{\sigma(2)} + a_{\sigma(2)}a_{\sigma(3)} + a_{\sigma(3)}a_{\sigma(4)} + a_{\sigma(4)}a_{\sigma(5)} + a_{\sigma(5)}a_{\sigma(1)}.$$

Clearly each one occurs at least 10 times for varying $\sigma \in \mathrm{S}_5$, corresponding to the fact that $e_{\boldsymbol{a}}^F$ factors through $\mathrm{D}_{10}\backslash\mathrm{S}_5$. The assumption that the map $e_{\boldsymbol{a}}^F : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective simply says that there are no more repetitions, and there are $120/10 = 12$ distinct values.

Suppose that this is indeed the case, and let $b_1, \dots, b_5$ be the roots of f in some other splitting field. If we substitute the b_i in F in all possible orders $\boldsymbol{b}^\sigma$, we get again 12 values, one of which is $F(a_1, \dots, a_5) \in K$. There are 10 isomorphisms $K(\boldsymbol{a}) \to K(\boldsymbol{b})$ obtained from one another by composing with Galois. They are determined by $\boldsymbol{a} \mapsto \boldsymbol{b}^\sigma$ for 10 permutations $\sigma \in \mathrm{S}_n$. Clearly, for each of these σ, we have $F(\boldsymbol{b}^\sigma) = F(\boldsymbol{a})$. But, since every value is taken exactly 10 times, we have the converse as well: if $F(\boldsymbol{b}^\sigma) = F(\boldsymbol{a})$ for some $\sigma \in \mathrm{S}_n$, then $\boldsymbol{a} \mapsto \boldsymbol{b}^\sigma$ must define an isomorphism of the splitting fields. So to find an isomorphism, we only need to locate $F(\boldsymbol{a})$ among the 12 values $F(\boldsymbol{b}^\sigma)$.

Note that the other values $F(\boldsymbol{b}^\sigma)$ are not in general K-rational, so we cannot compare them with the values on $\boldsymbol{a}$. Their minimal polynomials are the $\Gamma_{\boldsymbol{a},D}^F(X)$ for the 4 double cosets $\mathrm{D}_{10}\backslash\mathrm{S}_5/\mathrm{D}_{10}$.

3. Recognising conjugacy in Galois groups

In questions such as computing Frobenius elements in Galois groups it is not necessary to compare the roots in two splitting fields. It suffices to identify the conjugacy class of a specific Galois automorphism:

Problem 3.1. Let $f(x) \in K[x]$ be a separable polynomial that splits completely in $L \supset K$, and suppose we know $G = \mathrm{Gal}(f/K)$ as a permutation group on the roots in L. If L' is another field where f splits completely and we are given a permutation of the roots of f in L' that comes from some Galois automorphism, find the conjugacy class of this automorphism in G.

Remark 3.2. An isomorphism ϕ of the two splitting fields of f induces an isomorphism of Galois groups G and G'. We would like to identify an element $\mathcal{B} \in G'$ as an element $\mathcal{A} \in G$. Note, however, that $\mathcal{A}$ depends on the choice of ϕ. As any two isomorphisms differ by a Galois automorphism, the conjugacy class $[\mathcal{A}]$ is well-defined and this is what we are after.

It is easy to see that a solution to Problem 2.1 answers Problem 3.1 as well, so this is a weaker question. However, we aim for a more practical solution (see Remark 2.12). We may clearly restrict our attention to one cycle type in S_n. For convenience, throughout the section we also fix a representative:

Notation 3.3. Fix an element $\xi \in \mathrm{S}_n$ and write $Z_\xi < \mathrm{S}_n$ for its centraliser.

Definition 3.4. Suppose $\Psi \in \mathrm{S}_n$ is conjugate to ξ, in other words they have the same cycle type, say $\xi = \sigma_0 \Psi \sigma_0^{-1}$. For a T-invariant F and an ordering $\boldsymbol{a}$ of the roots of f, define the polynomial

$$M^F_{\boldsymbol{a},\Psi}(X) = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_0} \Gamma^F_{\boldsymbol{a},\sigma}(X).$$

It is well-defined by Lemma 2.5(3). Note that $Z_\xi \sigma_0$ is the set of all permutations that conjugate Ψ to ξ; in particular it is independent of the choice of σ_0.

Remark 3.5. The situation we have in mind is that we have two sets of roots $\boldsymbol{a}$ and $\boldsymbol{b}$ of f in different splitting fields. So there is an isomorphism $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$, but we do not have it explicitly. However, suppose we know that an automorphism $\mathcal{A} \in \mathrm{Gal}(K(\boldsymbol{a})/K)$ corresponds to $\mathcal{B} \in \mathrm{Gal}(K(\boldsymbol{b})/K)$ under ϕ, and that they permute the roots by

$$\mathcal{A}(\boldsymbol{a}) = \boldsymbol{a}^\Psi, \quad \mathcal{B}(\boldsymbol{b}) = \boldsymbol{b}^\xi, \quad \Psi, \xi \in \mathrm{S}_n.$$

Then $\{\boldsymbol{a}^\sigma\}_{\sigma \in Z_\xi \sigma_0}$ is the set of all reorderings of $\boldsymbol{a}$ on which $\mathcal{A}$ acts as ξ, and $M^F_{\boldsymbol{a},\Psi}(X)$ is the smallest K-rational polynomial that has $F(\boldsymbol{a}^\sigma)$ as roots for all such σ. But $\phi^{-1}(\boldsymbol{b})$ must be one of these reorderings because $\mathcal{B}$ acts on $\boldsymbol{b}$ as ξ. The upshot is that $M^F_{\boldsymbol{a},\Psi}(X)$ has $F(\boldsymbol{b})$ as a root, and its construction does not require the knowledge of ϕ. In other words, if $M^F_{\boldsymbol{a},\Psi}(F(\boldsymbol{b})) \neq 0$, then we know that $\mathcal{A}$ does not correspond to $\mathcal{B}$ under any isomorphism. (In Section 4 we will take $T = Z_\xi$ and turn this into an if and only if statement.)

Lemma 3.6. *Let $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$ be an isomorphism of two splitting fields of f, and define $\rho \in \mathrm{S}_n$ by $\boldsymbol{b} = \phi(\boldsymbol{a}^\rho)$. Then $M^F_{\boldsymbol{a},\rho^{-1}\Phi\rho} = M^F_{\boldsymbol{b},\Phi}$.*

Proof. Write $\Psi = \rho^{-1}\Phi\rho$. Pick σ_Φ with $\xi = \sigma_\Phi \Phi \sigma_\Phi^{-1}$, and let $\sigma_\Psi = \sigma_\Phi \rho$, so that

$$\sigma_\Psi \Psi \sigma_\Psi^{-1} = \sigma_\Phi \rho \Psi \rho^{-1} \sigma_\Phi^{-1} = \sigma_\Phi \Phi \sigma_\Phi^{-1} = \xi.$$

By definition,

$$M^F_{\boldsymbol{b},\Phi} = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_\Phi} \Gamma^F_{\boldsymbol{b},\sigma}, \qquad M^F_{\boldsymbol{a},\Psi} = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_\Psi} \Gamma^F_{\boldsymbol{a},\sigma}.$$

We claim that $\Gamma^F_{\boldsymbol{a},s\sigma_\Psi} = \Gamma^F_{\boldsymbol{b},s\sigma_\Phi}$ for $s \in Z_\xi$. First we show that they have the same degree. Because $G_{\boldsymbol{b}} = \rho G_{\boldsymbol{a}} \rho^{-1}$ by the definition of ρ,

$$\begin{aligned}\deg \Gamma^F_{\boldsymbol{a},s\sigma_\Psi} &= |T\backslash T s\sigma_\Psi G_{\boldsymbol{a}}| = |T\backslash T s\sigma_\Psi G_{\boldsymbol{a}}\rho^{-1}| \\ &= |T\backslash T s\sigma_\Phi \rho G_{\boldsymbol{a}}\rho^{-1}| = |T\backslash T s\sigma_\Phi G_{\boldsymbol{b}}| = \deg \Gamma^F_{\boldsymbol{b},s\sigma_\Phi}.\end{aligned}$$

Since both polynomials are powers of irreducible ones, it now suffices to identify one of the roots:

$$\begin{aligned}e^F_{\boldsymbol{a}}(s\sigma_\Psi) &= e^F_{\boldsymbol{a}}(s\sigma_\Phi\rho) = F(\boldsymbol{a}^{s\sigma_\Phi\rho})) = F(\phi^{-1}(\boldsymbol{b})^{s\sigma_\Phi})) \\ &= F(\phi^{-1}(\boldsymbol{b}^{s\sigma_\Phi})) = \phi^{-1}(F(\boldsymbol{b}^{s\sigma_\Phi})) = \phi^{-1}(e^F_{\boldsymbol{b}}(s\sigma_\Phi)).\end{aligned}$$

□

Corollary 3.7. *The map $\Psi \mapsto M^F_{\boldsymbol{a},\Psi}$ is constant on every conjugacy class of $G_{\boldsymbol{a}}$ with cycle type ξ.*

Proof. By the lemma above, $M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},g\Psi g^{-1}}$ for $g \in G_{\boldsymbol{a}}$. □

We now have an approach to Problem 3.1:

Proposition 3.8. *Let $\boldsymbol{a}, \boldsymbol{b}$ be orderings of the roots of f in two different splitting fields, and suppose $\Psi \in G_{\boldsymbol{a}}$ and $\Phi \in G_{\boldsymbol{b}}$ have cycle type ξ. If the polynomials $M^F_{\boldsymbol{a},\psi}$ are distinct for ψ in different conjugacy classes of $G_{\boldsymbol{a}}$ of cycle type ξ, then*

$$\begin{array}{l}\text{there is an isomorphism } K(\boldsymbol{a}) \to K(\boldsymbol{b}) \\ \text{under which } \Psi \text{ corresponds to } \Phi\end{array} \iff M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{b},\Phi}.$$

If, moreover, the $M^F_{\boldsymbol{a},\psi}$ are pairwise coprime, then this occurs precisely when $M^F_{\boldsymbol{a},\Psi}(F(\boldsymbol{b}^\sigma)) = 0$ for some (any) $\sigma \in \mathrm{S}_n$ with $\xi = \sigma\Phi\sigma^{-1}$.

Proof. "$\Longrightarrow$" is Lemma 3.6. For "$\Longleftarrow$", pick any isomorphism $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$. The polynomial $M^F_{\boldsymbol{b},\Phi}$ agrees with some $M^F_{\boldsymbol{a},\psi}$ by the lemma, and Ψ lies in the conjugacy class of ψ by assumption. Composing ϕ with an automorphism of $K(\boldsymbol{a})/K$ (which corresponds to conjugating ψ) we obtain the required isomorphism. □

Example 3.9 (Serre's trick [Buhler 1978; Roberts 2004]). Suppose $\mathrm{char}\, K \neq 2$, $f \in K[x]$ has degree n, and $G_{\boldsymbol{a}} = \mathrm{Gal}(f/K)$ is the alternating group A_n. There is a particularly nice T-invariant with $T = \mathrm{A}_n$, a "square root of the discriminant"

$$F(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j).$$

The only double cosets $T\sigma G_{\boldsymbol{a}}$ in S_n are $D = \mathrm{A}_n$ and its complement D' in S_n. Clearly $\Gamma^F_{\boldsymbol{a},D}(X) = X - F(\boldsymbol{a})$ and $\Gamma^F_{\boldsymbol{a},D'}(X) = X + F(\boldsymbol{a})$, and $F(\boldsymbol{a})^2 = \Delta_f$ is the discriminant of f. So if $\boldsymbol{b}$ is the list of roots of f in some other splitting field, we find that

$$\begin{array}{l}a_i \mapsto b_i \text{ defines an isomorphism} \\ K(\boldsymbol{a}) \to K(\boldsymbol{b})\end{array} \iff \prod_{i<j}(a_i - a_j) = \prod_{i<j}(b_i - b_j).$$

This illustrates Theorem 2.11 in the case of A_n. To explain Proposition 3.8 in this setting, suppose $\xi \in \mathrm{S}_n$ is a product of cycles of distinct odd degrees, so that there are two conjugacy classes $[\Psi_1]$, $[\Psi_2]$ in $G_{\boldsymbol{a}} = \mathrm{A}_n$ of cycle type ξ (for example 5-cycles in A_5). Say $\sigma_1\Psi_1\sigma_1^{-1} = \xi = \sigma_2\Psi_2\sigma_2^{-1}$ with $\sigma_1 \in \mathrm{A}_n$ and $\sigma_2 \notin \mathrm{A}_n$. In this case $Z_\xi \subset \mathrm{A}_n = T$, so

$$M^F_{\boldsymbol{a},\Psi_1}(X) = \Gamma^F_{\boldsymbol{a},\sigma_1}(X) = \Gamma^F_{\boldsymbol{a},D}(X) = X - F(\boldsymbol{a}),$$
$$M^F_{\boldsymbol{a},\Psi_2}(X) = \Gamma^F_{\boldsymbol{a},\sigma_2}(X) = \Gamma^F_{\boldsymbol{a},D'}(X) = X + F(\boldsymbol{a}).$$

Suppose again that $\boldsymbol{b}$ is the list of roots of f in some other splitting field, and $\mathcal{B} \in \mathrm{Gal}(K(\boldsymbol{b})/K)$ is an automorphism of cycle type ξ. Rearranging the b_i if necessary, assume that $\mathcal{B}$ acts on the b_i as ξ, that is, $\mathcal{B}(\boldsymbol{b}) = \boldsymbol{b}^\xi$. The statement of the proposition is that

$$\mathcal{B} \text{ comes from } [\Psi_1] \text{ under an isomorphism } K(\boldsymbol{a}) \to K(\boldsymbol{b}) \iff \prod_{i<j}(a_i - a_j) = \prod_{i<j}(b_i - b_j),$$

which is precisely Serre's trick. The same invariant F may sometimes be used in other subgroups of S_n to distinguish between the conjugacy classes of such cycle types. (It determines whether the two classes are conjugate in A_n or not.)

4. The directed edges invariant

As before, suppose $f(x) \in K[x]$ is separable and $\boldsymbol{a} = [a_1, \dots, a_n]$ are its (ordered) roots in a splitting field. We apply the results of Section 3 when $T = Z_\xi$, the centraliser of ξ. This is particularly nice for two reasons: First, the polynomials $M^F_{\boldsymbol{a},\psi}$ of Proposition 3.8 are irreducible and distinct, and second, it is easy to write down a T-invariant with just n terms and of degree 3 (compare the polynomials in Remark 2.4 and Example 4.2).

Proposition 4.1. *Let $\xi \in \mathrm{S}_n$ with centraliser Z_ξ. Suppose that F is a Z_ξ-invariant such that $e^F_{\boldsymbol{a}} : Z_\xi \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective. Let $\Psi, \Psi' \in G_{\boldsymbol{a}}$ be two elements of cycle type ξ. Then*

(1) *$M^F_{\boldsymbol{a},\Psi}$ is irreducible, and equals $\Gamma^F_{\boldsymbol{a},\sigma}$ for any $\sigma \in \mathrm{S}_n$ with $\xi = \sigma\Psi\sigma^{-1}$.*

(2) *$M^F_{\boldsymbol{a},\Psi}$ has degree $|[\Psi]|$.*

(3) *$M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},\Psi'}$ if and only if Ψ and Ψ' are conjugate in $G_{\boldsymbol{a}}$.*

Proof. For brevity, write $Z = Z_\xi$. Pick $\sigma, \sigma' \in \mathrm{S}_n$ with $\sigma\Psi\sigma^{-1} = \xi = \sigma'\Psi(\sigma')^{-1}$.

(1) By definition,

$$M^F_{\boldsymbol{a},\Psi} = \prod_{\tau \in (Z\cap Z)\setminus Z\sigma} \Gamma^F_{\boldsymbol{a},\tau} = \Gamma^F_{\boldsymbol{a},\sigma}.$$

It is irreducible by the assumed injectivity of $e^F_{\boldsymbol{a}}$; see Remark 2.8.

(2) By definition,

$$\deg \Gamma^F_{\boldsymbol{a},\sigma} = |Z\backslash Z\sigma G_{\boldsymbol{a}}| = \frac{|Z\sigma G_{\boldsymbol{a}}|}{|Z|} = \frac{|\sigma^{-1}Z\sigma G_{\boldsymbol{a}}|}{|Z|}$$
$$= \frac{|G_{\boldsymbol{a}}|}{|G_{\boldsymbol{a}} \cap \sigma^{-1}Z\sigma|} = \frac{|G_{\boldsymbol{a}}|}{|\operatorname{Cent}_{G_{\boldsymbol{a}}}(\Psi)|} = |[\Psi]|.$$

(3) If Ψ and Ψ' are conjugate, then $M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},\Psi'}$ by Corollary 3.7. Conversely, suppose that $M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},\Psi'}$. Since $e^F_{\boldsymbol{a}}$ is injective, $Z\sigma G_{\boldsymbol{a}} = Z\sigma' G_{\boldsymbol{a}}$, so $\sigma' = s\sigma g$ for some $s \in Z$ and $g \in G_{\boldsymbol{a}}$. Then

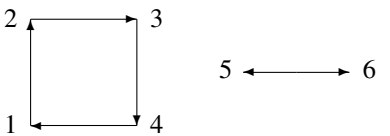
$$\Psi' = (\sigma')^{-1}\xi\sigma' = g^{-1}\sigma^{-1}s^{-1}\xi s\sigma g = g^{-1}\sigma^{-1}\xi\sigma g = g^{-1}\Psi g,$$

so $[\Psi'] = [\Psi]$. □

Example 4.2 (the directed edges invariant). Let $\xi \in \mathrm{S}_n$ and fix a polynomial $h \in K[x]$ of degree at least 2. Define

$$F(x_1, \ldots, x_n) = \sum_{j=1}^{n} h(x_j)\, x_{\xi(j)}.$$

It can be visualised as the directed edges in a graph that define the action by ξ. For instance, for $\xi = (1234)(56) \in \mathrm{S}_6$ and $h(x) = x^2$,



$$F = x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_1 + x_5^2x_6 + x_6^2x_5$$

It is clearly a Z_ξ-invariant.

Definition 4.3. Fix $h(x) \in K[x]$. For each conjugacy class C in $G_{\boldsymbol{a}}$ define

$$\Gamma_C(X) = \prod_{\sigma \in C} \Big(X - \sum_{j=1}^{n} h(a_j)\sigma(a_j) \Big).$$

Lemma 4.4. *Let F be as in Example 4.2. Then for every $\Psi \in G_{\boldsymbol{a}}$,*

$$M^F_{\boldsymbol{a},\Psi}(X) = \Gamma_{[\Psi]}(X).$$

Proof. Pick $\sigma \in \mathrm{S}_n$ with $\sigma\Psi\sigma^{-1} = \xi$. First, suppose $\tau \in [\Psi]$ and $u_\tau \in \mathrm{S}_n$ satisfies $u_\tau^{-1}\xi u_\tau = \tau$. Then

$$e^F_{\boldsymbol{a}}(u_\tau) = F(\boldsymbol{a}^{u_\tau}) = \sum_i h(a_{u_\tau^{-1}(i)})\, a_{u_\tau^{-1}(\xi(i))} = \sum_j h(a_j)\, a_{u_\tau^{-1}\xi u_\tau(j)} = \sum_j h(a_j)\tau(a_j).$$

On the other hand, note that for $t \in Z_\xi$ and $g \in G_{\boldsymbol{a}}$,

$$(t\sigma g)^{-1}\xi(t\sigma g) = g^{-1}\sigma^{-1}t^{-1}\xi t\sigma g = g^{-1}\sigma^{-1}\xi\sigma g = g^{-1}\Psi g.$$

So for $\tau = g^{-1}\Psi g \in [\Psi]$,

$$\{u_\tau \in S_n | u_\tau^{-1}\xi u_\tau = \tau\} = Z_\xi \sigma g,$$

because the left-hand side is clearly some right coset of Z_ξ. This equality gives a correspondence between $[\Psi]$ and $Z_\xi \backslash Z_\xi \sigma G_{\boldsymbol{a}}$. So

$$M^F_{\boldsymbol{a},\Psi}(X) = \Gamma^F_{\boldsymbol{a},\sigma}(X) = \prod_{u \in (Z_\xi \backslash Z_\xi \sigma G_{\boldsymbol{a}})} (X - e^F_{\boldsymbol{a}}(u))$$

$$= \prod_{\tau \in [\Psi]} \Big(X - \sum_{j=1}^{n} h(a)\tau(a_j)\Big) = \Gamma_{[\Psi]}(X). \qquad \square$$

Corollary 4.5. *Let $\boldsymbol{a}, \boldsymbol{b}$ be orderings of the roots of f in two different splitting fields, and let $\Psi \in G_{\boldsymbol{a}}$ and $\Phi \in G_{\boldsymbol{b}}$. If the $\Gamma_C(X)$ are pairwise coprime for different conjugacy classes of $G_{\boldsymbol{a}}$, then*

there is an isomorphism $K(\boldsymbol{a}) \to K(\boldsymbol{b})$ under which Ψ corresponds to Φ, $\iff$ $\Gamma_{[\Psi]}\big(\sum_j h(b_j)\Phi(b_j)\big) = 0.$

The condition that the Γ_C are coprime is satisfied for $h(x)$ in a Zariski dense open set in the space of all polynomials of degree at most $n-1$.

Proof. The equivalence follows from Proposition 3.8 and the lemma above. For the last assertion apply Lemma 8.2. $\square$

Example 4.6. Take $f(x) = x^4 + 14$ over $\mathbb{Q}$. It splits completely over $L = \mathbb{Q}_5$ and $L' = \mathbb{C}$, with roots in $\mathbb{Q}_5$

$$a_1 = 1+3\cdot 5+2\cdot 5^2+\cdots, \quad a_2 = 2+2\cdot 5+0\cdot 5^2+\cdots, \quad a_3 = -a_1, \quad a_4 = -a_2,$$

and

$$b_1 = \sqrt[4]{-14}, \quad b_2 = i\sqrt[4]{-14}, \quad b_3 = -\sqrt[4]{-14}, \quad b_4 = -i\sqrt[4]{-14}$$

in $\mathbb{C}$ (with, say, $\operatorname{Arg} b_1 = \pi/4$). The Galois group of f is $G = \mathrm{D}_8$, which we view as a subgroup of S_4 via the action on the a_i. It is generated by the 4-cycle $a_1 \mapsto a_2 \mapsto a_3 \mapsto a_4 \mapsto a_1$ and the transposition $a_1 \leftrightarrow a_3$. We will illustrate how to identify the conjugacy class of complex conjugation $b_1 \leftrightarrow b_4,\ b_2 \leftrightarrow b_3$ in G, using the polynomials $\Gamma_C(x)$.

There are two conjugacy classes of double transpositions in G, namely $C_1 = \{(12)(34), (14)(23)\}$ and $C_2 = \{(13)(24)\}$. Let $h(x) = x$ and compute

$$\Gamma_{C_1}(X) = (X - (2a_1a_2 + 2a_3a_4))(X - (2a_1a_4 + 2a_2a_3)) = X^2 - 224,$$

$$\Gamma_{C_2}(X) = X - (2a_1a_3 + 2a_2a_4) = X.$$

These are coprime, and Corollary 4.5 applies:

$$\sum_{j=1}^{4} b_j \bar{b}_j = 2b_1 b_4 + 2b_2 b_3 = \sqrt{224}$$

is a root of $\Gamma_{C_1}(X)$, so complex conjugation corresponds to an element of C_1.

Note that the coefficients of the $\Gamma_C(X)$ were computed as 5-adic numbers. Since they are integers and we can bound them from the (complex) absolute values of the roots of f, they can be identified exactly.

5. Frobenius elements

Now suppose K is a global field. We turn to our initial problem of computing Frobenius elements in Galois groups. We use the following remarkable property of the directed edges invariant:

Proposition 5.1. *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial with roots $a_1, \ldots, a_n \in \bar{\mathbb{F}}_q$ counted with multiplicity, and let $\phi = \mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. For every polynomial $h(x) \in \mathbb{F}_q[x]$,*

$$\sum_{j=1}^{n} h(a_j)\phi(a_j) = \mathrm{Tr}_{A/\mathbb{F}_q}(h(X)X^q),$$

where X is the class of x in the algebra $A = \mathbb{F}_q[x]/f$.

This is an immediate consequence of the lemma below (with $H(x) = h(x)x^q$).

Lemma 5.2. *Let k be a field and $f(x) \in k[x]$ a polynomial with roots $a_1, \ldots, a_n \in \bar{k}$ counted with multiplicity. Then for every $H(x) \in k[x]$,*

$$\sum_{j=1}^{n} H(a_j) = \mathrm{Tr}_{A/k}(H(X)),$$

where X is the class of x in $A = k[x]/f$.

Proof. Consider X as a linear map $A \to A$, $Y \mapsto XY$. Its minimal polynomial is f, since $f(X) = 0$ but no linear combination of $1, X, \ldots, X^{n-1}$ is zero. So the generalised eigenvalues of X are exactly the a_i, and those of $H(X)$ are therefore $H(a_i)$ (look at the Jordan normal form of X over $\bar{k}$). The result follows. □

Theorem 5.3 (generalised Euler's criterion). *Let K be a global field and let $f(x) \in K[x]$ be a separable polynomial with roots $a_1, \ldots, a_n$ in $\bar{K}$ and Galois group G. Fix $h(x) \in K[x]$ and for each conjugacy class C of G, set*

$$\Gamma_C(X) = \prod_{\sigma \in C} \Big(X - \sum_{j=1}^{n} h(a_j)\sigma(a_j) \Big).$$

(a) *The polynomials $\Gamma_C(X)$ have coefficients in K.*

(b) *Let $\mathfrak{p}$ be a prime of K with residue field $\mathbb{F}_q$, and C a conjugacy class of G. If $\mathfrak{p}$ does not divide the denominators of the coefficients of f and h, the leading coefficient of f and the resultants $\operatorname{Res}(\Gamma_C, \Gamma_{C'})$ for $C' \neq C$, then the coefficients of $\Gamma_C(X)$ are integral at $\mathfrak{p}$ and*

$$\operatorname{Frob}_\mathfrak{p} \in C \quad \Longleftrightarrow \quad \Gamma_C\big(\operatorname{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q)\big) = 0 \bmod \mathfrak{p}.$$

(c) *For all $h(x)$ in some Zariski dense open set in the space of polynomials of degree at most $n-1$, we have $\operatorname{Res}(\Gamma_C, \Gamma_{C'}) \neq 0$ for every pair of conjugacy classes $C \neq C'$.*

Proof. (a) This follows from Lemma 4.4, Definition 3.4 and Remark 2.8.

(b) $\Gamma_C(X)$ is clearly integral at the required primes.

$\Longrightarrow$: If $\operatorname{Frob}_\mathfrak{p} \in C$ then $\sum_{j=1}^n h(a_j)\operatorname{Frob}_\mathfrak{p}(a_j)$ is a root of $\Gamma_C(X)$ by the definition of Γ_C, and it reduces mod $\mathfrak{p}$ to $\operatorname{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(h(x)x^q)$ by Proposition 5.1.

$\Longleftarrow$: The polynomial $\Gamma_C(X)$ is distinguished from the others by any one of its roots mod $\mathfrak{p}$ by the assumption that $\mathfrak{p} \nmid \operatorname{Res}(\Gamma_C, \Gamma_{C'})$ for $C \neq C'$.

(c) Apply Lemma 8.2. □

Remark 5.4 (choice of h). If the resultants $\operatorname{Res}(\Gamma_C, \Gamma_{C'})$ are nonzero, then Theorem 5.3(b) describes the Frobenius element for all but finitely many primes $\mathfrak{p}$. If one of the resultants vanishes, or equivalently, Γ_C has a common factor with some $\Gamma_{C'}$, the statement does not apply to C for any $\mathfrak{p}$. However, this is rare and easily avoided by choosing a different h; most choices will work by Theorem 5.3(c).

Alternatively, for any fixed h with $1 < \deg h < n$ it is possible to replace f by another polynomial $\tilde{f}$ of degree n with the same splitting field so that the resulting Γ_C are coprime. To see this, consider

$$\gamma_C(X) = \prod_{\sigma \in C}\Big(X - \sum_{j=1}^n h(x_j)x_{\sigma(j)}\Big),$$

and note that they are coprime as polynomials in X over $K(x_1, \ldots, x_n)$. Now apply Lemma 8.1(b) to $F_1 = \prod_{C \neq C'} \operatorname{Res}(\gamma_C, \gamma_{C'})$ and $F_2 = 0$. We obtain a Zariski dense open set of polynomials $B(t)$ of degree at most $n-1$ for which $\tilde{f} = \prod_j (x - B(a_j))$ works.

Remark 5.5 (Euler's criterion). The classical criterion

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$$

says that $a^{(p-1)/2} = \pm 1$ determines whether $x^2 - a$ has a root modulo p. Similarly, to see whether $x^3 - a$ has a root modulo $p \equiv 1 \bmod 3$ one checks whether $a^{(p-1)/3}$ is 1 or another third root of unity in $\mathbb{F}_p^\times$, etc.

One can reformulate this as a matrix statement: Take a 2×2 matrix M with minimal polynomial $x^2 - a$ (respectively 3×3 and $x^3 - a$). Then M^{p-1} is the scalar matrix with $a^{(p-1)/2}$ or $a^{(p-1)/3}$, respectively, on the diagonal, so its trace determines whether the polynomial has a root in $\mathbb{F}_p$; for example, for $x^3 - a$ the distinction is whether $\frac{1}{3} \operatorname{Tr} M^{p-1}$ is 1 or a root of $x^2 + x + 1$.

Theorem 5.3 generalises this to arbitrary polynomials over global fields. Observe that for a polynomial

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0,$$

the trace in the theorem can be interpreted as a trace of a matrix, for instance,

$$\operatorname{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^d) = \operatorname{Tr} \begin{pmatrix} & & -c_0 \\ 1 & & -c_1 \\ & \ddots & \vdots \\ & 1 & -c_{n-1} \end{pmatrix}^d \bmod q.$$

Therefore (a minor modification of) the trace $\operatorname{Tr} M^{q-1}$ for a matrix M with minimal polynomial f determines the splitting behaviour of $f \bmod \mathfrak{p}$ and the conjugacy class of Frobenius, in the same way as above. See also Sections 1 and 7.

Remark 5.6 (ramified primes). The condition that $\mathfrak{p}$ does not divide any resultant $\operatorname{Res}(\Gamma_C, \Gamma_{C'})$ excludes all primes that ramify in the splitting field of f over K. Indeed, if $\sigma \neq 1$ is an element of inertia at $\mathfrak{q}$ for some $\mathfrak{q} \mid \mathfrak{p}$, it is easy to see that $\Gamma_{[1]}$ and $\Gamma_{[\sigma]}$ have a common root mod $\mathfrak{p}$.

Remark 5.7 (extending to all $\mathfrak{p}$). In order to deal with the primes dividing the resultants, we may work over the completion $K_\mathfrak{p}$ instead of the residue field $\mathbb{F}_q$. Compute the splitting field $L/K_\mathfrak{p}$ of f and the roots $b_1, \ldots, b_n$. Choose a lift Ψ of the Frobenius element in $\operatorname{Gal}(L/K_\mathfrak{p})$ and evaluate

$$\sum_{j=1}^{n} h(b_j)\Psi(b_j).$$

This number is now a root of precisely one of the Γ_C, and this C is the conjugacy class of the chosen Frobenius lift Ψ. (See Corollary 4.5.)

Remark 5.8 (Artin L-functions). Suppose L/K is a Galois extension of number fields with Galois group G, represented as a splitting field of some polynomial $f(x) \in K[x]$. Recall that a complex representation ρ of G is called an *Artin*

representation. It has an L-series defined by the Euler product over all primes of K,

$$L(\rho, s) = \prod_{\mathfrak{p}} \frac{1}{P_{\mathfrak{p}}(q^{-s})}\,.$$

Here q is the size of the residue field at $\mathfrak{p}$ and $P_{\mathfrak{p}}(T) = \det(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \mid \rho^{I_{\mathfrak{p}}})$ is the inverse characteristic polynomial of Frobenius on the subspace of ρ fixed by the inertia group $I_{\mathfrak{p}}$ at $\mathfrak{p}$.

Theorem 5.3 and Remark 5.7 allow us to explicitly compute the coefficients of such L-series. For the unramified primes, they recover the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ in G, which determines the local polynomial $P_{\mathfrak{p}}(T)$. For the ramified primes, it suffices to find the restriction of ρ to the local Galois group $G_{\mathfrak{p}}$ at $\mathfrak{p}$ with respect to an embedding $G_{\mathfrak{p}} \hookrightarrow G$ as a decomposition group. Assuming we can find $G_{\mathfrak{p}}$, Remark 5.7 enables us to identify the conjugacy class in G of any element of $G_{\mathfrak{p}}$, under this embedding. This is sufficient to compute the character of ρ on $G_{\mathfrak{p}}$, and thus also $\rho^{I_{\mathfrak{p}}}$ and $P_{\mathfrak{p}}(T)$. Note that we have *not* actually found the decomposition group at $\mathfrak{p}$ as a *subgroup* of G, which appears to be a harder problem.

This algorithm to compute Frobenius elements and L-series of Artin representations has now been implemented in Magma [Bosma et al. 1997]. For the functional equation of the L-series one also needs to identify the conjugacy class of the complex conjugation. If G is represented as acting on the roots of f in a p-adic field, this can be done with the same method. (See Corollary 4.5 and Example 4.6.)

Remark 5.9 (complexity). From the complexity point of view, the computation of Frobenius elements for "good" primes has two steps:

One is the initial precomputation of the polynomials Γ_C, each of which takes $O(n|C|)$ operations in some field containing the a_j (for instance $\mathbb{C}$ or $\overline{\mathbb{Q}}_p$). This needs to be done for all conjugacy classes that are not determined by their cycle type.

The second step deals with a specific prime $\mathfrak{p}$ of K with residue field $\mathbb{F}_q$. We determine the cycle type of $\mathrm{Frob}_{\mathfrak{p}}$ by computing $\gcd(f, x^{q^j} - x)$ for $j \le n/2$, which takes $O(n \log q)$ multiplications of $n \times n$ matrices over $\mathbb{F}_q$. Then we evaluate the trace $\mathrm{Tr}(h(x)x^q)$ with another $O(n + \log q)$ matrix multiplications. Finally, we substitute the trace into all Γ_C corresponding to the cycle type of $\mathrm{Frob}_{\mathfrak{p}}$, which is $O(d)$ coefficient reductions and multiplications in $\mathbb{F}_q$, where d is the number of elements in G of this cycle type.

Here is as an illustration for polynomials of degree at most 11. There are 474 transitive groups G on at most 11 points, for each of which we took a polynomial $f \in \mathbb{Q}[x]$ with $\mathrm{Gal}\, f = G$ as a permutation group on the roots. (We used the database in Magma [Bosma et al. 1997, V2.16].) For each G we computed Frob_p for all $p < 100000$ with $p \nmid \Delta_f$, using Serre's trick (Example 3.9) and the algorithm

above. Together with the Galois group computation and the precomputation of the Γ_C this took under 15 seconds on a 3GHz dual-core CPU for each G, with only four exceptions: $G = \mathrm{A}_5^2 \rtimes \mathrm{C}_2$, $\mathrm{A}_5^2 \rtimes \mathrm{C}_2^2$, $\mathrm{A}_5^2 \rtimes \mathrm{C}_4$ and M_{11}. These took 17, 254, 1512 and 61 seconds respectively, with approximately 10–30 seconds taken by computing Frobenius elements and the rest by precomputing the $\Gamma_C(x)$. These four groups have large conjugacy classes of the same cycle type (the largest being the two classes of size 1800 for $\mathrm{A}_5^2 \rtimes \mathrm{C}_4$).

Remark 5.10 (additional symmetries). Suppose all conjugacy classes of elements of some order o and a fixed cycle type are closed under the power maps $g \mapsto g^k$ for k in some nontrivial subgroup $H \subset (\mathbb{Z}/o\mathbb{Z})^\times$ (for instance they are self-inverse, like in dihedral groups). Then one may replace $\Gamma_C(X)$ in Theorem 5.3 by

$$\prod_\sigma \Big(X - \sum_{j=1}^{n} h(a_j) \Big(\sum_{k \in H} \sigma^k(a_j) \Big) \Big),$$

taking the product over some representatives for C modulo the action of H, and modifying the trace accordingly. In practice, this speeds up the computation of the Γ_C, as their degree drops by a factor of $|H|$.

6. Examples: Abelian groups

If the Galois group is abelian, its conjugacy classes are of size 1, and all the Γ_C of Theorem 5.3 are linear, that is, $\Gamma_C(X) = X - r_C$ with $r_C \in K$. For a good choice of $h(x)$ and all but finitely many primes $\mathfrak{p}$, the trace $\mathrm{Tr}(h(x)x^q)$ agrees with exactly one of the r_C modulo $\mathfrak{p}$, which then determines the conjugacy class of $\mathrm{Frob}_\mathfrak{p}$.

In the examples below, ζ_n denotes a primitive n-th root of unity.

Example 6.1. Let $K = \mathbb{Q}(i)$ and

$$f(x) = x^4 + 2x^3 + (3+3i)x^2 + 4ix - 1 + i.$$

Its complex roots are

$$a_1 = -0.31795 - 0.57510i, \qquad a_2 = 0.50870 - 1.1289i,$$
$$a_3 = -1.4682 + 1.8471i, \qquad a_4 = -0.72255 - 0.14308i,$$

to 5 decimal places. The splitting field L is a C_4-extension of $\mathbb{Q}(i)$, non-Galois over $\mathbb{Q}$, and the Galois group of L/K is $\langle (1234) \rangle < \mathrm{S}_4$. Take $h(x) = x^2$. An elementary computation gives

$$\Gamma_{[\mathrm{id}]} = X - (10+6i), \qquad \Gamma_{[(1234)]} = X - (4+4i),$$
$$\Gamma_{[(13)(24)]} = X - (-2+2i), \qquad \Gamma_{[(1432)]} = X + 8.$$

For a prime $\mathfrak{p} \neq (1+i), (2-i), (3)$ (the primes dividing $r_C - r_{C'}$ for $C \neq C'$) with residue field $\mathbb{F}_q$, we deduce that the Frobenius at $\mathfrak{p}$ is determined by

$\mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(x^{q+2}) \equiv$	$10+6i$	$4+4i$	$-2+2i$	-8
$\mathrm{Frob}_{\mathfrak{p}} =$	id	(1234)	(13)(24)	(1432)

Example 6.2 (Kummer extensions). Suppose $\zeta = \zeta_n \in K$ and $L = K(\sqrt[n]{s})$ is a Kummer extension of degree n. It is abelian with Galois group C_n whose elements are determined by

$$\sigma_i : \sqrt[n]{s} \mapsto \zeta^i \sqrt[n]{s} \quad \text{for } i = 1, \dots, n.$$

Take $f(x) = x^n - s$ and $h(x) = x^{n-1}$. Then

$$\Gamma_{[\sigma_i]}(X) = X - \sum_{j=1}^{n} h(\zeta^j \sqrt[n]{s})\sigma_i(\zeta^j \sqrt[n]{s}) = X - ns \cdot \zeta^i.$$

For a prime $\mathfrak{p}$ of K with residue field $\mathbb{F}_q$, because $n \mid q-1$, we have

$$\begin{aligned}\mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(h(x)x^q) &= \mathrm{Tr}_{(\mathbb{F}_q[x]/x^n-s)/\mathbb{F}_q}(x^{q+n-1}) \\ &= \mathrm{Tr}_{(\mathbb{F}_q[x]/x^n-s)/\mathbb{F}_q}(s^{(q-1)/n+1}) = ns \cdot s^{(q-1)/n}.\end{aligned}$$

So Theorem 5.3 says that for $\mathfrak{p} \nmid ns$,

$$\mathrm{Frob}_{\mathfrak{p}} = \sigma_i \quad \Longleftrightarrow \quad s^{(q-1)/n} \equiv \zeta^i \mod \mathfrak{p},$$

which is the classical criterion for Kummer extensions.

Example 6.3 ($\mathbb{Q}(\zeta_p)/\mathbb{Q}$). Let $\zeta = \zeta_p$ for some prime $p > 2$, and take

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\zeta), \quad f(x) = x^{p-1} + \cdots + x + 1.$$

Thus $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, with elements $\sigma_i : \zeta \mapsto \zeta^i$ for $i = 1, \dots, p-1$. For $h(x) = x^2$ we have $\Gamma_{[\sigma_i]}(X) = X - r_i$ with $r_i \in \mathbb{Q}$ given by

$$r_i = \sum_{j=1}^{p-1} (\zeta^j)^2 \sigma_i(\zeta^j) = \sum_{j=1}^{p-1} \zeta^{j(2+i)} = \begin{cases} -1 & \text{if } i \neq p-2, \\ p-1 & \text{if } i = p-2. \end{cases}$$

For a prime q of $\mathbb{Q}$,

$$\begin{aligned}\mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(h(x)x^q) &= \mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(x^{q+2}) \equiv \mathrm{Tr}_{(\mathbb{Z}[x]/f(x))/\mathbb{Z}}(x^{q+2}) \mod q \\ &\equiv \mathrm{Tr}_{F/\mathbb{Q}}(\zeta^{q+2}) \equiv \begin{cases} -1 \mod q & \text{if } p \nmid q+2, \\ p-1 \mod q & \text{if } p \mid q+2. \end{cases}\end{aligned}$$

Hence Theorem 5.3(b) shows that for all $q \neq p$,

$$\mathrm{Frob}_q = \sigma_{p-2} \quad \Longleftrightarrow \quad q \equiv -2 \mod p.$$

The same computation with $h(x) = x^{p-k}$ for varying k yields the classical criterion

$$\mathrm{Frob}_q = \sigma_k \quad \Longleftrightarrow \quad q \equiv k \mod p.$$

Note that none of these $h(x)$ work for all conjugacy classes simultaneously, because the $\Gamma_{[\sigma_j]}$ are not coprime. This tends to happen when the roots of f are "too nice" and $h(x)$ is "too simple". By Lemma 8.2, most h do work. In our example, a general polynomial

$$h(x) = \lambda_1 x^{p-1} + \cdots + \lambda_{p-1} x + \lambda_p \quad \text{has } \Gamma_{[\sigma_i]}(X) = X + h(1) - p\lambda_i,$$

and these are distinct if and only if $\lambda_1, \ldots, \lambda_{p-1}$ are. The primes to which the theorem then applies are those not dividing $p \prod(\lambda_i - \lambda_j)$.

Example 6.4 (cyclotomic extensions). In general, suppose $L = K(\zeta_n)$ is some cyclotomic extension, and $f(x)$ is the minimal polynomial of ζ_n over K. As in the previous example, $G = \mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, and we write σ_i for the automorphism with $\sigma_i(\zeta_n) = \zeta_n^i$. We do the same computation as above: For $h(x) = x^k$ and $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$,

$$\Gamma_{[\sigma_i]}(X) = X - \sum_{g \in G} g(\zeta_n)^k \sigma_i(g(\zeta_n)) = X - \sum_{g \in G} g(\zeta_n)^{k+i} = X - \mathrm{Tr}_{L/K}(\zeta_n^{k+i}),$$
$$\mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(x^{k+q}) \equiv \mathrm{Tr}_{L/K}(\zeta_n^{k+q}) \mod \mathfrak{p}.$$

Because $\mathrm{Tr}_{L/K}(\zeta_n^j)$ is $|G|$ precisely when $n \mid j$, the polynomial $\Gamma_{[\sigma_{n-k}]}$ differs from all the other $\Gamma_{[\sigma_j]}$, and we find that

$$\mathrm{Frob}_\mathfrak{p} = \sigma_{n-k} \quad \Longleftrightarrow \quad q \equiv n - k \mod n$$

for almost all $\mathfrak{p}$. (One may improve "almost all" to "all $\mathfrak{p} \nmid n$" by taking several h.)

Remark 6.5. The fact that we obtained a simple formula for Frobenius elements for cyclotomic and Kummer extensions relied on the existence of a universal expression for the trace $\mathrm{Tr}(h(x)x^q) \bmod \mathfrak{p}$. It follows from class field theory that there are such formulas in all abelian extensions.

For instance, consider Example 6.1 of a C_4-extension of $K = \mathbb{Q}(i)$ from the point of view of class field theory. There the conductor of L/K is

$$N = (1+i)^4(2-i) = 8 - 4i,$$

and the group $(\mathbb{O}_K/N)^\times$ is $C_4 \times C_4 \times C_2$, with generators i, 7 and $3 - 2i$, respectively. For a prime $\mathfrak{p} = (\alpha) \subset \mathbb{Z}[i]$ not dividing N, if $\alpha \equiv i^a 7^b (3-2i)^c \bmod N$, then $\mathrm{Frob}_\mathfrak{p} = (1234)^b$.

Now compare this with the description of Frobenius in Example 6.1. Writing $\mathbb{F}_q = \mathbb{Z}[i]/\mathfrak{p}$ and Tr for $\mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}$, we get 4 congruences for the traces:

$$\begin{aligned}
&\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^0(3-2i)^c \mod N &&\iff \mathrm{Tr}(x^{q+2})\equiv 10+6i &&\mod \mathfrak{p},\\
&\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^1(3-2i)^c \mod N &&\iff \mathrm{Tr}(x^{q+2})\equiv 4+4i &&\mod \mathfrak{p},\\
&\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^2(3-2i)^c \mod N &&\iff \mathrm{Tr}(x^{q+2})\equiv -2+2i &&\mod \mathfrak{p},\\
&\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^3(3-2i)^c \mod N &&\iff \mathrm{Tr}(x^{q+2})\equiv -8 &&\mod \mathfrak{p}
\end{aligned}$$

for $\mathfrak{p}\neq(1+i),(2-i),(3)$.

Note that if one had a way to prove these congruences directly, one would have a proof of Artin reciprocity in the extension L/K.

7. Examples: Nonabelian groups

We continue with examples to Theorem 5.3. When G is nonabelian, the only difference is that the Γ_C are no longer linear.

Example 7.1. Let $K=\mathbb{Q}$ and $f(x)=x^3-2$. It has Galois group S_3 and roots $a_1=\sqrt[3]{2}$, $a_2=\zeta\sqrt[3]{2}$ and $a_3=\zeta^2\sqrt[3]{2}$, where ζ is a primitive cube root of unity. Take $h(x)=x^2/6$ (the factor $\frac16$ is only chosen for convenience) and compute the polynomials Γ_C for the three conjugacy classes:

$$\begin{aligned}
\Gamma_{[\mathrm{id}]} &= X-\tfrac16(a_1^2a_1+a_2^2a_2+a_3^2a_3)\\
&= X-1,\\
\Gamma_{[(12)]} &= (X-\tfrac16(a_1^2a_2+a_2^2a_1+a_3^3))(X-\tfrac16(a_1^2a_3+a_2^3+a_3^2a_1))\\
&\qquad\qquad\cdot(X-\tfrac16(a_1^3+a_2^2a_3+a_3^2a_2))\\
&= (X-\tfrac13(\zeta+\zeta^2+1))(X-\tfrac13(\zeta^2+1+\zeta))(X-\tfrac13(1+\zeta+\zeta^2))\\
&= X^3,\\
\Gamma_{[(123)]} &= (X-\tfrac16(a_1^2a_2+a_2^2a_3+a_3^2a_1))(X-\tfrac16(a_1^2a_3+a_2^2a_1+a_3^2a_2))\\
&= (X-\tfrac13(\zeta+\zeta+\zeta))(X-\tfrac13(\zeta^2+\zeta^2+\zeta^2))=(X-\zeta)(X-\zeta^2)\\
&= X^2+X+1.
\end{aligned}$$

On the other hand, for a rational prime $q=3m+k$ with $k=1$ or 2,

$$\begin{aligned}
\mathrm{Tr}_{(\mathbb{F}_q[x]/x^3-2)/\mathbb{F}_q}\big(\tfrac16 x^{q+2}\big) &= \mathrm{Tr}\big(\tfrac16 2^{m+1}x^{k-1}\big)\\
&= \begin{cases} 2^m & \text{if } k=1,\\ 0 & \text{if } k=2\end{cases}\\
&= \begin{cases} 2^{(q-1/3)} & \text{if } q\equiv 1 \bmod 3,\\ 0 & \text{if } q\equiv 2 \bmod 3.\end{cases}
\end{aligned}$$

The conclusion of Theorem 5.3 is that, as expected, for $q \neq 2, 3$,

$$\begin{aligned} q \equiv 1 \bmod 3, 2 \in (\mathbb{F}_q)^{\times 3} &\implies \mathrm{Frob}_q = \mathrm{id}, \\ q \equiv 1 \bmod 3, 2 \notin (\mathbb{F}_q)^{\times 3} &\implies \mathrm{Frob}_q \in [(123)], \\ q \equiv 2 \bmod 3 &\implies \mathrm{Frob}_q \in [(12)]. \end{aligned}$$

Clearly, an identical computation goes through for $f(x) = x^3 - c$ (with $h(x) = x^2/3c$) over any global field K with $\zeta \notin K$.

We can also take a general cubic polynomial and obtain an analogue of Euler's criterion for its factorisation modulo primes:

Theorem 7.2. *Let $f(x) = x^3 + bx + c$ be a separable cubic polynomial over a global field K, and $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$. Write*

$$T = \mathrm{Tr}_{(\mathbb{F}_q[x]/f(x))/\mathbb{F}_q}(x^{q+1}) = \mathrm{Tr} \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & 0 \end{pmatrix}^{q+1} \bmod \mathfrak{p}.$$

If $\mathfrak{p}$ does not divide $3b(4b^3 + 27c^2)$ and the denominators of b and c, then

$$\begin{aligned} T \equiv -2b \bmod \mathfrak{p} &\iff f(x) \text{ has 3 roots mod } \mathfrak{p}, \\ T \equiv \quad b \bmod \mathfrak{p} &\iff f(x) \text{ is irreducible mod } \mathfrak{p}, \\ T \text{ is a root of } x^3 - 3b^2x - 2b^3 - 27c^2 &\iff f(x) \text{ has 1 root mod } \mathfrak{p}. \end{aligned}$$

Proof. We compute the polynomials Γ_C for $G = \mathrm{S}_3$, $h(x) = x$ by expressing their coefficients in terms the elementary symmetric functions $a_1 + a_2 + a_3 = 0$, $a_1a_2 + a_2a_3 + a_3a_1 = b$ and $a_1a_2a_3 = -c$:

$$\begin{aligned} \Gamma_{[\mathrm{id}]} &= X - (a_1^2 + a_2^2 + a_3^2) = X - (a_1 + a_2 + a_3)^2 + 2(a_1a_2 + a_1a_3 + a_2a_3) \\ &= X + 2b, \\ \Gamma_{[(12)]} &= (X - (a_1a_2 + a_2a_1 + a_3^2))(X - (a_1a_2 + a_2a_1 + a_3^2)) \\ &\qquad \cdot (X - (a_1a_2 + a_2a_1 + a_3^2)) \\ &= X^3 - 3b^2X - 2b^3 - 27c^2, \\ \Gamma_{[(123)]} &= (X - (a_1a_2 + a_2a_3 + a_3a_1))(X - (a_1a_3 + a_2a_1 + a_3a_2)) \\ &= (X - b)^2. \end{aligned}$$

The least common multiple of their pairwise resultants is $3b(4b^3 + 27c^2)$, which completes the proof by Theorem 5.3. □

An identical computation can be done for polynomials of higher degree, as long as one has the patience to work out the coefficients of the Γ_C. Here is the corresponding result for quartics:

Theorem 7.3. *Let $f(x)=x^4+bx^2+cx+d$ be a separable quartic polynomial over K, and $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$. Then the value*

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1})$$

is a root of one of the polynomials

$$\begin{aligned}
\Gamma_{[\mathrm{id}]} &= X+2b,\\
\Gamma_{[(12)(34)]} &= X^3-2bX^2-16dX+32bd-8c^2,\\
\Gamma_{[(12)]} &= X^6+4bX^5+(2b^2+8d)X^4+(-12b^3+48bd-26c^2)X^3\\
&\quad -(23b^4-120b^2d+108bc^2+112d^2)X^2\\
&\quad -(16b^5-128b^3d+138b^2c^2+256bd^2+216c^2d)X-4b^6\\
&\quad +48b^4d-56b^3c^2-192b^2d^2-288bc^2d-27c^4+256d^3,\\
\Gamma_{[(123)]} &= X^4+(-2b^2+8d)X^2-8c^2X+b^4-8b^2d+8bc^2+16d^2,\\
\Gamma_{[(1234)]} &= X^3-2bX^2+(b^2-4d)X+c^2.
\end{aligned}$$

If $\mathfrak{p}$ does not divide the denominators of b, c and d and the pairwise resultants of the Γ_C, then this determines the degrees in the factorisation of $f \bmod \mathfrak{p}$: They are the cycle lengths of the permutation in the index of Γ.

A theorem of Brumer (see [Jensen et al. 2002, Theorem 2.3.5]) states that any Galois extension L/K with Galois group $G=\mathrm{D}_{10}$ is a splitting field of

$$f_{a,b}(x)=x^5+(a-3)x^4+(b-a+3)x^3+(a^2-a-1-2b)x^2+bx+a$$

for some $a, b \in K$. Using a similar argument to $G=\mathrm{S}_3$ and S_4, we find:

Theorem 7.4. *Suppose L/K is the splitting field of $f_{a,b}(x)$ as above, with*

$$G=\mathrm{Gal}(L/K)\cong \mathrm{D}_{10}.$$

If $\mathfrak{p}$ is a prime of K with residue field $\mathbb{F}_q$, not dividing $3a-b+1$ and the denominators of a and b and such that $f \bmod \mathfrak{p}$ is irreducible, then

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1})$$

is either $-2a+b+1$ or $a+2$ modulo $\mathfrak{p}$. This determines which of the two conjugacy classes of 5-cycles contains $\mathrm{Frob}_{\mathfrak{p}}$.

Remark 7.5. In this setting, if $\mathrm{Frob}_{\mathfrak{p}}$ is not a 5-cycle, it is either the identity or an element of order 2. In the former case,

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1})=a^2-4a-2b+3 \bmod \mathfrak{p};$$

in the latter the trace is a root of

$$\begin{aligned}
&\Gamma_{[(23)(45)]}\\
&= X^5-(a-3)^2X^4+(31-2a^3+4b-3b^2+a^2(11+2b)-2a(21+2b))X^3\\
&\quad+(12a^3(3+2b)-a^2(137+44b)+a(114+6b-28b^2)\\
&\qquad -51+7a^4-4a^5-20b+14b^2-2b^3)X^2\\
&\quad+(40+16a^5-8a^6+32b-17b^2-4b^3+a^4(58+42b)+a^2(182+18b-52b^2)\\
&\qquad +4a^3(-49-21b+b^2)-2a(65+13b-17b^2+6b^3))X\\
&\quad+8a^6-4a^7+4a^5(7+5b)-4a^4(32+17b)+2a^3(123+85b+4b^2)\\
&-a^2(245+218b+24b^2)-2a(-30-6b+51b^2+22b^3)+2(-6-8b+3b^2+b^3-4b^4).
\end{aligned}$$

Example 7.6. Here is another example, to illustrate what the Γ_C look like in general. Take $K=\mathbb{Q}$ and $L=\mathbb{Q}(E[3])$, the 3-torsion field of the elliptic curve $E: y^2+y=x^3-x^2$. Then $\mathrm{Gal}(L/K)\cong \mathrm{GL}_2(\mathbb{F}_3)$, and L is the splitting field of

$$f(x)=x^8-9x^7+18x^6+33x^5-93x^4-15x^3-23x^2-36x-27.$$

The Γ_C for $h(x)=x^2$ are

$$\begin{aligned}
\Gamma_{[\mathrm{id}]} &= X-144,\\
\Gamma_{[(13)(24)(56)(78)]} &= X-3,\\
\Gamma_{[(24)(57)(68)]} &= X^{12}-699X^{11}+204666X^{10}-32922129X^9+3212225793X^8\\
&\quad -196600821903X^7+7340079612456X^6-145234777501584X^5\\
&\quad +566948224573848X^4+2674770056244808 2X^3\\
&\quad -187604198442957555X^2-2946247136394353892X\\
&\quad -24290099658154516203,\\
\Gamma_{[(148)(273)]} &= X^8-546X^7+120102X^6-14088342X^5+989228043X^4\\
&\quad -43566817716X^3+1248800990265X^2-21583664066961X\\
&\quad +167939769912993,\\
\Gamma_{[(1432)(5768)]} &= X^6-258X^5+26448X^4-1344378X^3+34859664X^2\\
&\quad -445164021X+2926293624,\\
\Gamma_{[(174382)(56)]} &= X^8-264X^7+29292X^6-1698042X^5+51288993X^4\\
&\quad -654852960X^3+3360584547X^2-277935306777X+7299371089503,\\
\Gamma_{[(15473628)]} &= X^6-258X^5+26250X^4-1336755X^3+35700471X^2\\
&\quad -477465444X+2707751520,\\
\Gamma_{[(16483527)]} &= X^6-258X^5+28230X^4-1674048X^3+57362760X^2\\
&\quad -1097286921X+9616023198.
\end{aligned}$$

Example 7.7. As an indication of the kind of Artin L-series that may be numerically computed, we give an example with a big Galois group over $\mathbb{Q}$. We take $G=\mathrm{PGSp}(4,\mathbb{F}_3)$ of order 51840, realised through the Galois action on the 3-torsion of the Jacobian of a genus 2 curve, and evaluate the Artin L-series of an irreducible 6-dimensional representation of G.

Specifically, G is the unique double cover of the simple group $\mathrm{Sp}(4,\mathbb{F}_3)/\mathbb{F}_3^\times$ in $\mathrm{PGL}(4,\mathbb{F}_3)=\mathrm{GL}(4,\mathbb{F}_3)/\mathbb{F}_3^\times$. To obtain it as a Galois group, take the hyperelliptic curve

$$\mathscr{C}/\mathbb{Q}: y^2-(x^2+1)y=x^5-x^4+x^3-x^2.$$

Consider the field $\mathbb{Q}(J[3])$ obtained by adjoining to $\mathbb{Q}$ the coordinates of the 3-torsion points of its Jacobian $J/\mathbb{Q}$. Then $\mathrm{Gal}(\mathbb{Q}(J[3])/\mathbb{Q})$ is $\mathrm{GSp}(4,\mathbb{F}_3)$. The group we want is $G=\mathrm{GSp}(4,\mathbb{F}_3)/\{\pm1\}$, and it can be obtained from the Galois action on the 40 lines through the origin in $J[3]$. Specifically, if $(P)+(Q)-2(O)\in J[3]$ is a nonzero point with $P=(x_P,y_P)$, $Q=(x_Q,y_Q)$, the minimal polynomial f of x_Px_Q over $\mathbb{Q}$ has Galois group G;

$$f=x^{40}+27x^{39}+39x^{38}-61x^{37}+\cdots+2259x^3+3471x^2+1057x+69.$$

In its action on the roots of f, the group has several conjugacy classes of the same cycle type, and the largest Γ_C that we need has degree 2160 (using Remark 5.10).

The group has two irreducible 6-dimensional representations, ρ and ρ' (whose traces on elements of order 10 in G are $+1$ and -1, respectively). The curve $\mathscr{C}$ has good reduction outside 2 and 3, so $L/\mathbb{Q}$ is unramified at all primes $p\neq 2,3$. The conductor of ρ is $2^{10}3^{17}$ and we used our machinery to compute the local polynomials for the Artin L-series $L(\rho,s)$ for primes up to 410203. Using Magma [Bosma et al. 1997], we then evaluate

$$L(\rho,1)\approx 1.852529796,\qquad L(\rho,2)\approx 1.119877506,$$

to 10-digit precision. This computation relies implicitly on the validity of Artin's conjecture for ρ. It took half an hour on a 3GHz dual-core CPU to compute $\mathrm{Gal}(f/\mathbb{Q})$, 5 hours for the Γ_C, 3 hours for the local information at $p=2$, and 3 (ramification groups, conductor exponents etc.), 3 minutes for the Frobenius elements and the local polynomial computation and half an hour for each of the L-values.

8. Appendix: Two lemmas on Zariski density

Lemma 8.1. *Suppose K is an infinite field, $f\in K[t]$ is a separable polynomial of degree n and $a_1,\dots,a_n$ are its roots in some splitting field L.*

(a) *If $F,G\in K[x_1,\dots,x_n]$ take the same values on*

$$x_1=\beta_0+\beta_1a_1+\cdots+\beta_{n-1}a_1^{n-1},\dots,x_n=\beta_0+\beta_1a_n+\cdots+\beta_{n-1}a_n^{n-1}$$

for all $[\beta_1,\dots,\beta_n]\in K^n$, then $F=G$.

(b) *Suppose $F_1,\dots,F_d\in K[x_1,\dots,x_n]$ are distinct. There exists a polynomial $B(t)=\beta_0+\cdots+\beta_{n-1}t^{n-1}\in K[t]$ such that $B(a_1),\dots,B(a_n)$ generate L and*

the F_i take distinct values on $[B(a_1), \dots, B(a_n)]$. The set of such B contains a Zariski dense open subset of $K \oplus Kt \oplus \cdots \oplus Kt^{n-1}$.

(c) *Let F be a T-invariant for some $T < \mathrm{S}_n$. There is a Zariski dense open set of polynomials $B(t) \in K \oplus Kt \oplus \cdots \oplus Kt^{n-1}$ for which $\boldsymbol{a}' = [B(a_1), \dots, B(a_n)]$ generate L and $e^F_{\boldsymbol{a}'} : T \setminus \mathrm{S}_n \to L$ is injective.*

Proof. (a) Let $U = K(t_1, \dots, t_n)$. As a first step, we observe that K^n is Zariski dense in $\mathbb{A}^n_U = U^n$: This is clear for $n = 1$ as K is infinite; generally, if K^n were not Zariski dense, it would be contained in a (not necessarily irreducible) hypersurface of some degree d, so it would contain at most d hyperplanes. But, by induction, it contains all $\{r\} \times U^{n-1}$ for all $r \in K$, which gives a contradiction.

Therefore, as F and G are continuous in the Zariski topology, they agree on all of U^n, that is, on all the combinations above with $[\beta_1, \dots, \beta_n] \in U^n$. Now solve the system of equations $\sum_{j=0}^{n-1} a_i^j \beta_j = t_j$ for $\beta_1, \dots, \beta_n$. (This is possible because $a_i \neq a_k$ for $i \neq k$, so the Vandermonde matrix is invertible.) Using this solution we find that $F(t_1, \dots, t_n) = G(t_1, \dots, t_n)$, so $F = G$ as polynomials.

(b) Put $F(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j)(F_i - F_j)$ and $G = 0$ and apply (a). This gives a polynomial $B(t) = \beta_0 + \cdots + \beta_{n-1}t^{n-1} \in K[t]$ that clearly satisfies the "distinct values" condition. Furthermore, $B(a_i) \neq B(a_j)$ guarantees the "generate L" condition as well: The Galois action permutes the $B(a_i)$ in the same way as the a_i, so the Galois group has the same order. Finally, consider $F(B(a_1), \dots, B(a_n))$ as a polynomial in $\beta_0, \dots, \beta_{n-1}$. Its zero set is Zariski closed in $\mathbb{A}^n$ and we proved that its complement is nonempty. This proves the last claim.

(c) Apply (b) to the set of polynomials $\{F^\sigma\}_{\sigma \in T \setminus \mathrm{S}_n}$, using that, by definition, $e^F_{\boldsymbol{a}'}(\sigma^{-1}) = F((\boldsymbol{a}')^{\sigma^{-1}}) = F^\sigma(\boldsymbol{a}')$. □

Lemma 8.2. *Suppose K is an infinite field, $f \in K[t]$ is a separable polynomial of degree n and $a_1, \dots, a_n$ are its roots in some splitting field L. Then on a Zariski dense open set of polynomials $h(x)$ in $K \oplus Kx \oplus \cdots \oplus Kx^{n-1} \cong \mathbb{A}^n_K$, the values*

$$v_h(\sigma) = \sum_{j=1}^{n} h(a_j)\sigma(a_j)$$

for $\sigma \in G = \mathrm{Gal}(L/K)$ are distinct.

Proof. For any $\sigma \in G$, the map $E_\sigma : h \mapsto v_h(\sigma)$ is K-linear $K^n \to L$. So E_σ agrees with E_τ on a K-linear subspace for every $\sigma, \tau \in G$. If none of these subspaces is all of K^n, then the complement of their union is the desired set (nonempty since K is infinite). It remains to prove that $E_\sigma \neq E_\tau$ for $\sigma \neq \tau$.

Suppose $E_\sigma = E_\tau : K^n \to L$. Then their extensions by linearity to maps $L^n \to L$ agree as well. In other words, $v_h(\sigma) = v_h(\tau)$ for all h in $L \oplus Lx \oplus \cdots \oplus Lx^{n-1}$. In

particular, taking

$$h(x) = \prod_{j \neq i} (x - a_j)$$

we get that $\sigma(a_i) = \tau(a_i)$. As this holds for all i, it follows that $\sigma = \tau$. □

Acknowledgements

Tim is supported by a Royal Society University Research Fellowship. We would like to thank Robinson College and Gonville & Caius College, Cambridge, where most of this research was carried out.

References

[Booker 2005] A. R. Booker, "Numerical tests of modularity", *J. Ramanujan Math. Soc.* **20**:4 (2005), 283–339. MR 2006k:11090 Zbl 1122.11032

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Buhler 1978] J. P. Buhler, *Icosahedral Galois representations*, Lecture Notes in Mathematics **654**, Springer, Berlin, 1978. MR 58 #22019 Zbl 0374.12002

[Jensen et al. 2002] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials: Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications **45**, Cambridge University Press, 2002. MR 2004d:12007 Zbl 1042.12001

[Roberts 2004] D. P. Roberts, "Frobenius classes in alternating groups", *Rocky Mountain J. Math.* **34**:4 (2004), 1483–1496. MR 2005m:12004 Zbl 1138.12306

[Zagier 2008] D. Zagier, "Elliptic modular forms and their applications", pp. 1–103 in *The 1-2-3 of modular forms*, edited by K. Ranestad, Springer, Berlin, 2008. MR 2010b:11047 Zbl 05808162

Communicated by Bjorn Poonen
Received 2011-08-04 Revised 2012-05-09 Accepted 2012-06-07

tim.dokchitser@bristol.ac.uk *Department of Mathematics, Bristol University, University Walk, Bristol, BS8 1TW, United Kingdom*
http://www.maths.bris.ac.uk/~matyd/

v.dokchitser@dpmms.cam.ac.uk *Emmanuel College, University of Cambridge, Cambridge, CB2 3AP, United Kingdom*
http://www.dpmms.cam.ac.uk/~vd209/

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1353

Weak approximation for cubic hypersurfaces of large dimension

Mike Swarbrick Jones

We address the problem of weak approximation for general cubic hypersurfaces defined over number fields with arbitrary singular locus. In particular, weak approximation is established for the smooth locus of projective, geometrically integral, nonconical cubic hypersurfaces of dimension at least 17. The proof utilises the Hardy–Littlewood circle method and the fibration method.

1. Introduction

Let k be an algebraic number field. The possible existence and structure of k-rational points on hypersurfaces defined over k is a major theme in number theory and arithmetic geometry. Let $X \subset \mathbb{P}^{n-1}_k$ be a variety defined over k. Given a place v of k, define k_v to be the completion with respect to that place. If X is smooth, recall that *weak approximation* holds for X if $X(k) \neq \varnothing$ and the image of the diagonal embedding

$$X(k) \to \prod_{v \in S} X(k_v)$$

is dense for any finite set of places S. Given a possibly singular X, we shall consider weak approximation for X_{smooth}, the smooth locus of X.

We say that X is k-rational if there is a k-birational map $\mathbb{P}^{n-1}_k \dashrightarrow X$. Weak approximation is a birational invariant of smooth integral varieties, and since weak approximation holds on $\mathbb{P}^m_k$ for any positive integer m, it must hold for any smooth k-rational variety.

A classical observation is that a quadric k-hypersurface Q with a nonsingular k-point will be k-rational, provided it is geometrically integral. Essentially this is because we can parameterise the surface by lines through the k-point. In this case, the smooth locus of the quadric satisfies weak approximation. The Hasse–Minkowski theorem implies that $Q_{smooth}(k) \neq \varnothing \iff Q_{smooth}(k_v) \neq \varnothing$ for all places v of k.

MSC2010: primary 11G35; secondary 11D25, 11D72, 11P55, 14G25.
Keywords: cubic hypersurfaces, weak approximation, local-global principles, fibration method, circle method, many variables.

For larger degree hypersurfaces, relatively little is known. The emergence of counterexamples to weak approximation, even when rational points are present, is an indication that the situation is much more complex. For instance, with $k = \mathbb{Q}$ we have a cubic surface from [Swinnerton-Dyer 1962],

$$x_1(x_2^2 + x_3^2) = (4x_4 - 7x_1)(x_4^2 - 2x_1^2). \tag{1-1}$$

Ignoring the subvariety $x_1 = x_4 = 0$, this has two components over the reals: one with $x_4/x_1 \geq 7/4$, which contains infinitely many rational points, and the other with $|x_4/x_1| \leq \sqrt{2}$, which contains none. Clearly then this fails weak approximation. This counterexample can be accounted for by the *Brauer–Manin obstruction*. A conjecture of Colliot-Thélène [2003] states that this will be the only such obstruction for rationally connected varieties such as cubic hypersurfaces of dimension at least 2.

Suppose (once and for all) that $Y \subset \mathbb{P}_k^{n-1}$ is a geometrically integral, nonconical cubic hypersurface given by the zero locus of a cubic form $C \in k[x_1, \ldots, x_n]$. The Brauer group of Y_{smooth} will be trivial if its dimension is at least 3, and the codimension of the singular locus is at least 4 (see the appendix by Colliot-Thélène in [Browning 2010]). Thus, we expect that these assumptions, together with $Y_{smooth}(k) \neq \varnothing$, imply that weak approximation holds for Y_{smooth}.

We should note at this point that $Y(k) \neq \varnothing$ for $n \geq 16$ by the Corollary in [Pleasants 1975]. Furthermore, $Y(K) \neq \varnothing \Longrightarrow Y_{smooth}(K) \neq \varnothing$ for any field K, for example, by [Kollár 2002, Theorem 2.3], and so the Hasse principle holds on Y_{smooth} as soon as $n \geq 16$.

Let us now consider a few cases where weak approximation for Y_{smooth} is known. We shall assume that $Y_{smooth}(k_v) \neq \varnothing$ for all v since otherwise the matter is trivial (this is in fact guaranteed if $n \geq 10$; see, for example, [Birch and Lewis 1960]). First a classical remark: if $Y_{sing}(k) \neq \varnothing$, where Y_{sing} is the singular locus, then we can parameterise Y by means of lines through a rational singular point, so Y is k-rational. If Y contains two conjugate singular points and $n \geq 7$, it follows from work of Harari [1995, §5.1; 1994]. If Y contains three conjugate singular points, it is known for $n = 4$ [Coray 1976, Corollary 2; Coray and Tsfasman 1988, Theorem A] and for $n \geq 6$ [Colliot-Thélène and Salberger 1989], but counterexamples exist for $n = 5$ [ibid., Section 8]. If $n \geq 5$ and Y is smooth and contains a k-rational line, then it follows from §5.2.2 of [Harari 1995]. Finally, Corollary 2 of [Skinner 1997] shows that if Y is smooth, $n \geq 17$ is sufficient.

Note that all the results mentioned so far rely fundamentally on the shape of the singular locus of Y, either that it is empty or contains some arithmetic structure. The aim of this paper is to consider general cubic hypersurfaces Y with arbitrary singular locus and to obtain a reasonable lower bound on the dimension required to guarantee that Y_{smooth} satisfies weak approximation. Our main result is the following:

Theorem A. *Let $Y \subset \mathbb{P}^{n-1}_k$ be a geometrically integral, nonconical cubic hypersurface defined over k. If $n \geq 19$, then Y_{smooth} satisfies weak approximation.*

In a qualitative sense, this result is best possible in that the geometrically integral and nonconical assumptions cannot be eliminated. For example, we could consider the union of a line and a quadric having no nonsingular rational points, or we could take a cone over the surface (1-1).

2. Structure of the proof

Theorem A is related to the result of Skinner [1997, Corollary 2], which was obtained using the Hardy–Littlewood circle method. This is advantageous when the dimension of the singular locus is small. The circle method can also be an effective tool when the equations involved have large 'h-invariant'. This concept was originally introduced by Davenport and Lewis [1964].

Given a cubic form C, define the h-invariant of C, $h = h_k(C)$, as follows: h is the smallest positive integer such that $C(\boldsymbol{x})$ is expressible identically as

$$L_1(\boldsymbol{x})Q_1(\boldsymbol{x}) + \cdots + L_h(\boldsymbol{x})Q_h(\boldsymbol{x}), \tag{2-1}$$

where L_i and Q_i are linear and quadratic forms, respectively, with coefficients in k. Similarly, for the cubic hypersurface Y, we shall define $h_k(Y)$ to mean the h-invariant of the underlying cubic form. Finally, for a cubic polynomial f, we define $h_k(f)$ to be the h-invariant of the homogeneous cubic part of the polynomial. Clearly it is an invariant with respect to nonsingular linear transformations on $\boldsymbol{x}$ over k. Also note that $h_k(Y) \leq n$ with equality if and only if $Y(k) = \varnothing$. Furthermore, if $n \geq h_k(Y)+r+1$, there is a k-rational r-plane contained in Y given by $L_i = 0$ in (2-1).

Our strategy is to show weak approximation for two classes of cubics, the union of which contains all of those considered in Theorem A. The first class is cubics for which the h-invariant is sufficiently large.

Lemma 1. *Suppose we have a geometrically integral, nonconical cubic hypersurface Y defined over k. If $h_k(Y) \geq 16$, then Y_{smooth} satisfies weak approximation.*

To prove this, we take a cue from the concluding remarks of [Skinner 1997] and note that to find k-rational points that are $\mathfrak{p}$-adically close to a $\mathfrak{p}$-adic point, it is sufficient to find *integer* points that are in specific classes modulo $\mathfrak{p}^t$ for some integer t; this is equivalent to finding integral solutions to a cubic polynomial f, where the cubic part has the same h-invariant as the original cubic form. For large h, this problem is tailor-made for the circle method. Indeed, we will use a mild generalisation of a previous result of Pleasants [1975] that obtains an asymptotic expression for the number of integral solutions to f in an expanding region under the assumption that $h_k(f) \geq 16$.

The second class of cubic hypersurfaces we consider are those for which the dimension is somewhat larger than the h-invariant.

Lemma 2. *Suppose we have a geometrically integral, nonconical cubic hypersurface Y defined over k. If $n \geq h_k(Y) + 4$, then Y_{smooth} satisfies weak approximation.*

This is based on the fibration method (see, for example, [Colliot-Thélène 2003] for a more general description), which reduces the question to proving weak approximation for the fibres of a particular map involving Y. Thanks to the assumptions of the lemma, the fibres in question are quadrics of dimension at least 3. As noted in the introduction, a quadric Q will satisfy weak approximation if $Q_{smooth}(k_v) \neq \varnothing$ for each place v of k. A well known theorem of Hasse [1923] tells us that this holds if the underlying quadratic form has rank at least 5 and $Q_{smooth}(k_v) \neq \varnothing$ for each real place v. We must then find conditions on Y under which we can assume that for a generic fibre Q, this is the case. This is achieved using an elementary argument.

Lemmas 1 and 2 immediately give Theorem A.

3. Proof of Lemma 1

First we introduce some notation. Let k be of degree d over $\mathbb{Q}$, and let $\mathfrak{o}$ be the ring of integers of k with $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_d$. Let $\mathfrak{m}$ be an integral ideal of $\mathfrak{o}$ with $\mathbb{Z}$-basis $\tau_1, \ldots, \tau_d$.

Define $\sigma_1, \ldots, \sigma_{d_1}$ to be the distinct real embeddings of k and $\sigma_{d_1+1}, \ldots, \sigma_{d_1+2d_2}$ the distinct complex embeddings such that σ_{d_1+i} is conjugate to $\sigma_{d_1+d_2+i}$. Put k_i to be the completion of k with respect to the embedding σ_i for $i = 1, \ldots, d_1 + d_2$.

Define V to be the commutative $\mathbb{R}$-algebra $\bigoplus_{i=1}^{d_1+d_2} k_i \cong k \otimes_{\mathbb{Q}} \mathbb{R}$ that has dimension d. For an element $x \in V$, we write $\pi_i(x)$ for its projection onto the i-th summand (so $x = \bigoplus \pi_i(x)$). There is a canonical embedding of k into V given by $\alpha \to \bigoplus \sigma_i(\alpha)$, and we identify k with its image in V. Under this image, $\mathfrak{m}$ forms a lattice in V, and $\tau_1, \ldots, \tau_d$ form a real basis for V.

We define a distance function $|\cdot|_\tau$ on V as follows:

$$|x|_\tau = |x_1\tau_1 + \cdots + x_d\tau_d|_\tau = \max_i |x_i|.$$

This extends to V^n in the obvious way: if $\boldsymbol{x} = (x^{(1)}, \ldots, x^{(n)}) \in V^n$, then

$$|\boldsymbol{x}|_\tau = \max_j |x^{(j)}|_\tau.$$

We note that there will be some constant c, dependent only on k and the choice of basis $\tau_1, \ldots, \tau_d$, such that

$$|\pi_i(x)| \leq c|x|_\tau \tag{3-1}$$

for all $x \in V$ and $1 \leq i \leq d_1 + d_2$ (since each π_i is linear, this is clear).

For any point $\boldsymbol{b} \in V^n$, let $\mathfrak{B}(\boldsymbol{b})$ be the box

$$\mathfrak{B}(\boldsymbol{b}) = \{\, \boldsymbol{x} \in V^n : |\boldsymbol{x} - \boldsymbol{b}|_\tau < \rho/2 \,\}, \tag{3-2}$$

where ρ will always be a real number $0 < \rho < 1$.

For any set $\mathscr{A} \subset V^n$ and positive real number P, we define $P\mathscr{A}$ to be the set $\{\, \boldsymbol{x} \in V^n : P^{-1}\boldsymbol{x} \in \mathscr{A} \,\}$. Given a polynomial $\psi(x_1, \dots, x_n)$ defined over k, we shall be interested in the quantity

$$\mathcal{N}_{\psi,\mathscr{A},\mathfrak{m}}(P) = \#\{\, \boldsymbol{x} \in P\mathscr{A} \cap \mathfrak{m}^n : \psi(\boldsymbol{x}) = 0 \,\}$$

and its asymptotic behaviour as $P \to \infty$.

We can now state the generalisation of the main theorem of [Pleasants 1975] we shall use.

Lemma 3 (Pleasants). *Let $\mathfrak{m}$ be an integral ideal of $\mathfrak{o}$, and let $f(\boldsymbol{x})$ be a cubic polynomial over k with homogeneous cubic part $C(\boldsymbol{x})$ that is not the cube of a linear form. Suppose that $h_k(f) \geq 16$ and that for every integral ideal $\mathfrak{a}$ of $\mathfrak{o}$, the congruence*

$$f(\boldsymbol{x}) \equiv 0 \pmod{\mathfrak{a}} \tag{3-3}$$

has nonsingular solutions in $\mathfrak{m}^n$. Also, let $\boldsymbol{\zeta}_0 = \bigoplus_{i=1}^{d_1+d_2} \boldsymbol{\zeta}_i$, where each $\boldsymbol{\zeta}_i \in \pi_i(V)^n$ is a nonsingular solution to $C(\boldsymbol{x}) = 0$. Then there exists a set $\mathfrak{R} \subset V^n$ containing $\boldsymbol{\zeta}_0$ and a real constant $c_{f,\mathfrak{R},\mathfrak{m}} > 0$ such that

$$\mathcal{N}_{f,\mathfrak{R},\mathfrak{m}}(P) = c_{f,\mathfrak{R},\mathfrak{m}} P^{(n-3)d} + o(P^{(n-3)d}).$$

Proof. In the case where $\mathfrak{m} = \mathfrak{o}$, this is equivalent to Lemmas 6.1, 7.1, 7.2, and 7.4 of [Pleasants 1975], which were proved using the circle method. However, all the arguments go through unchanged to prove the generalisation. Indeed, if one just changes the words 'integral points' to 'elements of $\mathfrak{m}$' and '$\omega_1, \dots, \omega_d$' to '$\tau_1, \dots, \tau_d$' in the relevant places, essentially all the arguments work verbatim in the same way. In terms of the circle method, the commutative algebra V does not behave differently whether $\mathfrak{m}$ is the ring of integers or an arbitrary integral ideal, and the nontrivial algebraic number theory results required [Pleasants 1975, Section 4] were not specific to $\mathfrak{o}$. □

It is straightforward to show that a suitable $\boldsymbol{\zeta}_0$ exists, for example, the argument following [Pleasants 1975, Lemma 7.2]. Thus, Lemma 3 shows that any such cubic polynomial has infinitely many solutions in $\mathfrak{m}^n$.

We now prove Lemma 1. Recall Y is the hypersurface associated to a rational cubic form C with $h_k(C) \geq 16$. As noted in the introduction, since Y is not a cone and C has at least ten variables, the congruences (3-3) have nonsingular solutions in $\mathfrak{o}^n$ for all ideals $\mathfrak{a}$. Then it is clear upon taking $\mathfrak{m} = \mathfrak{o}$ in Lemma 3 that $Y(k) \neq \varnothing$. Furthermore, this implies that $Y_{smooth}(k) \neq \varnothing$ as in the introduction. Suppose

we are given $\varepsilon > 0$, any finite set of places S, and any set of nonsingular points $\{\boldsymbol{x}_v = (x_v^{(1)}, \dots, x_v^{(n)}) \in Y_{smooth}(k_v) : v \in S\}$. To show that weak approximation holds for Y_{smooth}, it suffices to show there exists a point $\boldsymbol{x} = (x^{(1)}, \dots, x^{(n)}) \in Y_{smooth}(k)$ such that $|x^{(i)} - x_v^{(i)}|_v < \varepsilon$ for each i and every $v \in S$ (where $|\cdot|_v$ is the valuation with respect to v). We follow the line of argument of [Skinner 1997, Section 5].

Let $\varepsilon < 1$, S, and $\{\boldsymbol{x}_v\}_{v \in S}$ be given. Write $S = S_\infty \cup S_f$, where S_∞ consists of infinite places and S_f consists of finite places. Without loss of generality, we can assume that S_∞ consists of all the infinite places of k since there are only finitely many of them and $Y_{smooth}(k_v) \supset Y_{smooth}(k) \neq \varnothing$ for all v. We may also assume that $\mathrm{ord}_v(x_v^{(i)}) \geq 0$ for every i and every $v \in S_f$.

We can find $\boldsymbol{a} = (a^{(1)}, \dots, a^{(n)}) \in \mathfrak{o}^n$ such that $|a^{(i)} - x_v^{(i)}|_v < \varepsilon/3$ for all i and $v \in S_f$ (by the Chinese remainder theorem). Let

$$r_v = \min_i \mathrm{ord}_v\{a^{(i)} - x_v^{(i)}\},$$

and let $\mathfrak{p}_v$ be the prime ideal corresponding to v. Put

$$\mathfrak{m} = \prod_{v \in S_f} \mathfrak{p}_v^{r_v}.$$

Consider $f(\boldsymbol{x}) = C(\boldsymbol{x} + \boldsymbol{a})$, a cubic polynomial defined over k. Let t be a positive integer. Choose $D \equiv 1 \pmod{\mathfrak{m}^t}$ to be a positive integer such that

$$D > \frac{2c}{\varepsilon}$$

with c as in (3-1). For each infinite place v, let

$$\boldsymbol{r}_v = D\boldsymbol{x}_v.$$

Put

$$\boldsymbol{\zeta}_0 = \bigoplus_{i=1}^{d_1+d_2} \boldsymbol{r}_{v_i} \in V^n,$$

where v_i is the infinite place corresponding to the embedding σ_i. Note that $\boldsymbol{\zeta}_0$ satisfies the conditions of Lemma 3. Take a set $\mathfrak{R}$ as in Lemma 3 centred at $\boldsymbol{\zeta}_0$. In [Pleasants 1975], the region $\mathfrak{R}$ is essentially a box-like shape, and the only extra condition it needs to have is that it is sufficiently small. Therefore, we can take its 'diameter' with respect to $|\cdot|_\tau$ to be as small as we like, and we can assume it is contained inside a box of side length $\rho < 1$ as in (3-2).

We consider the congruence conditions (3-3). For any finite place $v \notin S_f$, we have $\mathfrak{o}_v = \mathfrak{m}_v$, and so any point in $Y_{smooth}(k_v)$ will give rise to a nonsingular solution in $\mathfrak{m}_v^n$ of $f(\boldsymbol{x}) = 0$. On the other hand, if $v \in S_f$, then $\boldsymbol{x}_v - \boldsymbol{a} \in \mathfrak{m}_v^n$ is a nonsingular

solution to $f(\boldsymbol{x}) = 0$. Thus, the conditions hold for all integral ideals $\mathfrak{a}$ in k by the Chinese remainder theorem.

Finally, we note that the cubic part of f is just C and $h_k(C) \geq 16$. Thus, the conditions for Lemma 3 are met, so for a sufficiently large integer $P \equiv 1 \pmod{\mathfrak{m}^t}$, there exists a point $\boldsymbol{y} \in \mathfrak{m}^n \cap P\mathfrak{R}$ that is a zero of f, and thus, $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{a}$ is a zero of C. Also, since we can have arbitrarily many such points, we can choose one such that $\boldsymbol{z} \neq \boldsymbol{0}$. We now fix our point $\boldsymbol{x}$ to be $\boldsymbol{z}/(DP)$.

For $\nu \in S_\infty$ we have

$$|DPx_\nu^{(i)} - y^{(i)}|_\nu \leq \rho c P < cP,$$

whence

$$\begin{aligned} |x_\nu^{(i)} - x^{(i)}|_\nu &= \left|x_\nu^{(i)} - \frac{z^{(i)}}{DP}\right|_\nu \\ &\leq \left|x_\nu^{(i)} - \frac{y^{(i)}}{DP}\right|_\nu + \frac{|a^{(i)}|_\nu}{DP} \\ &\leq \frac{c}{D} + \frac{|a^{(i)}|_\nu}{DP} < \varepsilon \end{aligned}$$

for P sufficiently large.

For every $\nu \in S_f$ and when $DP \equiv 1 \pmod{\mathfrak{m}^t}$ for sufficiently large t, we have

$$\begin{aligned} |x_\nu^{(i)} - x^{(i)}|_\nu &= \left|x_\nu^{(i)} - \frac{z^{(i)}}{DP}\right|_\nu \\ &\leq |x_\nu^{(i)} - z^{(i)}|_\nu + \frac{|DP-1|_\nu}{|DP|_\nu}|z^{(i)}|_\nu \\ &\leq |x_\nu^{(i)} - z^{(i)}|_\nu + 2^{-t} \\ &= \left|(z^{(i)} - a^{(i)}) - (x_\nu^{(i)} - a^{(i)})\right|_\nu + 2^{-t} \\ &\leq \tfrac{2}{3}\varepsilon + 2^{-t} < \varepsilon. \end{aligned}$$

Finally, we note that by taking ε sufficiently small, we can make $\boldsymbol{x}$ be arbitrarily close to a nonsingular point on $Y(k_\nu)$ for each $\nu \in S$. In this way, we may clearly assume that $\boldsymbol{x} \in Y_{smooth}(k)$. This proves Lemma 1. □

4. Proof of Lemma 2

Throughout this section, we shall suppose that $h = h_k(Y)$ and that $n \geq h + 4$. In fact, for simplification, we shall only consider the case $n = h + 4$, other cases being handled similarly. After a change of variables if necessary, we can express the cubic form C in terms of variables $(\boldsymbol{x}, \boldsymbol{y}) = (x_1 \ldots, x_4, y_1, \ldots, y_h)$ as follows:

$$\begin{aligned} Y : C(\boldsymbol{x}, \boldsymbol{y}) = y_1 Q_1(x_1, \ldots, x_4, y_1, \ldots, y_h) + \cdots \\ + y_h Q_h(x_1, \ldots, x_4, y_1, \ldots, y_h) = 0, \end{aligned}$$

where the Q_i are quadratic forms defined over k. Clearly $Y(k) \neq \varnothing$ since $h < n$, so $Y_{smooth}(k) \neq \varnothing$ as in the introduction.

Consider the three-dimensional linear space L given by $y_1 = \cdots = y_h = 0$. Take the blow-up W of Y along L. Let $z_1, \ldots, z_h$ be coordinates for $\mathbb{A}^h_k$. Then the variety given by the vanishing of C and $y_i z_j - y_j z_i$ for all $i, j \in \{1, \ldots, h\}$ is $L \cup W$. Our plan is to prove weak approximation for W_{smooth}, which, by birationality, will prove it for Y_{smooth}.

Let $\pi : W \to \mathbb{A}^h_k$ be the projection $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \mapsto \boldsymbol{z}$. The generic fibres of this map are quadrics in $\mathbb{P}^4_k$. Abusing our notation slightly, suppose that for $\boldsymbol{y} \in \mathbb{A}^h_k \setminus \{\boldsymbol{0}\}$, the fibre of $W/\mathbb{A}^h_k$ at the point $\boldsymbol{y}$ is given by the quadric

$$X_{\boldsymbol{y}} : Q_{\boldsymbol{y}}(\boldsymbol{x}, t) = 0. \tag{4-1}$$

Then we see that

$$Q_{\boldsymbol{y}}(\boldsymbol{x}, t)t = C(\boldsymbol{x}, \boldsymbol{y}t). \tag{4-2}$$

For an alternative description of the fibres, consider a generic four-dimensional linear space L_4 that contains L. Then this cuts out on Y the union of L and one such quadric Q.

We now quote a simple case of the fibration method, which is given in the paper of Colliot-Thélène, Sansuc, and Swinnerton-Dyer [1987]. To avoid confusion, we say that a *generic fibre* of a fibration Z/X, for varieties X and Z, is one where the image lies in some Zariski dense open subset $X' \subset X$.

Lemma 4. *Let X be a smooth geometrically integral variety such that $X(k) \neq \varnothing$ and X satisfies weak approximation. Let Z/X be a fibration such that the generic fibre is a smooth quadric of dimension at least 3. Then weak approximation holds for any smooth model of Z.*

Proof. This is essentially [Colliot-Thélène et al. 1987, Proposition 3.9] with the caveat that only the generic fibre is smooth. This amounts to trivial changes in the argument that we will not discuss here. □

We may write

$$Y : C(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{h} y_i Q_i(\boldsymbol{x}) + 2\sum_{j=1}^{4} x_j q_j(\boldsymbol{y}) + c(\boldsymbol{y}),$$

where Q_i and q_j are quadratic forms and c is a cubic form. Then by (4-2), $Q_{\boldsymbol{y}}$ takes the form

$$Q_{\boldsymbol{y}}(\boldsymbol{x}, t) = \sum_{i=1}^{h} y_i Q_i(\boldsymbol{x}) + 2\sum_{j=1}^{4} x_j q_j(\boldsymbol{y})t + c(\boldsymbol{y})t^2. \tag{4-3}$$

We rewrite this in terms of a 5×5 matrix $A = A(\boldsymbol{y})$ defined by

$$Q_{\boldsymbol{y}}(\boldsymbol{x}, t) = (\boldsymbol{x}, t)^{\mathrm{T}} A(\boldsymbol{x}, t).$$

Also we consider the 4×4 submatrices M_i given by $Q_i(\boldsymbol{x}) = \boldsymbol{x}^{\mathrm{T}} M_i \boldsymbol{x}$.

By (4-3), A must take the shape

$$A(\boldsymbol{y}) = \left(\begin{array}{ccc|c} & \sum_i y_i M_i & & \begin{matrix} q_1(\boldsymbol{y}) \\ \vdots \\ q_4(\boldsymbol{y}) \end{matrix} \\ \hline q_1(\boldsymbol{y}) & \cdots & q_4(\boldsymbol{y}) & c(\boldsymbol{y}) \end{array}\right). \tag{4-4}$$

Now we can reduce Lemma 2 to the following:

Lemma 5. *Suppose Y is as in Lemma 2. For $\boldsymbol{y} \in \mathbb{A}_k^h$, we define $A(\boldsymbol{y})$ as in (4-4). Either $A(\boldsymbol{y})$ is generically of full rank, or $Y_{sing}(k) \neq \varnothing$.*

If $A(\boldsymbol{y})$ is generically of full rank at least 5, then $Q_{\boldsymbol{y}}$ is generically smooth and of dimension at least 3, so we apply Lemma 4 with $Z = W$ and $X = \mathbb{A}_k^h$ to prove weak approximation for W_{smooth} and hence Y_{smooth}. In the alternative, $Y_{sing}(k) \neq \varnothing$, which is sufficient for weak approximation as noted in the introduction.

We now establish Lemma 5. Note that the equation $\det[A(\boldsymbol{y})] = 0$ defines an algebraic set, $\mathscr{A}$ say, in $\mathbb{A}_k^h$, so if $A(\boldsymbol{y})$ is not generically of full rank, then $\det[A(\boldsymbol{y})] = 0$ identically in $\boldsymbol{y}$.

We examine the leading 4×4 submatrix $M = M(\boldsymbol{y}) = \sum_i y_i M_i$.

Lemma 6. *Let $M_1, \ldots, M_h$ be $m \times m$ symmetric matrices defined over an arbitrary field k with* $\mathrm{char}(k) \neq 2$. *For $(y_1, \ldots, y_h) \in k^h$, put $M(y_1, \ldots, y_h) = \sum_i y_i M_i$. Either there exists a vector $v \in \mathbb{A}_k^m$ such that $v^T M_i v = 0$ for each $1 \leq i \leq h$, or the polynomial* $\det[M(\boldsymbol{y})]$ *is not identically zero in $\boldsymbol{y}$.*

Proof. This is essentially contained in [Colliot-Thélène et al. 1987, Lemma 1.14], which deals with the case $h = 2$, but there are enough changes to warrant giving detail. We proceed by induction. Suppose that $\det[M(\boldsymbol{y})] = 0$ identically. If $h = 1$, then the lemma follows from the fact that $\det(M_1) = 0$ implies that M_1 has a nonzero null space. Now assume that $h \geq 2$ and that the lemma is true for smaller values of h. If $M_1 = \cdots = M_h = 0$, then the lemma is obvious. So we assume that $M_1 \neq 0$. Inserting $\boldsymbol{y} = (1, 0, \ldots, 0)$, we see that $\det(M_1) = 0$. Since $\mathrm{char}(k) \neq 2$, we can choose a basis $v_1, \ldots, v_m$ of $\mathbb{A}_k^m$ such that $M_1 = \mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0)$ with each $a_i \neq 0$ for some $0 < r < m$. Let $M_2', \ldots, M_h'$ be the $(m-r) \times (m-r)$ symmetric matrices corresponding to the basis elements $v_{r+1}, \ldots, v_m$. Then for fixed $y_2, \ldots, y_h$, the coefficient of y_1^r in $\det[M(\boldsymbol{y})]$ is $a_1 \cdots a_r \det[\sum_{i=2}^h y_i M_i']$. Hence, by assumption this must vanish identically. By the induction hypothesis, this implies that there is a nonzero vector $w = (b_{r+1}, \ldots, b_m) \in \mathbb{A}^{m-r}$ such that $w^t M_i' w = 0$ for $2 \leq i \leq h$. Then $v = (0, \ldots, 0, b_{r+1}, \ldots, b_m)$ satisfies $v^T M_i v = 0$ for $1 \leq i \leq h$. □

Now we prove Lemma 5. First suppose that $\det[M(\boldsymbol{y})]$ is identically zero. Then we apply the previous lemma with $m = 4$ to show that there is a nonzero $v \in \mathbb{A}_k^h$ such that $v^T M_i v = 0$ for $1 \le i \le h$, i.e., $Q_i(\boldsymbol{v}) = 0$. We can assume after a change of variables that this vector is $(1, 0, 0, 0)$. Now note that this implies there is no x_1^2 term in any of the Q_i. This implies that all terms in $C(\boldsymbol{x}, \boldsymbol{y})$ are at most linear in x_1. But then $Y_{sing}(k) \neq \varnothing$ since it contains the point $(1, 0, \ldots, 0)$, so we are done.

Next, we suppose that $\det[M(\boldsymbol{y})]$ is not identically zero. In particular, after a change of variables involving only $y_1, \ldots, y_h$, we can assume that it is not zero at $(1, 0 \ldots, 0)$, so $\det(M_1) \neq 0$. Now applying another change of variables involving only $x_1, \ldots, x_4$, we can assume that $M_1 = \operatorname{diag}(a_1, \ldots, a_4)$ with $a_j \in k^\times$.

We write

$$q_j(\boldsymbol{y}) = 2d_j y_1^2 + \cdots \quad \text{for } 1 \le j \le 4$$

and

$$c(\boldsymbol{y}) = e y_1^3 + y_1^2 L(y_2, \ldots, y_h) + \cdots,$$

with L a linear form defined over k.

Assume that $\det[A(\boldsymbol{y})]$ is identically zero. Now

$$\begin{aligned} C(\boldsymbol{x}, y_1, 0 \ldots, 0) &= y_1 \left(\sum_{j=1}^{4} a_j x_j^2 \right) + \sum_{j=1}^{4} 2 d_j x_j y_1^2 + e y_1^3 \\ &= y_1 \sum_{j=1}^{4} a_j \left(\sum_{j=1}^{4} x_j + \frac{d_j}{a_j} y_1 \right)^2 + e' y_1^3 \end{aligned}$$

for some $e' \in k$. The invertible linear change of variables $x_j' = x_j + (d_j/a_j) y_1$ shows that we can assume that each $d_j = 0$. The coefficient of y_1^7 in $\det[A(\boldsymbol{y})]$ is $a_1 \cdots a_4 e$, which must be zero; hence, $e = 0$. The coefficient of y_1^6 in $\det[A(\boldsymbol{y})]$ is $a_1 \cdots a_4 L(y_2, \ldots, y_h)$, which is also identically zero in $y_2, \ldots, y_h$; hence, $L = 0$. Now we see that all terms in C are at most linear in y_1; consequently, the point $(\boldsymbol{x}_0, \boldsymbol{y}_0) = (0, 0, 0, 0; 1, 0, \ldots, 0)$ lies in $Y_{sing}(k)$, completing the proof of the lemma. □

Acknowledgements

I am indebted to Professor Colliot-Thélène and Professor Leep for numerous remarks on an earlier version of this paper. These ultimately led to a substantially improved version of Lemma 2, and hence Theorem A, as well as streamlining the proof of this lemma. I would also like to thank my supervisor Tim Browning for suggesting the original problem and for his excellent supervision over the course of the project. Finally, I am grateful to Dan Loughran for several useful discussions.

References

[Birch and Lewis 1960] B. J. Birch and D. J. Lewis, "$\mathfrak{p}$-adic forms", *J. Indian Math. Soc.* (*N.S.*) **23** (1960), 11–32. MR 23 #A859 Zbl 0096.02503

[Browning 2010] T. D. Browning, "Rational points on cubic hypersurfaces that split off a form", *Compos. Math.* **146**:4 (2010), 853–885. MR 2012g:11178 Zbl 1198.14021

[Colliot-Thélène 2003] J.-L. Colliot-Thélène, "Points rationnels sur les fibrations", pp. 171–221 in *Higher dimensional varieties and rational points* (Budapest, 2001), edited by K. Böröczky, Jr. et al., Bolyai Soc. Math. Stud. **12**, Springer, Berlin, 2003. In French. MR 2005a:14027 Zbl 1077.14029

[Colliot-Thélène and Salberger 1989] J.-L. Colliot-Thélène and P. Salberger, "Arithmetic on some singular cubic hypersurfaces", *Proc. London Math. Soc.* (3) **58**:3 (1989), 519–549. MR 90e:11091 Zbl 0638.14011

[Colliot-Thélène et al. 1987] J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer, "Intersections of two quadrics and Châtelet surfaces. I", *J. Reine Angew. Math.* **373** (1987), 37–107. MR 88m:11045a Zbl 0622.14029

[Coray 1976] D. F. Coray, "Arithmetic on singular cubic surfaces", *Compositio Math.* **33**:1 (1976), 55–67. MR 55 #5636 Zbl 0337.14028

[Coray and Tsfasman 1988] D. F. Coray and M. A. Tsfasman, "Arithmetic on singular Del Pezzo surfaces", *Proc. London Math. Soc.* (3) **57**:1 (1988), 25–87. MR 89f:11083 Zbl 0653.14018

[Davenport and Lewis 1964] H. Davenport and D. J. Lewis, "Non-homogeneous cubic equations", *J. London Math. Soc.* **39** (1964), 657–671. MR 29 #4731 Zbl 0125.02402

[Harari 1994] D. Harari, "Méthode des fibrations et obstruction de Manin", *Duke Math. J.* **75**:1 (1994), 221–260. In French. MR 95j:11056 Zbl 0847.14001

[Harari 1995] D. Harari, "Principe de Hasse et approximation faible sur certaines hypersurfaces", *Ann. Fac. Sci. Toulouse Math.* (6) **4**:4 (1995), 731–762. In French. MR 99c:11080 Zbl 0870.14014

[Hasse 1923] H. Hasse, "Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper.", *J. für Math.* 153 (1923), 113–130. In German. Zbl 49.0114.01

[Kollár 2002] J. Kollár, "Unirationality of cubic hypersurfaces", *J. Inst. Math. Jussieu* **1**:3 (2002), 467–476. MR 2003m:14082 Zbl 1077.14556

[Pleasants 1975] P. A. B. Pleasants, "Cubic polynomials over algebraic number fields", *J. Number Theory* **7**:3 (1975), 310–344. MR 56 #11895 Zbl 0328.12003

[Skinner 1997] C. M. Skinner, "Forms over number fields and weak approximation", *Compositio Math.* **106**:1 (1997), 11–29. MR 98b:14021 Zbl 0892.11014

[Swinnerton-Dyer 1962] H. P. F. Swinnerton-Dyer, "Two special cubic surfaces", *Mathematika* **9** (1962), 54–56. MR 25 #3413 Zbl 0103.38302

Communicated by Jean-Louis Colliot-Thélène
Received 2011-10-25 Revised 2012-07-24 Accepted 2012-09-07

mampsj@bristol.ac.uk *School of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom*

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1365

The Picard crossed module of a braided tensor category

Alexei Davydov and Dmitri Nikshych

For a finite braided tensor category $\mathcal{C}$ we introduce its *Picard crossed module* $\mathfrak{P}(\mathcal{C})$ consisting of the group of invertible $\mathcal{C}$-module categories and the group of braided tensor autoequivalences of $\mathcal{C}$. We describe $\mathfrak{P}(\mathcal{C})$ in terms of braided autoequivalences of the Drinfeld center of $\mathcal{C}$. As an illustration, we compute the Picard crossed module of a braided pointed fusion category.

1. Introduction

Tensor categories can be thought of as categorical analogues of associative algebras. One can adapt standard notions and constructions of the classical theory of associative algebras to tensor categories. Analogues of (bi-)modules over algebras are *(bi-@)module categories* over tensor categories [Quillen 1973; Janelidze and Kelly 2001; Ostrik 2003b].

Given an algebra C the isomorphism classes of invertible C-bimodules form a group $\mathrm{BrPic}(C)$ called the *Brauer–Picard* group of C. There is a well-known homomorphism

$$\phi : \mathrm{BrPic}(\mathcal{C}) \to \mathrm{Aut}(Z(C)), \tag{1}$$

where $Z(C)$ denotes the center of C, constructed as follows. Given an invertible C-bimodule M and $z \in Z(C)$, the element $\phi(M)(z) \in Z(C)$ is defined by the condition that the endomorphism of M given by the left multiplication by $\phi(M)(z)$ equals that given by the right multiplication by z.

There is an analogue of the homomorphism (1) for tensor categories. Given a finite tensor category $\mathcal{C}$ one defines its *Brauer–Picard* group $\mathrm{BrPic}(\mathcal{C})$ of equivalence classes of invertible $\mathcal{C}$-bimodule categories (see [Etingof et al. 2010]) and a homomorphism

$$\Phi : \mathrm{BrPic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C})), \tag{2}$$

Nikshych's work was partially supported by the NSF grant DMS-0800545.
MSC2010: primary 18D10; secondary 16W30.
Keywords: braided tensor category, Drinfeld center, braided autoequivalence, invertible module category.

where $\mathcal{Z}(\mathcal{C})$ is the *Drinfeld center* of $\mathcal{C}$ and $\mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ is the group of braided autoequivalences of $\mathcal{Z}(\mathcal{C})$.

It was shown in [Etingof et al. 2010] that (2) is an isomorphism when $\mathcal{C}$ is a fusion category.

Braided tensor categories are analogues of commutative algebras. Similarly to the classical case, module categories over a braided tensor category $\mathcal{C}$ can be regarded as bimodule categories. In this case the group $\mathrm{BrPic}(\mathcal{C})$ contains a subgroup $\mathrm{Pic}(\mathcal{C})$, called the *Picard group* of $\mathcal{C}$, consisting of invertible $\mathcal{C}$-module categories [Etingof et al. 2010]. One defines a homomorphism

$$\partial : \mathrm{Pic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}) \tag{3}$$

in a way parallel to (2). The classical analogue of (3) for commutative algebras is trivial, but in general ∂ is far from being trivial. It was shown in [Etingof et al. 2010] that it is an isomorphism for every nondegenerate braided fusion category $\mathcal{C}$.

Groups $\mathrm{Pic}(\mathcal{C})$ and $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ play important roles in the theory of braided tensor categories. In particular, they are used in the classification of group extensions of fusion categories [Etingof et al. 2010]. They also appear as parts of an important invariant of $\mathcal{C}$ called the *core*, studied in [Drinfeld et al. 2010]. We thus hope that our description of the algebraic structure formed by these groups will shed more light on these constructions.

The starting point of this paper is a conjecture of V. Drinfeld that for a braided tensor category $\mathcal{C}$ the pair $\mathfrak{P}(\mathcal{C}) = (\mathrm{Pic}(\mathcal{C}), \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}))$ along with the homomorphism (3) and the natural action of $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ on $\mathrm{Pic}(\mathcal{C})$ is a *crossed module*, called the *Picard crossed module* of $\mathcal{C}$. See Section 3D for the definition of a crossed module and [Joyal and Street 1993; Drinfeld et al. 2010, Appendix E.5.3] for an interpretation of crossed modules in terms of monoidal categories. We prove this conjecture in Theorem 3.10.

For a finite tensor category $\mathcal{C}$ we define its Brauer–Picard group $\mathrm{BrPic}(\mathcal{C})$ as the group of equivalence classes of invertible *exact* $\mathcal{C}$-bimodule categories. We prove in Theorem 4.1 that the canonical homomorphism (2) is an isomorphism. This extends the corresponding result for fusion categories proved in [Etingof et al. 2010].

Next, for a braided finite tensor category $\mathcal{C}$ we show in Theorem 4.3 that the image of $\mathrm{Pic}(\mathcal{C}) \subset \mathrm{BrPic}(\mathcal{C})$ under the isomorphism (2) is the subgroup of braided autoequivalences of $\mathcal{Z}(\mathcal{C})$ trivializable on $\mathcal{C}$.

Finally, we explicitly compute the Picard crossed module of a pointed braided fusion category in Section 5. It turns out that the Picard groups of pointed braided fusion categories interpolate between the orthogonal groups of quadratic forms and the exterior squares of finite abelian groups.

The paper is organized as follows.

Section 2 contains basic facts about finite tensor categories and module categories over them. Here we also define the Brauer–Picard group of a finite tensor category and the Picard group of a finite braided tensor category. (They were previously defined in [Etingof et al. 2010] in the setting of fusion categories.)

In Section 3 we introduce the Picard crossed module of a braided tensor category.

In Section 4 we prove our Main Theorems 4.1 and 4.3 and describe the Picard crossed module of a braided tensor category in terms of braided autoequivalences of its center.

Section 5 is devoted to the computation of the Picard crossed module of a pointed braided fusion category and its invariants.

2. Preliminaries

2A. ***General conventions.*** We work over an algebraically closed field k. Recall that a k-linear abelian category $\mathcal{C}$ is *finite* if

(i) $\mathcal{C}$ has finite dimensional spaces of morphisms;

(ii) every object of $\mathcal{C}$ has finite length;

(iii) $\mathcal{C}$ has *enough projectives*, that is, every simple object of $\mathcal{C}$ has a projective cover; and

(iv) there are finitely many isomorphism classes of simple objects in $\mathcal{C}$.

All abelian categories considered in this paper will be finite. Any such category is equivalent to the category $\mathrm{Rep}(A)$ of finite dimensional representations of a finite dimensional k-algebra A. All functors between such categories will be additive and k-linear. We use the symbol $\simeq$ for equivalence between categories and the symbol $\cong$ for isomorphisms between objects.

In this paper we freely use basic results of the theory of finite tensor categories and module categories over them [Bakalov and Kirillov 2001; Etingof and Ostrik 2004; Ostrik 2003b] and the theory of braided categories [Joyal and Street 1993; Drinfeld et al. 2010].

2B. ***Tensor categories.*** By a *tensor category* we mean a finite rigid tensor category $\mathcal{A}$ whose unit object $\mathbf{1}$ is simple [Etingof and Ostrik 2004]. A semisimple tensor category is called a *fusion* category.

Let $\mathcal{A}$ be a tensor category with the associativity constraint

$$a_{X,Y,Z} : (X \otimes Y) \otimes Z \xrightarrow{\sim} X \otimes (Y \otimes Z).$$

The tensor category with the opposite tensor product $X \otimes^{\mathrm{op}} Y := Y \otimes X$ and the

accordingly adjusted associativity constraint a^{op}

$$\begin{array}{ccc} (X \otimes^{\mathrm{op}} Y) \otimes^{\mathrm{op}} Z & \xrightarrow{a^{\mathrm{op}}_{X,Y,Z}} & X \otimes^{\mathrm{op}} (Y \otimes^{\mathrm{op}} Z) \\ \| & & \| \\ Z \otimes (Y \otimes X) & \xrightarrow{a^{-1}_{Z,Y,X}} & (Z \otimes Y) \otimes X \end{array}$$

will be called the category *opposite* to $\mathscr{A}$ and will be denoted $\mathscr{A}^{\mathrm{op}}$.

Let $\mathscr{A}$ and $\mathscr{B}$ be tensor categories. Their *Deligne* tensor product [Deligne 2002] will be denoted by $\mathscr{A} \boxtimes \mathscr{B}$.

Definition 2.1. Let $\mathscr{A}$ be a tensor category and let $\mathscr{B} \subset \mathscr{A}$ be a tensor subcategory. A tensor autoequivalence α of $\mathscr{A}$ is called *trivializable* on $\mathscr{B}$ if the restriction $\alpha|_{\mathscr{B}}$ is isomorphic to $\mathrm{id}_{\mathscr{B}}$ as a tensor functor.

We will denote by $\mathrm{Aut}(\mathscr{A})$ (respectively, $\mathrm{Aut}(\mathscr{A}, \mathscr{B})$) the group of isomorphism classes of tensor autoequivalences of $\mathscr{A}$ (respectively, tensor autoequivalences of $\mathscr{A}$ trivializable on $\mathscr{B}$).

2C. ***Braided tensor categories.*** Recall that a *braided* tensor category $\mathscr{C}$ is a finite tensor category equipped with a natural isomorphism

$$c_{X,Y} : X \otimes Y \xrightarrow{\simeq} Y \otimes X$$

satisfying the hexagon axioms [Joyal and Street 1993]. The braiding of $\mathscr{C}$ gives rise to a tensor equivalence between $\mathscr{C}$ and $\mathscr{C}^{\mathrm{op}}$.

An important example of a braided tensor category is the *center* $\mathcal{Z}(\mathscr{A})$ of a finite tensor category $\mathscr{A}$. It is defined as the category whose objects are pairs (Z, γ), where X is an object of $\mathscr{A}$ and γ is a natural family of isomorphisms

$$\gamma_X : X \otimes Z \xrightarrow{\simeq} Z \otimes X, \quad X \in \mathscr{A},$$

called *half-braidings*, satisfying compatibility conditions. The center is a finite braided tensor category with the braiding given by

$$\delta_Z : (Z, \gamma) \otimes (Y, \delta) \xrightarrow{\simeq} (Y, \delta) \otimes (Z, \gamma).$$

Let $\mathscr{C}^{\mathrm{rev}}$ denote the tensor category $\mathscr{C}$ equipped with the reversed braiding

$$\tilde{c}_{X,Y} = c^{-1}_{Y,X}.$$

For a braided tensor category $\mathscr{C}$ there are canonical embeddings $\mathscr{C} \hookrightarrow \mathcal{Z}(\mathscr{C})$ and $\mathscr{C}^{\mathrm{rev}} \hookrightarrow \mathcal{Z}(\mathscr{C})$ given by

$$X \mapsto (X, c_{-,X}) \quad \text{and} \quad X \mapsto (X, \tilde{c}_{-,X}). \tag{4}$$

For a braided tensor category $\mathcal{C}$ the embeddings (4) combine into a single braided tensor functor

$$\mathcal{C} \boxtimes \mathcal{C}^{\mathrm{rev}} \to \mathcal{Z}(\mathcal{C}). \tag{5}$$

A braided tensor category $\mathcal{C}$ is called *factorizable* if the functor (5) is an equivalence.

We will denote by $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ the group of isomorphism classes of braided tensor autoequivalences of a braided tensor category $\mathcal{C}$.

Recall that a tensor category is called *pointed* if its every simple object is invertible.

Example 2.2. Let $\mathcal{C}$ be a pointed braided fusion category. Then isomorphism classes of simple objects of $\mathcal{C}$ form a finite abelian group A.

The associativity constraint of $\mathcal{C}$ determines a 3-cocycle $\omega : A \times A \times A \to k^\times$. The braiding determines a function

$$c : A \times A \to k^\times \tag{6}$$

satisfying the following identities coming from the hexagon axioms of the braided tensor category:

$$c(x, y+z)c(x, y)^{-1}c(x, z)^{-1} = \omega(x, y, z)\omega(y, x, z)^{-1}\omega(y, z, x), \tag{7}$$

$$c(x+y, z)c(x, z)^{-1}c(y, z)^{-1} = \omega(x, y, z)^{-1}\omega(x, z, y)\omega(z, x, y)^{-1}, \tag{8}$$

for all $x, y, z \in A$. Following [Eilenberg and Mac Lane 1953; 1954], we denote by $Z^3_{ab}(A, k^\times)$ the set of pairs (ω, c), where ω is a 3-cocycle on A and c is a function satisfying (7) and (8). Note that $Z^3_{ab}(A, k^\times)$ is a group with respect to pointwise multiplication.

Thus, every pointed braided fusion category determines an element of $Z^3_{ab}(A, k^\times)$. Conversely, given $(\omega, c) \in Z^3_{ab}(A, k^\times)$ one defines a braided category structure on the fusion category Vec_A of finite dimensional A-graded vector spaces using ω for the associativity constraint and c for braiding.

Let $\mathcal{C}$ and $\mathcal{C}'$ be pointed braided fusion categories corresponding to $(\omega, c) \in Z^3_{ab}(A, k^\times)$ and $(\omega', c') \in Z^3_{ab}(A', k^\times)$, respectively. A tensor functor $F : \mathcal{C} \to \mathcal{C}'$ gives rise to a group homomorphism $f : A \to A'$. The tensor structure of F gives rise to a map $\phi : A \times A \to k^\times$. The coherence axiom for the tensor structure becomes the 2-coboundary condition

$$\phi(y, z)\phi(x+y, z)^{-1}\phi(x, y+z)^{-1}\phi(x, y)^{-1} = \omega(x, y, z)\omega'(f(x), f(y), f(z))^{-1}, \tag{9}$$

for all $x, y, z \in A$. Here ω, ω' are the associativity constraints in $\mathcal{C}, \mathcal{C}'$ respectively. The tensor functor F is braided if

$$c(x, y)c'(f(x), f(y))^{-1} = \phi(x, y)\phi(y, x)^{-1}. \tag{10}$$

Tensor autoequivalences isomorphic to the identity functor (identity f) define an equivalence relation on the group of pairs (ω, c), where (ω, c) and (ω', c') are related as in (9) and (10) with trivial f. The quotient group is known as the *third abelian cohomology* $H^3_{ab}(A, k^\times)$ [Eilenberg and Mac Lane 1954]. Elements of the latter group parametrize equivalence classes of pointed braided fusion categories.

The function

$$q(x) := c(x, x), \quad x \in A$$

is a *quadratic form* on A, that is, $q(-x) = q(x)$ and the symmetric function

$$\sigma(x, y) = \frac{q(x+y)}{q(a)q(b)}, \quad x, y \in A \tag{11}$$

is bimultiplicative. We have the identity

$$\sigma(x, y) = c(x, y)c(y, x), \quad x, y \in A. \tag{12}$$

Mac Lane proved that the map $(\omega, c) \mapsto q$ defines an isomorphism between $H^3_{ab}(A, k^*)$ and the group of quadratic forms $A \to k^\times$.

By associating to $\mathcal{C}$ the pair (A, q) one gets a functor from the 1-categorical contraction of the 2-category of pointed braided fusion categories to the category of *premetric groups*. Each objects of the latter category is a finite abelian group equipped with a quadratic form, and the morphisms are group homomorphisms preserving the quadratic forms (that is, orthogonal homomorphisms).

It was proved by Joyal and Street [1993] that the above functor is an equivalence (see also [Drinfeld et al. 2010, Appendix D]). The braided fusion category associated to (A, q) will be denoted $\mathcal{C}(A, q)$.

It follows from the above that

$$\mathrm{Aut}^{\mathrm{br}}(\mathcal{C}(A, q)) = O(A, q),$$

where $O(A, q)$ denotes the group of orthogonal automorphisms of (A, q), that is, automorphisms $\alpha : A \to A$ such that $q \circ \alpha = q$.

2D. *Centralizers in braided tensor categories.*

Definition 2.3 (M. Müger [2003]). Two objects X and Y of a braided tensor category $\mathcal{C}$ are said to *centralize* each other if

$$c_{Y,X}c_{X,Y} = \mathrm{id}_{X\otimes Y}.$$

The *centralizer* $\mathcal{D}'$ of a tensor subcategory $\mathcal{D} \subset \mathcal{C}$ is defined to be the full subcategory of objects of $\mathcal{C}$ that centralize each object of $\mathcal{D}$. It is easy to see that $\mathcal{D}'$ is a tensor subcategory.

We will denote the self-centralizer $\mathcal{C}'$ of $\mathcal{C}$ by $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ and call it the *symmetric* center of $\mathcal{C}$. We say that $\mathcal{C}$ is *nondegenerate* if and only if $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ is trivial, that is, consists of extensions of the unit object $\mathbf{1}$.

Remark 2.4. It was shown in [Drinfeld et al. 2010, Proposition 3.7] that a braided fusion category $\mathcal{C}$ is nondegenerate if and only if it is factorizable.

Let $\mathcal{C}$ be a braided tensor category. Let us identify $\mathcal{C}$ and $\mathcal{C}^{\mathrm{rev}}$ with their images in $\mathcal{Z}(\mathcal{C})$ under the embeddings (4). Then $\mathcal{C}$ and $\mathcal{C}^{\mathrm{rev}}$ are centralizers of each other.

Example 2.5. Let us describe the centralizers in the pointed braided fusion category $\mathcal{C}(A, q)$, see Example 2.2. Two simple objects $x, y \in A$ of this category centralize each other if and only if $\sigma(x, y) = 1$, where σ is the bimultiplicative symmetric function (11) corresponding to q. That is, in this case the centralizing property coincides with orthogonality.

Every fusion subcategory of $\mathcal{C}(A, q)$ corresponds to a subgroup $B \subset A$ and is equivalent to $\mathcal{C}(B, q|_B)$. We have $\mathcal{C}(B, q|_B)' = \mathcal{C}(B^\perp, q|B^\perp)$, where $B^\perp$ is the subgroup of A orthogonal to B. In particular,

$$\mathcal{Z}_{\mathrm{sym}}(\mathcal{C}(A, q)) = \mathcal{C}(A^\perp, q|_{A^\perp}),$$

where $A^\perp = \{a \in A \mid \sigma(a, b) = 1 \text{ for all } b \in A\}$ is the kernel of σ. The category $\mathcal{C}(A, q)$ is nondegenerate if and only if σ is nondegenerate.

2E. ***Module categories over tensor categories.*** Let $\mathcal{A}$ be a finite tensor category. A left $\mathcal{A}$*-module* category (see [Quillen 1973; Janelidze and Kelly 2001; Ostrik 2003b]) is a finite category $\mathcal{M}$ together with a bifunctor

$$\mathcal{A} \times \mathcal{M} \to \mathcal{M}, \quad (X, M) \mapsto X * M$$

equipped with a functorial isomorphism

$$a_{X,Y,M} : X * (Y * M) \xrightarrow{\simeq} (X \otimes Y) * M, \quad X, Y \in \mathcal{A}, M \in \mathcal{M},$$

called the *associativity constraint*, plus a unit constraint, the whole satisfying natural compatibility axioms.

Equivalently, $\mathcal{M}$ is a left module category over $\mathcal{A}$ if there is given a tensor functor $\mathcal{A} \to \mathrm{End}(\mathcal{M})$ to the tensor category $\mathrm{End}(\mathcal{M})$ of endofunctors of $\mathcal{M}$ (with tensor structure given by composition of functors).

A right $\mathcal{A}$-module category is defined in a similar way. It corresponds to a tensor functor $\mathcal{A}^{\mathrm{op}} \to \mathrm{End}(\mathcal{M})$. For a right $\mathcal{A}$-module category $\mathcal{M}$ the category obtained from $\mathcal{M}$ reversing the directions of morphisms is a left $\mathcal{A}$-module category via

$$X \odot M = M * X^*, \quad M \in \mathcal{M}, X \in \mathcal{A}.$$

We will denote this category $\mathcal{M}^{\mathrm{op}}$ and call it the *opposite* module category.

Functors between $\mathcal{A}$-module categories and natural transformations between them are defined in an obvious way, see [Ostrik 2003b].

Let $\mathcal{A}$ be a tensor category. Following [Etingof and Ostrik 2004] we say that an $\mathcal{A}$-module category $\mathcal{M}$ is *exact* if for any projective object P of $\mathcal{A}$ and every object M of $\mathcal{M}$ the object $P \otimes M$ is projective. An $\mathcal{A}$-module category $\mathcal{M}$ is exact if and only if for every $\mathcal{C}$-module category $\mathcal{N}$ any $\mathcal{C}$-module functor $\mathcal{M} \to \mathcal{N}$ is exact.

Example 2.6. If $\mathcal{A}$ is a fusion category then an $\mathcal{A}$-module category is exact if and only if it is semisimple.

Note 2.7. All module categories in this paper are assumed to be exact.

Given an indecomposable left $\mathcal{A}$-module category $\mathcal{M}$ the *dual* category of $\mathcal{A}$ with respect to $\mathcal{M}$ is the category $\mathcal{A}^*_{\mathcal{M}} = \mathrm{Fun}_{\mathcal{A}}(\mathcal{M}, \mathcal{M})$ of $\mathcal{A}$-module endofunctors of $\mathcal{M}$. It was shown in [Etingof and Ostrik 2004, Section 3.3] that $\mathcal{A}^*_{\mathcal{M}}$ is a finite tensor category. Furthermore, $\mathcal{M}$ is an exact indecomposable left $\mathcal{A}^*_{\mathcal{M}}$-module category and there is a canonical tensor equivalence $\mathcal{A} \cong (\mathcal{A}^*_{\mathcal{M}})^*_{\mathcal{M}}$.

Remark 2.8. It was proved in [Etingof and Ostrik 2004, Theorem 3.31] that the assignment

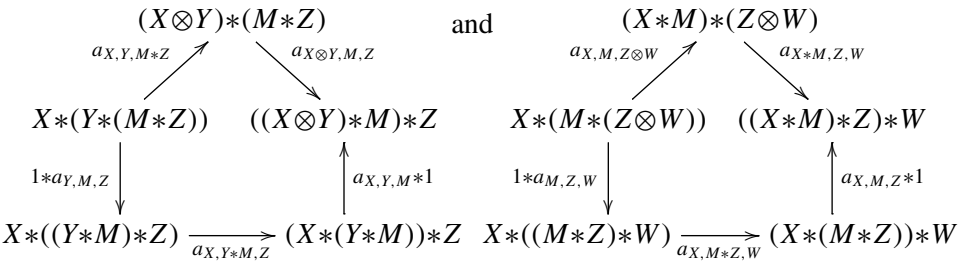
$$\mathcal{N} \mapsto \mathrm{Fun}_{\mathcal{A}}(\mathcal{M}, \mathcal{N})$$

is an equivalence between the 2-category of exact left $\mathcal{A}$-module categories and that of exact right $\mathcal{A}^*_{\mathcal{M}}$-module categories.

2F. *Bimodule categories.* Let $\mathcal{A}$, $\mathcal{B}$ be tensor categories.

By definition, an $(\mathcal{A}-\mathcal{B})$-*bimodule* category $\mathcal{M}$ is an $(\mathcal{A}\boxtimes\mathcal{B}^{\mathrm{op}})$-module category.

Equivalently, a category $\mathcal{M}$ is an $(\mathcal{A}-\mathcal{B})$-bimodule category if it has left $\mathcal{A}$-module and right $\mathcal{B}$-module category structures compatible by a collection of isomorphisms $a_{X,M,Y} : X*(M*Y) \to (X*M)*Y$ called *middle associativity constraints* natural in $X \in \mathcal{A}$, $Y \in \mathcal{B}$, $M \in \mathcal{M}$, and such that the diagrams



commute for all $X, Y \in \mathcal{A}$, $Z, W \in \mathcal{B}$, and $M \in \mathcal{M}$.

Example 2.9. A left $\mathcal{A}$-module category $\mathcal{M}$ has a structure of an $(\mathcal{A} - (\mathcal{A}^*_{\mathcal{M}})^{\mathrm{op}})$-bimodule category.

2G. ***Tensor product of module categories and the Brauer–Picard group of a tensor category.*** Let $\mathcal{A}$ be a finite tensor category, let $\mathcal{M}$ be a right $\mathcal{A}$-module category, and let $\mathcal{N}$ be a left $\mathcal{A}$-module category. The $\mathcal{A}$-module tensor product of $\mathcal{M}$ and $\mathcal{N}$ was defined in [Etingof et al. 2010, Section 3.1]. Let us recall this definition. A bifunctor $F : \mathcal{M} \times \mathcal{N} \to \mathcal{H}$, where $\mathcal{H}$ is an abelian category, is called *$\mathcal{A}$-balanced* if there exists a family of isomorphisms $F(M \otimes X, N) \xrightarrow{\sim} F(M, X \otimes N)$ natural in $M \in \mathcal{M}$, $N \in \mathcal{N}$, and $X \in \mathcal{A}$ satisfying coherence axioms. Let $\mathrm{Fun}_{bal,re}(\mathcal{M} \times \mathcal{N}, \mathcal{H})$ denote the category of $\mathcal{A}$-balanced functors from $\mathcal{M} \times \mathcal{N}$ to $\mathcal{H}$ right exact in each variable.

The $\mathcal{A}$-module tensor product of $\mathcal{M}$ and $\mathcal{N}$ is an abelian category $\mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N}$ together with the $\mathcal{C}$-balanced bifunctor

$$B_{\mathcal{M},\mathcal{N}} : \mathcal{M} \times \mathcal{N} \to \mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N}$$

which is right exact in each variable and for every abelian category $\mathcal{H}$ induces an equivalence

$$\mathrm{Fun}_{bal,re}(\mathcal{M} \times \mathcal{N}, \mathcal{A}) \simeq \mathrm{Fun}_{re}(\mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N}, \mathcal{H}).$$

Here and below, the subscript *re* indicates that functors under consideration are right exact. The existence of the $\mathcal{A}$-module tensor product was established in [Etingof et al. 2010, Section 3.2]. Namely, it was shown that

$$\mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N} \simeq \mathrm{Fun}_{\mathcal{A},re}(\mathcal{M}^{\mathrm{op}}, \mathcal{N}). \tag{13}$$

Note that although the categories considered in [Etingof et al. 2010] were assumed to be semisimple the proof of this particular result does not use semisimplicity. Indeed, first observe that $\mathcal{M} \boxtimes \mathcal{N}$ is equivalent to $\mathrm{Fun}_{re}(\mathcal{M}^{\mathrm{op}}, \mathcal{N})$, since for $\mathcal{M} = \mathrm{Rep}(A)$ and $\mathcal{N} = \mathrm{Rep}(B)$, where A and B are algebras, both categories are identified with $\mathrm{Rep}(A \otimes B)$. Next, by [Etingof et al. 2010, Proposition 3.5] every balanced bifunctor $\mathcal{M} \times \mathcal{N} \to \mathcal{H}$ that is right exact in every variable canonically factors through the functor

$$\mathcal{M} \boxtimes \mathcal{N} \simeq \mathrm{Fun}_{re}(\mathcal{M}^{\mathrm{op}}, \mathcal{N}) \xrightarrow{B_{\mathcal{M},\mathcal{N}}} \mathrm{Fun}_{\mathcal{A},re}(\mathcal{M}^{\mathrm{op}}, \mathcal{N}),$$

where $B_{\mathcal{M},\mathcal{N}}$ is the left adjoint to the forgetful functor

$$\mathrm{Fun}_{\mathcal{A},re}(\mathcal{M}^{\mathrm{op}}, \mathcal{N}) \to \mathrm{Fun}_{re}(\mathcal{M}^{\mathrm{op}}, \mathcal{N}).$$

Furthermore, if $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{A}$-bimodule categories then so is $\mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N}$ (the $\mathcal{A}$-bimodule structure on $\mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N}$ is induced by the $\mathcal{A}$-bimodule structure on $\mathcal{M} \boxtimes \mathcal{N}$).

Proposition 2.10. *Let $\mathcal{M}$ and $\mathcal{N}$ be exact $\mathcal{A}$-bimodule categories. Then $\mathcal{M} \boxtimes_{\mathcal{A}} \mathcal{N}$ is an exact $\mathcal{A}$-bimodule category.*

Proof. It is enough to check that for all objects F in $\mathcal{M}\boxtimes_{\mathcal{A}}\mathcal{N}$ and projective objects P_1, P_2 in $\mathcal{C}$ the object $P_1\otimes F\otimes P_2$ is projective. That is, we need to show that the compositions of an $\mathcal{A}$-module functor $F:\mathcal{M}^{\mathrm{op}}\to\mathcal{N}$ with the functors

$$\mathcal{M}^{\mathrm{op}}\to\mathcal{M}^{\mathrm{op}}: M\mapsto M\otimes P_1,$$
$$\mathcal{N}\to\mathcal{N}: N\mapsto N\otimes P_2$$

are projective objects in $\mathrm{Fun}_{\mathcal{A}}(\mathcal{M}^{\mathrm{op}},\mathcal{N})$. This is clear since the latter category is exact over $\mathcal{A}^*_{\mathcal{M}}$ and $\mathcal{A}^*_{\mathcal{N}}$ and the right multiplications by P_1, P_2 are $\mathcal{A}$-module endofunctors. □

We say that an exact $\mathcal{A}$-bimodule category $\mathcal{M}$ is *invertible* if there exists an exact $\mathcal{A}$-bimodule category $\mathcal{N}$ such that

$$\mathcal{M}\boxtimes_{\mathcal{A}}\mathcal{N}\simeq\mathcal{N}\boxtimes_{\mathcal{A}}\mathcal{M}\simeq\mathcal{A},$$

where $\mathcal{A}$ is viewed as an $\mathcal{A}$-bimodule category via the regular left and right actions of $\mathcal{A}$.

Remark 2.11. It was proved in [Etingof et al. 2010, Propositon 4.2] that an $\mathcal{A}$-bimodule category $\mathcal{M}$ is invertible if and only if the tensor functor

$$L:\mathcal{A}\to(\mathcal{A}^*_{\mathcal{M}})^{\mathrm{op}}: X\mapsto ?\otimes X \tag{14}$$

is an equivalence.

The group of equivalence classes of invertible $\mathcal{A}$-bimodule categories is called the *Brauer–Picard* group of $\mathcal{A}$ and is denoted by $\mathrm{BrPic}(\mathcal{A})$.

2H. ***Module categories over braided tensor categories.*** Let now $\mathcal{C}$ be a braided tensor category with the braiding

$$c_{X,Y}: X\otimes Y\xrightarrow{\simeq} Y\otimes X,\quad X,Y\in\mathcal{C}.$$

The braiding of $\mathcal{C}$ gives a tensor structure on the multiplication functor $\mathcal{C}\boxtimes\mathcal{C}\to\mathcal{C}$ [Joyal and Street 1993]. Hence, there is a canonical tensor functor

$$\otimes:\mathcal{C}\boxtimes\mathcal{C}^{\mathrm{op}}\simeq\mathcal{C}\boxtimes\mathcal{C}\to\mathcal{C}. \tag{15}$$

This allows us to turn any left $\mathcal{C}$-module category $\mathcal{M}$ into a $\mathcal{C}$-bimodule category as follows. The right action is $M*X:=X*M$ for all $X\in\mathcal{C}$ and $M\in\mathcal{M}$. Let $a_{X,Y,M}:X\otimes(Y\otimes M)\xrightarrow{\simeq}(X\otimes Y)\otimes M$ denote the left $\mathcal{C}$-module associativity constraint of $\mathcal{M}$. The right $\mathcal{C}$-module associativity constraint of $\mathcal{M}$ is given by

$$\begin{array}{ccccc}(M*X)*Y & & \xrightarrow{\quad a_{M,X,Y}\quad} & & M*(X\otimes Y)\\ \| & & & & \| \\ Y*(X*M) & \xrightarrow{a_{Y,X,M}} & (Y\otimes X)*M & \xrightarrow{c_{Y,X}} & (X\otimes Y)*M\end{array} \tag{16}$$

and the middle associativity constraint is given by

$$\begin{array}{ccccccc} X*(M*Y) & & \xrightarrow{\quad a_{X,Y,M} \quad} & & & & (X*M)*Y \\ \| & & & & & & \| \\ X*(Y*M) & \xrightarrow{a_{X,Y,M}} & (X\otimes Y)*M & \xrightarrow{c_{X,Y}} & (Y\otimes X)*M & \xrightarrow{a^{-1}_{Y,X,M}} & Y*(X*M) \end{array} \tag{17}$$

for all $X, Y \in \mathscr{C}$ and $M \in \mathscr{M}$.

Let **Mod**($\mathscr{C}$) and **Bimod**($\mathscr{C}$) denote the 2-categories of exact module and bimodule categories over $\mathscr{C}$, respectively. The above tensor functor (15) yields a 2-functor

$$\mathscr{B} : \mathbf{Mod}(\mathscr{C}) \to \mathbf{Bimod}(\mathscr{C}). \tag{18}$$

Clearly, the 2-functor $\mathscr{B}$ is an embedding of 2-categories.

Definition 2.12. We will call a $\mathscr{C}$-bimodule category *one-sided* if it is equivalent to $\mathscr{B}(\mathscr{M})$ for some left $\mathscr{C}$-module category $\mathscr{M}$.

Remark 2.13. One can give an explicit characterization of one-sided categories. Namely, a $\mathscr{C}$-bimodule category $\mathscr{M}$ is one-sided if it is equipped with a collection of isomorphisms

$$d_{M,X} : M*X \to X*M, \tag{19}$$

natural in $X \in \mathscr{C}$ and $M \in \mathscr{M}$, such that the diagrams

$$\begin{array}{ccccc} & & M*(X\otimes Y) & \xrightarrow{d_{M,X\otimes Y}} & (X\otimes Y)*M & & \\ & \swarrow^{a_{M,X,Y}} & & & & \nwarrow^{a_{X,Y,M}} & \\ (M*X)*Y & & & & & & X*(Y*M) \\ & \searrow_{d_{M,X}1} & & & & \nearrow_{1d_{M,Y}} & \\ & & (X*M)*Y & \xrightarrow{a^{-1}_{X,M,Y}} & X*(M*Y) & & \end{array} \tag{20}$$

and

$$\begin{array}{ccccc} & & (X*M)*Y & \xrightarrow{d_{X*M,Y}} & Y*(X*M) & & \\ & \nearrow^{a_{X,M,Y}} & & & & \searrow^{a_{Y,X,M}} & \\ X*(M*Y) & & & & & & X*(M*Y), \\ & \searrow_{1*d_{M,Y}} & & & & \nearrow_{c_{X,Y}*1} & \\ & & X*(Y*M) & \xrightarrow{a_{X,Y,M}} & (X\otimes Y)*M & & \end{array} \tag{21}$$

commute, where a denotes the associativity constraint of $\mathscr{M}$.

Given left $\mathcal{C}$-module categories $\mathcal{M}$ and $\mathcal{N}$, there is an obvious $\mathcal{C}$-bimodule equivalence

$$\mathcal{B}\big(\mathcal{B}(\mathcal{M})\boxtimes_{\mathcal{C}}\mathcal{N}\big)\simeq\mathcal{B}(\mathcal{M})\boxtimes_{\mathcal{C}}\mathcal{B}(\mathcal{N}).$$

Hence, when $\mathcal{C}$ is braided, the group $\mathrm{BrPic}(\mathcal{C})$ contains a subgroup $\mathrm{Pic}(\mathcal{C})$ consisting of equivalence classes of one-sided invertible $\mathcal{C}$-bimodule categories. Following [Etingof et al. 2010], we call this group the *Picard group* of $\mathcal{C}$.

In what follows we will omit the 2-functor $\mathcal{B}$ from notation and identify invertible $\mathcal{C}$-module categories with their images in $\mathbf{Bimod}(\mathcal{C})$.

2I. ***The α-induction.*** Let $\mathcal{C}$ be a braided tensor category and let $\mathcal{M}$ be a $\mathcal{C}$-module category. There is a pair of tensor functors

$$\alpha^{\pm}_{\mathcal{M}}:\mathcal{C}\to\mathcal{C}^{*}_{\mathcal{M}} \tag{22}$$

defined as follows (see [Böckenhauer et al. 2001; Ostrik 2003b]). For each $X\in\mathcal{C}$ the endofunctors $\alpha^{\pm}_{\mathcal{M}}(X):\mathcal{M}\to\mathcal{M}$ coincide with left multiplication by X, that is,

$$\alpha^{\pm}_{\mathcal{M}}(X)=X\otimes-.$$

Their $\mathcal{C}$-module functor structures are given by

$$\alpha^{+}_{\mathcal{M}}(X)(Y\otimes M)=X\otimes Y\otimes M\xrightarrow{c_{X,Y}}Y\otimes X\otimes M=Y\otimes\alpha^{+}_{\mathcal{M}}(X)(M),$$

$$\alpha^{-}_{\mathcal{M}}(X)(M\otimes Y)=X\otimes Y\otimes M\xrightarrow{c^{-1}_{Y,X}}Y\otimes X\otimes M=Y\otimes\alpha^{-}_{\mathcal{M}}(X)(M),$$

for all $X,Y\in\mathcal{C}$ and $M\in\mathcal{M}$. Here we suppress the associativity constraints.

When $\mathcal{M}$ is invertible the functors $\alpha^{\pm}_{\mathcal{M}}$ are equivalences and the functor $\partial_{\mathcal{M}}:\mathcal{C}\to\mathcal{C}$ defined by

$$(\alpha^{-}_{\mathcal{M}})\circ\partial_{\mathcal{M}}=\alpha^{+}_{\mathcal{M}} \tag{23}$$

is a braided autoequivalence of $\mathcal{C}$. The assignment $\mathcal{M}\mapsto\partial_{\mathcal{M}}$ gives rise to a group homomorphism

$$\partial:\mathrm{Pic}(\mathcal{C})\to\mathrm{Aut}^{\mathrm{br}}(\mathcal{C}),\quad \mathcal{M}\mapsto\partial_{\mathcal{M}}. \tag{24}$$

To be precise, the condition (23) defines a tensor autoequivalence of $\mathcal{C}$. The reason why it is braided is explained in Remark 4.5 (see also [Etingof et al. 2010] for details in the fusion case).

3. The Picard crossed module of a braided tensor category

3A. ***Algebras and their modules.*** We refer the reader to [Ostrik 2003b] for basic definitions and facts about algebras in tensor categories and modules over them.

Let A be an algebra in a tensor category $\mathscr{A}$ with the multiplication $\mu : A \otimes A \to A$ and let M be a right A-module in $\mathscr{A}$ with the structural map $\nu : M \otimes A \to M$. For any $X \in \mathscr{A}$ there is an A-module structure on $X \otimes M$ defined by

$$\mathrm{id}_X \otimes \nu : X \otimes M \otimes A \to X \otimes M.$$

Thus the category $\mathscr{A}_A$ of right A-modules in $\mathscr{A}$ is a left $\mathscr{A}$-module category via

$$\mathscr{A} \times \mathscr{A}_A \to \mathscr{A}_A, \quad (X, M) \mapsto X \otimes M.$$

Similarly, the category ${}_A\mathscr{A}$ of left A-modules in $\mathscr{A}$ is a right $\mathscr{A}$-module category.

We say that an algebra A is *exact* if the $\mathscr{A}$-module categories $\mathscr{A}_A$ and ${}_A\mathscr{A}$ are exact.

Remark 3.1. Let A be an algebra in $\mathscr{A}$. Then the left $\mathscr{A}$-module category $({}_A\mathscr{A})^{\mathrm{op}}$ is equivalent to $\mathscr{A}_A$.

It was shown in [Etingof and Ostrik 2004] that every left (respectively, right) $\mathscr{A}$-module category is equivalent to $\mathscr{A}_A$ (respectively, to ${}_A\mathscr{A}$) for some algebra A in $\mathscr{A}$.

Let A be an algebra in a tensor category $\mathscr{A}$ and $\mathscr{M}$ be a left $\mathscr{A}$-module category. Define ${}_A\mathscr{M}$ (the category of *A-modules in $\mathscr{M}$*) as the category of pairs (M, m), where M is an object of $\mathscr{M}$ and $m : A * M \to M$ is a morphism in $\mathscr{M}$ such that the diagram

$$\begin{array}{ccccc} A*(A*M) & & \xrightarrow{1*m} & & A*M \\ \downarrow{\scriptstyle a_{A,A,M}} & & & \searrow^{m} & \\ & & & & M \\ & & & \nearrow_{m} & \\ (A\otimes A)*M & & \xrightarrow{\mu*1} & & A*M \end{array}$$

commutes.

A morphism between (M, m) and (M', m') is a morphism $f : M \to M'$ such that $f \circ m = m' \circ (\mathrm{id}_A * f)$.

Lemma 3.2. *Let $\mathscr{A}$ be a finite tensor category and let $\mathscr{M}$ be an exact right $\mathscr{A}$-module category. The functor*

$$T : \mathrm{Fun}_{\mathscr{A}}(\mathscr{A}_A, \mathscr{M}) \to {}_A\mathscr{M} : F \mapsto F(A) \tag{25}$$

is an equivalence of categories.

Proof. For any $\mathscr{A}$-module functor $F : \mathscr{A}_A \to \mathscr{M}$ the object $F(A) \in \mathscr{M}$ has a structure of an A-module,

$$A * F(A) \xrightarrow{\simeq} F(A \otimes A) \xrightarrow{F(\mu)} F(A), \tag{26}$$

where the first arrow is given by the $\mathscr{A}$-module structure of F and the second arrow is the image of the multiplication of A. It is easy to see that $\mathscr{A}$-module transformations between $\mathscr{A}$-module functors F, G correspond to morphisms of A-modules $F(A), G(A)$ in $\mathscr{M}$. Thus, T is a well-defined functor.

Define a functor $S : {}_A\mathscr{M} \to \mathrm{Fun}_{\mathscr{A}}(\mathscr{A}_A, \mathscr{M})$ by $M \mapsto S_M$, where $S_M(X) = X \otimes_A M$. It is clear that S_M is an $\mathscr{A}$-module functor and that $T \circ S$ is isomorphic to the identity endofunctor of ${}_A\mathscr{M}$.

Also, $S \circ T$ is isomorphic to the identity functor since for every $\mathscr{A}$-module functor $F : \mathscr{A}_A \to \mathscr{M}$ and a right A-module X in $\mathscr{A}$ there is a natural isomorphism $X \otimes_A F(A) \cong F(X)$. Thus, T is an equivalence. □

A particular case of Lemma 3.2 that will be useful for us later is the category of A-modules in $\mathscr{M} = \mathscr{A}_B$, where B is an exact algebra in $\mathscr{A}$. The category ${}_A\mathscr{A}_B$ is the category of *$(A$-$B)$-bimodules in $\mathscr{C}$*.

Corollary 3.3. *The functor*

$$\mathrm{Fun}_{\mathscr{A}}(\mathscr{A}_A, \mathscr{A}_B) \to {}_A\mathscr{A}_B, \quad F \mapsto F(A)$$

is an equivalence of categories.

3B. ***Tensor product of algebras in a braided category.*** Let now $\mathscr{C}$ be a braided tensor category and let A be an algebra in $\mathscr{C}$. Given a left $\mathscr{C}$-module category $\mathscr{M}$, the braiding in $\mathscr{C}$ allows us to turn ${}_A\mathscr{M}$ into a left $\mathscr{C}$-module category. In this situation the functor $\mathrm{Fun}_{\mathscr{C}}(\mathscr{C}_A, \mathscr{M}) \xrightarrow{\sim} {}_A\mathscr{M}$ from Lemma 3.2 is an equivalence of $\mathscr{C}$-module categories.

It is well-known that for braided $\mathscr{C}$ the tensor product $A \otimes B$ of two algebras $A, B \in \mathscr{C}$ has an algebra structure, with the multiplication map $\mu_{A\otimes B}$ defined as

$$A \otimes B \otimes A \otimes B \xrightarrow{\mathrm{id}_A \otimes c_{B,A} \otimes \mathrm{id}_B} A \otimes A \otimes B \otimes B \xrightarrow{\mu_A \otimes \mu_B} A \otimes B,$$

where μ_A and μ_B are multiplications of algebras A and B, respectively (here we suppress the associativity constraints in $\mathscr{C}$).

Let $A^{\mathrm{op}} = A$ denote the algebra with the multiplication opposite to that of A:

$$A \otimes A \xrightarrow{c_{A,A}} A \otimes A \xrightarrow{\mu_A} A.$$

Proposition 3.4. *Let $\mathscr{C}$ be a braided tensor category and let A and B be exact algebras in $\mathscr{C}$. Then*

$$\mathscr{C}_A \boxtimes_{\mathscr{C}} \mathscr{C}_B \simeq \mathscr{C}_{A\otimes B}$$

as $\mathscr{C}$-module categories.

Proof. Note that a left $\mathscr{C}$-module category $\mathscr{C}_A$ considered as a right $\mathscr{C}$-module category is equivalent to ${}_{A^{\mathrm{op}}}\mathscr{C}$. By Remark 3.1 the opposite category $({}_{A^{\mathrm{op}}}\mathscr{C})^{\mathrm{op}}$ is equivalent to $\mathscr{C}_{A^{\mathrm{op}}}$ as a left $\mathscr{C}$-module category.

Hence, using (13) and Corollary 3.3 we obtain $\mathcal{C}_A \boxtimes_{\mathcal{C}} \mathcal{C}_B \simeq \mathrm{Fun}_{\mathcal{C}}\big({}_{(A^{\mathrm{op}}\mathcal{C})^{\mathrm{op}}}\mathcal{C}_B\big) \simeq \mathrm{Fun}_{\mathcal{C}}({}_{A^{\mathrm{op}}}\mathcal{C}_B, \mathcal{C}_B) \simeq {}_{A^{\mathrm{op}}}\mathcal{C}_B \simeq \mathcal{C}_{A\otimes B}$, since an $(A\otimes B)$-module in $\mathcal{C}$ is the same thing as an $(A^{\mathrm{op}} - B)$-bimodule. □

3C. ***Azumaya algebras.*** Here we recall the characterization of algebras in $\mathcal{C}$ whose categories of modules are invertible.

Let A be an exact algebra in a braided tensor category $\mathcal{C}$.

Note that multiplication on A, via

$$A \otimes A^{\mathrm{op}} \otimes A \xrightarrow{\mathrm{id}_A \otimes c_{A,A}} A \otimes A \otimes A \xrightarrow{\mu_A \otimes \mathrm{id}_A} A \otimes A \xrightarrow{\mu_A} A,$$

induces a homomorphism of algebras

$$A \otimes A^{\mathrm{op}} \to A \otimes A^*, \tag{27}$$

where A^* is the dual object to A and the multiplication in $A \otimes A^*$ is defined using the evaluation morphism.

Definition 3.5. An exact algebra A in a braided tensor category $\mathcal{C}$ is *Azumaya* if the map (27) is an isomorphism.

It was established in [Van Oystaeyen and Zhang 1998, Theorem 3.1] that A is an Azumaya algebra if and only if the tensor functors

$$\alpha^{\pm}_{\mathcal{C}_A} : \mathcal{C} \to {}_A\mathcal{C}_A$$

defined in (22) are equivalences. Thus, the Picard group of $\mathcal{C}$ is isomorphic to the group of Morita equivalence classes of Azumaya algebras (the latter group was considered in [Van Oystaeyen and Zhang 1998]).

Let A be an Azumaya algebra in $\mathcal{C}$. Let $\partial_A = \partial_{\mathcal{C}_A}$ denote the braided autoequivalence introduced in (24). By definition of ∂_A, there exists a natural isomorphism of right A-modules

$$\phi_X : A \otimes X \xrightarrow{\simeq} \partial_A(X) \otimes A, \quad X \in \mathcal{C}.$$

This means that the following diagram commutes:

$$\begin{array}{ccc}
A \otimes X \otimes A & \xrightarrow{\phi_X \otimes \mathrm{id}_A} & \partial_A(X) \otimes A \otimes A \\
{\scriptstyle c_{A,X}\otimes \mathrm{id}_A}\downarrow & & \\
X \otimes A \otimes A & & \\
{\scriptstyle \mathrm{id}_X \otimes \mu_A}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{\partial_A(X)}\otimes \mu_A} \\
X \otimes A & & \\
{\scriptstyle c_{X,A}}\downarrow & & \\
A \otimes X & \xrightarrow{\phi_X} & \partial_A(X) \otimes A.
\end{array} \tag{28}$$

The tensor structure

$$\nu_{X,Y} : \partial_A(X \otimes Y) \xrightarrow{\simeq} \partial_A(X) \otimes \partial_A(Y), \quad X, Y \in \mathcal{C}$$

of ∂_A satisfies the following commutative diagram:

$$\begin{array}{ccc} A \otimes X \otimes Y & \xrightarrow{\phi_X \otimes \mathrm{id}_Y} & \partial_A(X) \otimes A \otimes Y \\ \downarrow{\scriptstyle \phi_{X\otimes Y}} & & \downarrow{\scriptstyle \mathrm{id}_{\partial_A(X)} \otimes \phi_Y} \\ \partial_A(X \otimes Y) \otimes A & \xrightarrow{\nu_{X,Y}} & \partial_A(X) \otimes \partial_A(Y) \otimes A. \end{array} \tag{29}$$

Lemma 3.6. *The diagram*

$$\begin{array}{ccccc} A \otimes X \otimes A \otimes Y & & \xrightarrow{\phi_X \otimes \phi_Y} & & \partial_A(X) \otimes A \otimes \partial_A(Y) \otimes A \\ \downarrow{\scriptstyle c_{X,A}} & & & & \downarrow{\scriptstyle c_{A,\partial_A(Y)}} \\ A \otimes A \otimes X \otimes Y & & & & \partial_A(X) \otimes \partial_A(Y) \otimes A \otimes A \\ \downarrow{\scriptstyle m_A} & & & & \downarrow{\scriptstyle m_A} \\ A \otimes X \otimes Y & \xrightarrow{\phi_{X\otimes Y}} & \partial_A(X \otimes Y) \otimes A & \xrightarrow{\nu_{X,Y}} & \partial_A(X) \otimes \partial_A(Y) \otimes A \end{array} \tag{30}$$

is commutative (*here*, *as usual*, *we suppress the associativity constraints and identity morphisms*).

Proof. Note that compositions of the left and the right vertical arrows in diagram (30) coincide, respectively, with the canonical epimorphisms

$$A \otimes X \otimes A \otimes Y \to (A \otimes X) \otimes_A (A \otimes Y) \cong A \otimes X \otimes Y$$

and

$$\partial_{\mathcal{A}}(X) \otimes A \otimes \partial_{\mathcal{A}}(Y) \otimes A \to (\partial_A(X) \otimes A) \otimes_A (\partial_A(Y) \otimes A) \cong \partial_{\mathcal{A}}(X) \otimes \partial_{\mathcal{A}}(Y) \otimes A.$$

Hence, the diagram

$$\begin{array}{ccccc} A \otimes X \otimes A \otimes Y & & \xrightarrow{\phi_X \otimes \phi_Y} & & \partial_A(X) \otimes A \otimes \partial_A(Y) \otimes A \\ \downarrow{\scriptstyle c_{X,A}} & & & & \downarrow{\scriptstyle c_{A,\partial_A(Y)}} \\ A \otimes A \otimes X \otimes Y & & & & \partial_A(X) \otimes \partial_A(Y) \otimes A \otimes A \\ \downarrow{\scriptstyle \mu_A} & & & & \downarrow{\scriptstyle m_A} \\ A \otimes X \otimes Y & \xrightarrow{\phi_X} & \partial_A(X) \otimes A \otimes Y & \xrightarrow{\phi_Y} & \partial_A(X) \otimes \partial_A(Y) \otimes A \end{array} \tag{31}$$

is commutative by functoriality of $\otimes_A$. But the bottom row composition in diagram (31) coincides with that of diagram (30) by the identity (29). □

Let B be an algebra in $\mathscr{C}$ and suppose that A is an Azumaya algebra in $\mathscr{C}$. Then $\partial_A(B)$ is also an algebra in $\mathscr{C}$. We will denote by

$$\mu_B : B \otimes B \to B \quad \text{and} \quad \mu_{\partial_A(B)} : \partial_A(B) \otimes \partial_A(B) \to \partial_A(B)$$

the multiplications of B and $\partial_A(B)$ respectively.

Proposition 3.7. *The morphism $\phi_B : A \otimes B \to \partial_A(B) \otimes A$ is an isomorphism of algebras.*

Proof. Consider the diagram

$$\begin{array}{ccccc}
A \otimes B \otimes A \otimes B & & \xrightarrow{\phi_B \otimes \phi_B} & & \partial_A(B) \otimes A \otimes \partial_A(B) \otimes A \\
\downarrow{\scriptstyle c_{B,A}} & & & & \downarrow{\scriptstyle c_{A,\partial_A(B)}} \\
A \otimes A \otimes B \otimes B & & & & \partial_A(B) \otimes \partial_A(B) \otimes A \otimes A \\
\downarrow{\scriptstyle \mu_A} & & & & \downarrow{\scriptstyle \mu_A} \\
A \otimes B \otimes B & \xrightarrow{\phi_{B\otimes B}} & \partial_A(B \otimes B) \otimes A & \xrightarrow{\nu_{B,B}} & \partial_A(B) \otimes \partial_A(B) \otimes A \\
\downarrow{\scriptstyle \mu_B} & & & & \downarrow{\scriptstyle \mu_{\partial_A(B)}} \\
A \otimes B & & \xrightarrow{\phi_B} & & \partial(B) \otimes A.
\end{array} \tag{32}$$

The upper subdiagram is commutative by Lemma 3.6 and the lower subdiagram is the definition of multiplication $\mu_{\partial_A(B)}$. Hence, diagram (32) is commutative. This is precisely the property of ϕ_B being an algebra homomorphism. □

3D. *Definition of the Picard crossed module.*

Definition 3.8. A *crossed module* (G, C) is a pair of groups G and C together with an action of G on C, denoted by $(g, c) \mapsto {}^g c$, and a homomorphism $\partial : C \to G$ satisfying

$$\partial({}^g c) = g\partial(c)g^{-1} \tag{33}$$

and

$${}^{\partial(c)}c' = cc'c^{-1} \quad c, c' \in C, g \in G. \tag{34}$$

Let (G_1, C_1) and (G_2, C_2) be crossed modules with structural maps $\partial_1 : C_1 \to G_1$ and $\partial_1 : C_2 \to G_2$. A *homomorphism* between these crossed modules is a pair of group homomorphisms $\gamma : G_1 \to G_2$ and $\phi : \mathscr{C}_1 \to \mathscr{C}_2$ such that $\partial_2 \circ \phi = \gamma \circ \partial_1$ and $\phi({}^g c) = {}^{\gamma(g)}\phi(c)$ for all $c \in C_1$ and $g \in G_1$.

Remark 3.9. It is clear that the kernel of the homomorphism ∂ in Definition 3.8 is a subgroup of the center of C and the image of ∂ is a normal subgroup of G.

Let $\mathscr{C}$ be a braided tensor category. Set

$$G := \mathrm{Aut}^{\mathrm{br}}(\mathscr{C}), \quad C := \mathrm{Pic}(\mathscr{C}). \tag{35}$$

In (24) we defined a canonical homomorphism

$$\partial : C \to G : \mathcal{M} \mapsto \partial_{\mathcal{M}}.$$

There is also a canonical action of $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ on $\mathrm{Pic}(\mathcal{C})$. Namely, for $g \in \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ and a $\mathcal{C}$-module category $\mathcal{M}$ the category ${}^g\mathcal{M}$ is defined as follows. As an abelian category, ${}^g\mathcal{M} = \mathcal{M}$. The action of $\mathcal{C}$ on $\mathcal{M}$ is defined by

$$X \odot M := g^{-1}(X) * M \quad \text{for all } M \in \mathcal{M},\ X \in \mathcal{C}.$$

Note that for an algebra $A \in \mathcal{C}$ the $\mathcal{C}$-module category ${}^g(\mathcal{C}_A)$ is equivalent to $\mathcal{C}_{g(A)}$. Here $g(A)$ is the algebra with multiplication $\mu_{g(A)} = g(\mu_A)$.

Theorem 3.10. *The pair* $(G, C) = (\mathrm{Aut}^{\mathrm{br}}(\mathcal{C}), \mathrm{Pic}(\mathcal{C}))$ *equipped with the above structural operations is a crossed module.*

Proof. To check the axiom (33), note that tensor equivalences

$$\alpha^{\pm}_{{}^g\mathcal{M}} : \mathcal{C} \to \mathcal{C}^*_{{}^g\mathcal{M}}$$

defined in (22) satisfy $\alpha^{\pm}_{{}^g\mathcal{M}} \cong \alpha^{\pm}_{\mathcal{M}} \circ g^{-1}$. Hence,

$$\partial_{{}^g\mathcal{M}} \cong (\alpha^{-}_{{}^g\mathcal{M}})^{-1} \circ \alpha^{+}_{{}^g\mathcal{M}} \cong g \circ \partial_{\mathcal{M}} \circ g^{-1} \quad \text{for all } \mathcal{M} \in \mathrm{Pic}(\mathcal{C}),\ g \in G. \tag{36}$$

Let us check axiom (34). Take $\mathcal{M}, \mathcal{N} \in \mathrm{Pic}(\mathcal{C})$ and let A and B be algebras in $\mathcal{C}$ such that $\mathcal{M} \simeq \mathcal{C}_A$ and $\mathcal{N} \simeq \mathcal{C}_B$. By Proposition 3.4 we have

$$\mathcal{M} \boxtimes_{\mathcal{C}} \mathcal{N} \simeq \mathcal{C}_{A \otimes B} \quad \text{and} \quad {}^{\partial_{\mathcal{M}}}\mathcal{N} \boxtimes_{\mathcal{C}} \mathcal{M} \simeq \mathcal{C}_{\partial_{\mathcal{M}}(B) \otimes A}.$$

Since by Proposition 3.7 the algebras $A \otimes B$ and $\partial_{\mathcal{M}}(B) \otimes A$ are isomorphic, we conclude $\mathcal{M} \boxtimes_{\mathcal{C}} \mathcal{N} \simeq {}^{\partial_{\mathcal{M}}}\mathcal{N} \boxtimes_{\mathcal{C}} \mathcal{M}$, as required. □

Definition 3.11. We will call the pair $\big(\mathrm{Aut}^{\mathrm{br}}(\mathcal{C}), \mathrm{Pic}(\mathcal{C})\big)$ the *Picard crossed module* of $\mathcal{C}$ and denote it $\mathfrak{P}(\mathcal{C})$.

4. Picard crossed module and braided autoequivalences of the center

In this section we give a characterization of the Picard crossed module of a braided tensor category $\mathcal{C}$ in terms of braided autoequivalences of $\mathcal{Z}(\mathcal{C})$.

4A. ***The Brauer–Picard group and braided autoequivalences of the center.*** Let $\mathcal{M}$ be an exact left $\mathcal{C}$-module category. It can be regarded as a $(\mathcal{C} \boxtimes \mathcal{C}^*_{\mathcal{M}})$-module category. The following constructions are taken from [Etingof and Ostrik 2004, Section 3.4]: There are canonical equivalences

$$a_{\mathcal{M}} : \mathcal{Z}(\mathcal{C}) \xrightarrow{\sim} (\mathcal{C} \boxtimes \mathcal{C}^*_{\mathcal{M}})^*_{\mathcal{M}} : (Z, \gamma) \mapsto Z * ?, \tag{37}$$

where the left $\mathscr{C}$-module functor structure of $a_{\mathcal{M}}(Z,\gamma)$ is given by

$$X*(Z*M)\xrightarrow{a_{X,Z,M}}(X\otimes Z)*M\xrightarrow{\gamma_X}(Z\otimes X)*M\xrightarrow{a^{-1}_{Z,X,M}}Z*(X*M) \tag{38}$$

for all $X\in\mathscr{C}$ and $M\in\mathcal{M}$, and its left $\mathscr{C}^*_{\mathcal{M}}$-module functor structure

$$F(Z*M)\xrightarrow{\simeq}Z*F(M) \tag{39}$$

for $F\in\mathscr{C}^*_{\mathcal{M}}$ is given using the $\mathscr{C}$-module functor structure of F.

One defines a functor

$$\tilde{a}_{\mathcal{M}}:\mathfrak{Z}(\mathscr{C}^*_{\mathcal{M}})\xrightarrow{\sim}(\mathscr{C}\boxtimes\mathscr{C}^*_{\mathcal{M}})^*_{\mathcal{M}} \tag{40}$$

in an analogous way.

The composition $\tilde{a}^{-1}_{\mathcal{M}}\circ a_{\mathcal{M}}$ is a braided tensor equivalence between $\mathfrak{Z}(\mathscr{C})$ and $\mathfrak{Z}(\mathscr{C}^*_{\mathcal{M}})^{\mathrm{rev}}=\mathfrak{Z}((\mathscr{C}^*_{\mathcal{M}})^{\mathrm{op}})$.

When $\mathcal{M}$ is an invertible $\mathscr{C}$-bimodule category, the composition of $\tilde{a}_{\mathcal{M}}$ and the braided tensor equivalence $\mathfrak{Z}(\mathscr{C})\xrightarrow{\sim}\mathfrak{Z}((\mathscr{C}^*_{\mathcal{M}})^{\mathrm{op}})$ induced by the tensor equivalence

$$L:\mathscr{C}\xrightarrow{\sim}(\mathscr{C}^*_{\mathcal{M}})^{\mathrm{op}}:X\mapsto ?*X$$

from Remark 2.11 gives a tensor equivalence

$$b_{\mathcal{M}}:\mathfrak{Z}(\mathscr{C})\xrightarrow{\sim}(\mathscr{C}\boxtimes\mathscr{C}^*_{\mathcal{M}})^*_{\mathcal{M}}:(Z,\gamma)\mapsto ?*Z, \tag{41}$$

where the left $\mathscr{C}$-module functor structure of $b_{\mathcal{M}}(Z,\gamma)$ is given by the middle associativity constraint of $\mathcal{M}$,

$$X*(M*Z)\xrightarrow{a_{X,M,Z}}(X*M)*Z, \tag{42}$$

while the right $\mathscr{C}$-module functor structure (which is the same as the left $C^*_{\mathcal{M}}$-module functor structure upon the identification $\mathscr{C}^*_{\mathcal{M}}\simeq\mathscr{C}^{\mathrm{op}}$) of $b_{\mathcal{M}}(Z,\gamma)$ is given using the right $\mathscr{C}$-module associativity constraint of $\mathcal{M}$ and the half-braiding:

$$(M*Z)*Y\xrightarrow{a_{M,Z,Y}}M*(Z\otimes Y)\xrightarrow{\gamma^{-1}_Y}M*(Y\otimes Z)\xrightarrow{a^{-1}_{M,Y,Z}}(M*Y)*Z, \tag{43}$$

for all $X,Y\in\mathscr{C}$ and $M\in\mathcal{M}$.

Thus, we have a canonical braided tensor autoequivalence

$$\Phi(\mathcal{M})=b^{-1}_{\mathcal{M}}\circ a_{\mathcal{M}}:\mathfrak{Z}(\mathscr{C})\to\mathfrak{Z}(\mathscr{C}). \tag{44}$$

The following result was proved in [Etingof et al. 2010, Section 5] when $\mathscr{C}$ is a fusion category. This argument carries over verbatim to the case of finite tensor categories. We recall the proof for the reader's convenience and also for future reference.

Theorem 4.1. *Let $\mathcal{C}$ be a finite tensor category. The assignment $\mathcal{M} \mapsto \Phi(\mathcal{M})$, where $\Phi(\mathcal{M})$ is defined in (44), gives rise to a group isomorphism*

$$\Phi : \mathrm{BrPic}(\mathcal{C}) \xrightarrow{\simeq} \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C})). \tag{45}$$

Proof. To see that Φ is a homomorphism observe that the $\mathcal{C}$-bimodule functor of right multiplication by an object $Z \in \mathcal{Z}(\mathcal{C})$ on $\mathcal{M} \boxtimes_{\mathcal{C}} \mathcal{N}$, where $\mathcal{M}$ and $\mathcal{N}$ are invertible $\mathcal{C}$-bimodule categories, is isomorphic to the well-defined functor of "middle" multiplication by $(\Phi(\mathcal{N}))(Z)$, which, in turn, is isomorphic to the functor of left multiplication by $\big(\Phi(\mathcal{M}) \circ \Phi(\mathcal{N})\big)(Z)$. This gives a natural isomorphism of tensor functors $\Phi(\mathcal{M}) \circ \Phi(\mathcal{N}) \cong \Phi(\mathcal{M} \boxtimes_{\mathcal{C}} \mathcal{N})$. Hence, Φ is a homomorphism.

Let us recall the construction of the map

$$\Psi : \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C})) \to \mathrm{BrPic}(\mathcal{C}), \tag{46}$$

inverse to the homomorphism (45).

Let $F : \mathcal{Z}(\mathcal{C}) \to \mathcal{C}$ and $I : \mathcal{C} \to \mathcal{Z}(\mathcal{C})$ denote the canonical forgetful functor and its right adjoint. Given a braided autoequivalence $\alpha \in \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ let $L_\alpha := \alpha^{-1}(I(\mathbf{1}))$. The category ${}_{L_\alpha}\mathcal{Z}(\mathcal{C})$ is a finite tensor category with respect to $\otimes_{L_\alpha}$.

Let us show that the algebra $F(L_\alpha) \in \mathcal{C}$ is exact, that is, that the category ${}_{L_\alpha}\mathcal{C}$ of $F(L_\alpha)$-modules in $\mathcal{C}$ is exact. By Lemma 3.2 this category is equivalent to $\mathrm{Fun}_{\mathcal{Z}(\mathcal{C})}(\mathcal{Z}(\mathcal{C})_{L_\alpha}, \mathcal{C})$ as a $\mathcal{C}$-module category. By Remark 2.8 the latter category is exact as a $\mathrm{Fun}_{\mathcal{Z}(\mathcal{C})}(\mathcal{C}, \mathcal{C})$-module category. In particular, it is exact as a $\mathcal{C}$-module category.

Let

$$F(L_\alpha) = \bigoplus_{i \in J} L_\alpha^i$$

be the decomposition of $F(L_\alpha)$ into a direct sum of indecomposable exact algebras in $\mathcal{C}$.

For any $i \in J$ the composition

$$\mathcal{C} \xrightarrow{\iota} {}_{L_\alpha}\mathcal{Z}(\mathcal{C}) \xrightarrow{F} {}_{F(L_\alpha)}\mathcal{C}_{F(L_\alpha)} \xrightarrow{\pi_i} {}_{L_\alpha^i}\mathcal{C}_{L_\alpha^i} \tag{47}$$

is a tensor equivalence, where

$$\iota : \mathcal{C} \xrightarrow{\sim} {}_{L_\alpha}\mathcal{Z}(\mathcal{C}) : X \mapsto \alpha^{-1}(I(X)) \tag{48}$$

and π_i is a projection from ${}_{F(L_\alpha)}\mathcal{C}_{F(L_\alpha)} = \bigoplus_{i,j \in J} {}_{L_i}\mathcal{C}_{L_j}$ to the (i,i) component.

Hence, $\mathcal{C}_{L_i}$ gets a structure of an invertible $\mathcal{C}$-bimodule category. Its equivalence class does not depend on a particular $i \in J$. One sets $\Psi(\alpha) := \mathcal{C}_{L_i}$.

The verification of the identities $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$ is the same as in [Etingof et al. 2010, Section 5.3]. □

Remark 4.2. Note that $\mathrm{BrPic}(\mathcal{C})$ and $\mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ are monoidal groupoids (that is, monoidal categories in which every object is invertible). In fact, the assignment (45) is a monoidal equivalence rather than just a group isomorphism, see [Etingof et al. 2010, Section 5].

4B. ***The image of*** $\mathbf{Pic}(\mathcal{C})$ ***in*** $\mathbf{Aut}^{\mathbf{br}}(\mathcal{Z}(\mathcal{C}))$**.** Recall from Section 2H that the group $\mathrm{BrPic}(\mathcal{C})$ contains a subgroup $\mathrm{Pic}(\mathcal{C})$ consisting of equivalence classes of invertible $\mathcal{C}$-module categories (regarded as one-sided $\mathcal{C}$-bimodule categories).

Our goal now is to describe the image of $\mathrm{Pic}(\mathcal{C})$ in $\mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ under isomorphism (45).

Let $\mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C}) \subset \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ be the subgroup consisting of isomorphism classes of braided autoequivalences of $\mathcal{Z}(\mathcal{C})$ trivializable on $\mathcal{C}$, see Definition 2.1.

The next theorem was suggested to us by V. Drinfeld.

Theorem 4.3. *Let $\mathcal{C}$ be a braided tensor category. The canonical isomorphism $\Phi : \mathrm{BrPic}(\mathcal{C}) \xrightarrow{\simeq} \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ restricts to an isomorphism*

$$\Phi|_{\mathrm{Pic}(\mathcal{C})} : \mathrm{Pic}(\mathcal{C}) \xrightarrow{\simeq} \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C}). \tag{49}$$

Proof. First, let us show that $\Phi(\mathrm{Pic}(\mathcal{C})) \subset \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C})$. Let $\mathcal{M}$ be an invertible one-sided $\mathcal{C}$-module category. Let $\Phi(\mathcal{M}) \in \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ be the braided autoequivalence of $\mathcal{Z}(\mathcal{C})$ defined in Section 4A. The equivalences $a_{\mathcal{M}}$ and $b_{\mathcal{M}}$ defined in (37) and (41) can be explicitly described as follows. Let (Z, γ) be an object in $\mathcal{Z}(\mathcal{C})$, where

$$\gamma_X : X \otimes Z \to Z \otimes X, \quad X \in \mathcal{C}$$

is the half-braiding. Then $a_{\mathcal{M}}(Z, \gamma)(M) = Z * M$ and its left and right $\mathcal{C}$-module functor structures are found by translating (38) and (39) to our setting:

$$\begin{array}{ccc} X * (Z * M) & \xrightarrow{\simeq} & Z * (X * M) \\ \downarrow{\scriptstyle a_{X,Z,M}} & & \uparrow{\scriptstyle a^{-1}_{Z,X,M}} \\ (X \otimes Z) * M & \xrightarrow{\gamma_X} & (Z \otimes X) * M \end{array} \tag{50}$$

and

$$\begin{array}{ccccccc} (Z * M) * Y & & \xrightarrow{\quad\simeq\quad} & & & & Z * (M * Y) \\ \| & & & & & & \| \\ Y * (Z * M) & \xrightarrow{a_{Y,Z,M}} & (Y \otimes Z) * M & \xrightarrow{c^{-1}_{Z,Y}} & (Z \otimes Y) * M & \xrightarrow{a^{-1}_{Z,Y,M}} & Z * (Y * M) \end{array} \tag{51}$$

for all $X, Y \in \mathcal{C}$ and $M \in \mathcal{M}$, where a denotes the left $\mathcal{C}$-module associativity constraint of $\mathcal{M}$.

Also, $b_{\mathcal{M}}(Z,\gamma)(M) = M*Z = Z*M$ as a functor and its left and right $\mathcal{C}$-module functor structures are found from (42) and (43):

$$\begin{array}{ccccccc} X*(M*Z) & & \xrightarrow{\quad\simeq\quad} & & & & (X*M)*Z \\ \| & & & & & & \| \\ X*(Z*M) & \xrightarrow{a_{X,Z,M}} & (X\otimes Z)*M & \xrightarrow{c_{X,Z}} & (Z\otimes X)*M & \xrightarrow{a^{-1}_{Z,X,M}} & Z*(X*M) \end{array} \tag{52}$$

and

$$\begin{array}{ccccccc} (M*Z)*Y & & \xrightarrow{\quad\simeq\quad} & & & & (M*Y)*Z \\ \| & & & & & & \| \\ Y*(Z*M) & & & & & & Z*(Y*M) \\ \downarrow{\scriptstyle a_{Y,Z,M}} & & & & & & \uparrow{\scriptstyle a^{-1}_{Z,Y,M}} \\ (Y\otimes Z)*M & \xrightarrow{c_{Y,Z}} & (Z\otimes Y)*M & \xrightarrow{\gamma_Y^{-1}} & (Y\otimes Z)*M & \xrightarrow{c^{-1}_{Z,Y}} & (Z\otimes Y)*M \end{array} \tag{53}$$

for all $X, Y \in \mathcal{C}$ and $M \in \mathcal{M}$.

The diagrams (52) and (51) are nothing but middle associativity isomorphism (17) and its inverse. The diagram (53) uses the right $\mathcal{C}$-module associativity (16) and its inverse as well as the half-braiding of Z.

Since $\mathcal{C}$ is embedded into $\mathcal{Z}(\mathcal{C})$ via

$$Z \mapsto (Z, c_{-,Z}),$$

that is, $\gamma_X = c_{X,Z}$ in this case, we see from (50), (51) and (52), (53) that the restrictions of $a_{\mathcal{M}}$ and $b_{\mathcal{M}}$ on the subcategory $\mathcal{C} \subset \mathcal{Z}(\mathcal{C})$ coincide, that is, $\Phi(\mathcal{M})$ is trivializable on $\mathcal{C}$. So $\Phi(\mathrm{Pic}(\mathcal{C})) \subset \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C})$.

It remains to show that $\Phi(\mathrm{Pic}(\mathcal{C})) = \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C})$. Let $\alpha \in \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C})$. We need to show that the equivalence class of invertible $\mathcal{C}$-bimodule category $\mathcal{M} := \Psi(\alpha)$ $\big($where $\Psi : \mathrm{BrPic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ is the inverse of Φ, see (46)$\big)$ is in $\mathrm{Pic}(\mathcal{C})$.

According to the description from the proof of Theorem 4.1 $\mathcal{M}$ is equivalent to any indecomposable component of the $\mathcal{C}$-module category $\mathcal{C}_{F(L_\alpha)}$ of left modules over the algebra $F(L_\alpha)$, where $L_\alpha = \alpha^{-1}(I(\mathbf{1})) \in \mathcal{Z}(\mathcal{C})$. Thus, it suffices to show that the $\mathcal{C}$-bimodule category $\mathcal{C}_{F(L_\alpha)}$ is one-sided.

The left action of $X \in \mathcal{C}$ on $\mathcal{C}_{F(L_\alpha)}$ is via tensor multiplication:

$$X * M = X \otimes M. \tag{54}$$

The right action of X is via module multiplication over $F(L_\alpha)$ with the image of X under equivalence (47). Let us describe this action explicitly. Since $I(X) \cong X \otimes I(1)$ for all $X \in \mathcal{C} \subset \mathcal{Z}(\mathcal{C})$ and α is trivializable on $\mathcal{C}$ we see that equivalence (48) in

our situation becomes

$$\mathcal{C} \xrightarrow{\sim} \mathcal{Z}(\mathcal{C})_{L_\alpha} : X \mapsto X \otimes L_\alpha. \tag{55}$$

Therefore, the right action of X on $\mathcal{C}_{F(L_\alpha)}$ is given by

$$M * X = M \otimes_{F(L_\alpha)} (X \otimes F(L_\alpha)) \cong M \otimes X \tag{56}$$

for all $X \in \mathcal{C}$, $M \in \mathcal{C}_{F(L_\alpha)}$. The action of $F(L_\alpha)$ on $M * X \cong M \otimes X$ is given by

$$M \otimes X \otimes F(L_\alpha) \xrightarrow{1 \otimes c_{X,F(L_\alpha)}} M \otimes F(L_\alpha) \otimes X \xrightarrow{\rho_M \otimes 1} M \otimes X,$$

where we omit the associativity constraints. Here $\rho_M : M \otimes F(L_\alpha) \to M$ denotes the $F(L_\alpha)$-module structure on M.

We have a natural family of $F(L_\alpha)$-module isomorphisms

$$d_{M,X} := c_{M,X} : M \otimes X \to X \otimes M.$$

To show that the $\mathcal{C}$-bimodule category $\mathcal{C}_{F(L_\alpha)}$ is one-sided we need to check that isomorphisms $d_{X,M}$ satisfy commutative diagrams (20) and (21). But these diagrams are nothing but hexagon axioms of the braiding.

Thus, $\mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C}) \subset \Phi(\mathrm{Pic}(\mathcal{C}))$ and the proof is complete. □

4C. ***A characterization of the Picard crossed module.*** Let $\mathcal{C}$ be a finite braided tensor category. There is a canonical homomorphism

$$\Sigma : \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}) \tag{57}$$

defined as follows. Every braided autoequivalence $\alpha \in \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}))$ trivializable on $\mathcal{C}$ maps the centralizer $\mathcal{C}$ in $\mathcal{Z}(\mathcal{C})$ to itself. This centralizer is $\mathcal{C}^{\mathrm{rev}} \subset \mathcal{Z}(\mathcal{C})$. Hence, α restricts to a braided autoequivalence of $\mathcal{C}^{\mathrm{rev}}$, that is, to an element of $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C}^{\mathrm{rev}}) = \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ which we denote $\Sigma(\alpha)$.

Lemma 4.4. *Let $\mathcal{C}$ be a braided tensor category. The composition*

$$\mathrm{Pic}(\mathcal{C}) \xrightarrow{\Phi} \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}(\mathcal{C}); \mathcal{C}) \xrightarrow{\Sigma} \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$$

coincides with homomorphism $\partial : \mathrm{Pic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ defined in (24).

Proof. We need to show that for each invertible $\mathcal{C}$-module category $\mathcal{M}$ the restriction of the braided autoequivalence $\Phi(\mathcal{M})$ on $\mathcal{C}^{\mathrm{rev}} \subset \mathcal{Z}(\mathcal{C})$ is isomorphic to $\partial_{\mathcal{M}}$ defined in (23). This result follows from comparing definitions. Indeed, $\Phi(\mathcal{M}) = b_{\mathcal{M}}^{-1} \circ a_{\mathcal{M}}$, where $a_{\mathcal{M}}$ and $b_{\mathcal{M}}$ are defined in (37) and (41), and $\partial_{\mathcal{M}} = (\alpha_{\mathcal{M}}^{-})^{-1} \circ \alpha_{\mathcal{M}}^{+}$, where $\alpha_{\mathcal{M}}^{\pm}$ are defined in (22).

Thus, it suffices to check the commutativity of the diagrams

$$\begin{array}{ccc} \mathfrak{Z}(\mathcal{C}) & \xrightarrow{a_{\mathcal{M}}} & (\mathcal{C}\boxtimes\mathcal{C}^{\mathrm{op}})^*_{\mathcal{M}} \\ \uparrow & & \downarrow \\ \mathcal{C}^{\mathrm{rev}} & \xrightarrow{\alpha^+_{\mathcal{M}}} & \mathcal{C}^*_{\mathcal{M}} \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathfrak{Z}(\mathcal{C}) & \xrightarrow{b_{\mathcal{M}}} & (\mathcal{C}\boxtimes\mathcal{C}^{\mathrm{op}})^*_{\mathcal{M}} \\ \uparrow & & \downarrow \\ \mathcal{C}^{\mathrm{rev}} & \xrightarrow{\alpha^-_{\mathcal{M}}} & \mathcal{C}^*_{\mathcal{M}}, \end{array} \tag{58}$$

where the arrows $\mathcal{C}^{\mathrm{rev}} \to \mathfrak{Z}(\mathcal{C})$ are given by the embedding (4) and the arrows $(\mathcal{C}\boxtimes\mathcal{C}^{\mathrm{op}})^*_{\mathcal{M}} \to \mathcal{C}^*_{\mathcal{M}}$ are given by the restriction of $\mathcal{C}$-bimodule functors to left $\mathcal{C}$-module functors. The commutativity is checked directly using definitions of $\alpha^{\pm}_{\mathcal{M}}$ in Section 2I and explicit formulas (50) and (52) for the $\mathcal{C}$-module functor structures of $a_{\mathcal{M}}(Z,\gamma)$ and $b_{\mathcal{M}}(Z,\gamma)$, where (Z,γ) is an object in $\mathfrak{Z}(\mathcal{C})$. In the bottom row of (58) we use that $\mathcal{C}^{\mathrm{rev}} = \mathcal{C}$ as tensor categories.

Hence, $\Phi(\mathcal{M})|_{\mathcal{C}^{\mathrm{rev}}} = \partial_{\mathcal{M}}$ in $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C}) = \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}^{\mathrm{rev}})$. □

Remark 4.5. Lemma 4.4 shows that the homomorphism $\partial : \mathrm{Pic}(\mathcal{C}) \to \mathrm{Aut}(\mathcal{C})$ defined in (24) factors through $\mathrm{Pic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$.

The next corollary was established in [Etingof et al. 2010] for braided fusion categories.

Corollary 4.6. *Let $\mathcal{C}$ be a factorizable braided tensor category. Then $\partial : \mathrm{Pic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ is an isomorphism.*

Proof. We have $\mathfrak{Z}(\mathcal{C}) \cong \mathcal{C}\boxtimes\mathcal{C}^{\mathrm{rev}}$ and $\mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C});\mathcal{C}) = \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}^{\mathrm{rev}}) = \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$. □

There is canonical action of $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ on $\mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C});\mathcal{C})$ defined as follows. Any tensor autoequivalence g of $\mathcal{C}$ induces a braided autoequivalence $\tilde{g} \in \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C}))$:

$$\tilde{g}(Z,\gamma) = (g(Z), \gamma^g),$$

where $(\gamma^g)_X : X\otimes g(Z) \xrightarrow{\simeq} g(Z)\otimes X$ is given by $(\gamma^g)_X = g(\gamma_{g^{-1}(X)})$.

For all $g \in \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$ and $\alpha \in \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C});\mathcal{C})$ set

$$^g\alpha := \tilde{g}\circ\alpha\circ\tilde{g}^{-1}. \tag{59}$$

It is clear that $^g\alpha$ is trivializable on $\mathcal{C}$, that is, (59) defines the required action.

Lemma 4.7. *The isomorphism*

$$\Phi : \mathrm{Pic}(\mathcal{C}) \xrightarrow{\sim} \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C});\mathcal{C})$$

is $\mathrm{Aut}^{\mathrm{br}}(\mathcal{C})$*-equivariant*; *that is*,

$$\Phi(^g\mathcal{M}) = {}^g\Phi(\mathcal{M})$$

for all $g \in \mathrm{Aut}^{\mathrm{br}}(\mathscr{C})$ *and* $\mathscr{M} \in \mathrm{Pic}(\mathscr{C})$.

Proof. This is an immediate consequence of the identities

$$a_{{}^g\mathscr{M}} = a_{\mathscr{M}} \circ \tilde{g}^{-1} \quad \text{and} \quad b_{{}^g\mathscr{M}} = b_{\mathscr{M}} \circ \tilde{g}^{-1}.$$

We have $\Phi({}^g\mathscr{M}) = b_{{}^g\mathscr{M}}^{-1} \circ a_{{}^g\mathscr{M}} = \tilde{g} \circ \Phi(\mathscr{M}) \circ \tilde{g}^{-1} = {}^g\Phi(\mathscr{M})$. □

Corollary 4.8. *The pair of groups* $\big(\mathrm{Aut}^{\mathrm{br}}(\mathscr{C}), \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}); \mathscr{C})\big)$ *along with the action* (59) *and homomorphism* $\Sigma : \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}); \mathscr{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathscr{C})$ *from* (57) *is a crossed module.*

Proof. This follows from Lemmas 4.4 and 4.7. □

We will call the crossed module $\big(\mathrm{Aut}^{\mathrm{br}}(\mathscr{C}), \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}); \mathscr{C})\big)$ the *autoequivalence* crossed module of $\mathscr{C}$ and denote it by $\mathfrak{A}(\mathscr{C})$.

Corollary 4.9. *The pair of group isomorphisms* $(\mathrm{id}_{\mathrm{Aut}^{\mathrm{br}}(\mathscr{C})}, \Phi)$ *is an isomorphism of crossed modules*

$$\mathfrak{P}(\mathscr{C}) \cong \mathfrak{A}(\mathscr{C}). \tag{60}$$

Proof. This follows from Lemmas 4.4 and 4.7. □

4D. ***On the kernel and cokernel of*** ∂ **:** $\mathbf{Pic}(\mathscr{C}) \to \mathbf{Aut}^{\mathbf{br}}(\mathscr{C})$**.** Since the Picard crossed module $\mathfrak{P}(\mathscr{C})$ is isomorphic to the autoequivalence crossed module of $\mathfrak{A}(\mathscr{C})$, the kernel of $\partial : \mathrm{Pic}(\mathscr{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathscr{C})$ is isomorphic to the kernel of the restriction map $\partial : \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}), \mathscr{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathscr{C})$.

The natural tensor embeddings $\mathfrak{Z}_{\mathrm{sym}}(\mathscr{C}) \hookrightarrow \mathscr{C}, \mathscr{C}^{\mathrm{rev}}$ allow us to look at $\mathscr{C}$ and $\mathscr{C}^{\mathrm{rev}}$ as $\mathfrak{Z}_{\mathrm{sym}}(\mathscr{C})$-module categories. The functor $\mathscr{C} \boxtimes \mathscr{C}^{\mathrm{rev}} \to \mathfrak{Z}(\mathscr{C})$ of (5) is clearly balanced with respect to these module structures. Hence, it factors through $\mathscr{C} \boxtimes_{\mathfrak{Z}_{\mathrm{sym}}(\mathscr{C})} \mathscr{C}^{\mathrm{rev}}$. Here the tensor product $\mathscr{C} \boxtimes_{\mathfrak{Z}_{\mathrm{sym}}(\mathscr{C})} \mathscr{C}^{\mathrm{rev}}$ of module categories over a symmetric tensor category $\mathfrak{Z}_{\mathrm{sym}}(\mathscr{C})$ has a natural structure of braided tensor category, see [Davydov et al. 2013]. The image of $\mathscr{C} \boxtimes_{\mathfrak{Z}_{\mathrm{sym}}(\mathscr{C})} \mathscr{C}^{\mathrm{rev}}$ in $\mathfrak{Z}(\mathscr{C})$ coincides with the full tensor subcategory $\mathscr{C} \vee \mathscr{C}^{\mathrm{rev}}$ generated by $\mathscr{C}$ and $\mathscr{C}^{\mathrm{rev}}$ in $\mathfrak{Z}(\mathscr{C})$.

Proposition 4.10. *The kernel of the restriction map* $\partial : \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}), \mathscr{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathscr{C})$ *coincides with the group* $\mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}), \mathscr{C} \vee \mathscr{C}^{\mathrm{rev}})$ *of braided autoequivalences of* $\mathfrak{Z}(\mathscr{C})$ *trivializable on* $\mathscr{C} \vee \mathscr{C}^{\mathrm{rev}}$.

Proof. The kernel of the restriction map $\partial : \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}), \mathscr{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathscr{C})$ coincides with the subgroup $\mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathscr{C}))$ of braided autoequivalences of $\mathfrak{Z}(\mathscr{C})$, trivializable on both $\mathscr{C}$ and $\mathscr{C}^{\mathrm{rev}}$. All we need to show is that a braided autoequivalence of $\mathfrak{Z}(\mathscr{C})$ that is trivializable on both $\mathscr{C}$ and $\mathscr{C}^{\mathrm{rev}}$ is trivializable on $\mathscr{C} \vee \mathscr{C}^{\mathrm{rev}}$.

A braided autoequivalence F of $\mathcal{Z}(\mathcal{C})$ stabilizing both $\mathcal{C}$ and $\mathcal{C}^{\mathrm{rev}}$ and trivializable on $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ fits into a commutative diagram:

$$\begin{array}{ccccc}
\mathcal{C}\boxtimes\mathcal{C}^{\mathrm{rev}} & \longrightarrow & \mathcal{C}\boxtimes_{\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})}\mathcal{C}^{\mathrm{rev}} & \longrightarrow & \mathcal{Z}(\mathcal{C}) \\
\downarrow{\scriptstyle F\boxtimes F} & & \downarrow{\scriptstyle F\boxtimes_{\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})}F} & & \downarrow{\scriptstyle F} \\
\mathcal{C}\boxtimes\mathcal{C}^{\mathrm{rev}} & \longrightarrow & \mathcal{C}\boxtimes_{\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})}\mathcal{C}^{\mathrm{rev}} & \longrightarrow & \mathcal{Z}(\mathcal{C}).
\end{array}$$

Thus a braided autoequivalence F of $\mathcal{Z}(\mathcal{C})$ that is trivializable on both $\mathcal{C}$ and $\mathcal{C}^{\mathrm{rev}}$ is also trivializable on $\mathcal{C}\vee\mathcal{C}^{\mathrm{rev}}$. □

Note that there is a canonical homomorphism

$$j : \mathrm{Pic}(\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})) \to \ker\bigl(\mathrm{Pic}(\mathcal{C}) \xrightarrow{\partial} \mathrm{Aut}^{\mathrm{br}}(\mathcal{C};\mathcal{Z}_{\mathrm{sym}}(\mathcal{C}))\bigr) \tag{61}$$

given by the induction of module categories. Namely, if $\mathcal{M}$ is an invertible $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$-module category then

$$j(\mathcal{M}) = \mathcal{C}\boxtimes_{\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})}\mathcal{M}.$$

To see that $j(\mathcal{M})$ is in the kernel of ∂, let us take an algebra A in $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ such that $\mathcal{M}\simeq\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})_A$. By Lemma 3.2 we have

$$j(\mathcal{M}) = \mathrm{Fun}_{\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})}(\mathcal{C},\mathcal{M}) \simeq \mathcal{C}_A.$$

The functors $\alpha^{\pm}_{j(\mathcal{M})}$ coincide with each other since $c_{X,A} = c^{-1}_{A,X}$ for all objects X in $\mathcal{C}$, that is, $\partial(j(\mathcal{M}))$ is a trivial autoequivalence.

Let $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ be the symmetric center of $\mathcal{C}$, see Section 2D. Clearly the restrictions of $\alpha^{\pm}_{\mathcal{M}}$ to $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ coincide. Hence for an invertible $\mathcal{M}$ the autoequivalence $\partial_{\mathcal{M}}$ is trivializable on $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$, that is, the restriction of $\partial_{\mathcal{M}}$ to $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})$ is isomorphic to the identity functor. Thus the homomorphism (24) factors as follows.

$$\mathrm{Pic}(\mathcal{C}) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C};\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}).$$

Hence, the restriction map defines canonical homomorphism from the cokernel of ∂:

$$\mathrm{coker}\bigl(\mathrm{Pic}(\mathcal{C}) \xrightarrow{\partial} \mathrm{Aut}^{\mathrm{br}}(\mathcal{C})\bigr) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{Z}_{\mathrm{sym}}(\mathcal{C})). \tag{62}$$

5. The Picard crossed module of a pointed braided fusion category

Let A be a finite abelian group and let $q : A \to k^{\times}$ be a quadratic form on A. In this section we explicitly compute the Picard crossed module of the pointed braided fusion category $\mathcal{C} := \mathcal{C}(A,q)$ associated to the pair (A,q) as in Example 2.2.

Note that $\mathcal{C}(A,q)^{\mathrm{rev}} \simeq \mathcal{C}(A,q^{-1})$.

5A. ***Invertible module categories over a braided pointed fusion category.*** The classification of module categories over pointed fusion categories is well-known [Ostrik 2003a]. Any indecomposable $\mathcal{C}$-module category $\mathcal{M}$ corresponds to a pair (B,γ), where $B \subset A$ is a subgroup and $\gamma : B \times B \to k^\times$ is a function such that

$$d(\gamma)(x,y,z) := \frac{\gamma(x+y,z)\gamma(x,y)}{\gamma(x,y+z)\gamma(y,z)} = \omega(x,y,z), \quad x,y,z \in B. \tag{63}$$

Here $\omega : A^3 \to k^\times$ is the 3-cocycle defining the associativity constraint of $\mathcal{C}$.

The pair (B,γ) is constructed from $\mathcal{M}$ as follows. The simple objects of $\mathcal{M}$ form a transitive A-set and B denotes the stabilizer of a point in this set. The function $\gamma : B \times B \to k^\times$ comes from the module associativity constraint of $\mathcal{M}$. This function is determined by $\mathcal{M}$ up to a 2-coboundary.

Let us define a function $\beta : B \times B \to k^\times$ by

$$\beta(x,y) = c(x,y)\frac{\gamma(x,y)}{\gamma(y,x)}, \quad x,y \in B, \tag{64}$$

where the function $c : A \times A \to k^\times$ is defined in Example 2.2.

Proposition 5.1. *The function (64) is bimultiplicative and satisfies*

$$\beta(x,x) = q(x) \quad \textit{for all } x \in B. \tag{65}$$

Proof. For all $x,y,z \in B$ we compute

$$\begin{aligned}
&\beta(x,y+z)\\
&\quad = c(x,y+z)\frac{\gamma(x,y+z)\gamma(y,z)}{\gamma(y+z,x)\gamma(y,z)}\\
&\quad = c(x,y+z)\frac{\gamma(x+y,z)\gamma(x,y)}{\gamma(y,z+x)\gamma(z,x)}\omega^{-1}(x,y,z)\omega^{-1}(y,z,x)\\
&\quad = c(x,y+z)\frac{\gamma(y+x,z)\gamma(y,x)}{\gamma(y,x+z)\gamma(x,z)}\frac{\gamma(x,y)}{\gamma(y,x)}\frac{\gamma(x,z)}{\gamma(z,x)}\omega^{-1}(x,y,z)\omega^{-1}(y,z,x)\\
&\quad = \beta(x,y)\beta(x,z)\frac{c(x,y+z)}{c(x,y)c(x,z)}\frac{\omega(y,x,z)}{\omega(x,y,z)\omega(y,z,x)}\\
&\quad = \beta(x,y)\beta(x,z).
\end{aligned}$$

In the second and the fourth equalities we used identity (63) and in the last equality we used (7). Thus, β is multiplicative in the second argument. That it is multiplicative in the first argument is proved in a similar way. Finally, the identity $\beta(x,x) = q(x)$ is obtained by setting $y = x$ in (64). □

Corollary 5.2. *There is a bijection between*

$$\left\{\begin{array}{c}\text{equivalence classes of}\\ \text{indecomposable module}\\ \mathcal{C}(A,\,q)\text{-categories}\end{array}\right\} \text{ and } \left\{\begin{array}{c}\text{pairs } (B,\,\beta),\text{ where } B \text{ is a subgroup of } A,\\ \beta : B\times B\to k^\times \text{ is bimultiplicative and}\\ \beta(x,\,x)=q(x),\ x\in B\end{array}\right\}.$$

Proof. Let B be a subgroup of A corresponding to an indecomposable $\mathcal{C}$-module category. Formula (64) defines a map between sets

$$\left\{\begin{array}{c}\text{maps } \gamma : B\times B\to k^\times\\ \text{such that } d(\gamma)=\omega\\ \text{modulo coboundaries}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\beta\in \mathrm{Hom}(B^{\otimes 2},k^\times)\\ \text{such that}\\ \beta(x,\,x)=q(x),\ x\in B\end{array}\right\}. \tag{66}$$

We need to prove that (66) is a bijection.

Let $\gamma_1,\,\gamma_2$ be 2-cochains on B such that $d(\gamma_1)=d(\gamma_2)=\omega$ and such that

$$c(x,\,y)\frac{\gamma_1(x,\,y)}{\gamma_1(y,\,x)}=c(x,\,y)\frac{\gamma_2(x,\,y)}{\gamma_2(y,\,x)},\quad x,\,y\in B.$$

Then γ_2/γ_1 is a symmetric 2-cocycle on B. Since a symmetric 2-cocycle is cohomologically trivial, γ_1 and γ_2 differ by a coboundary. Thus the map (66) is injective.

Consider the diagram

$$\begin{array}{ccccc} & & H^3_{ab}(A,k^\times) & \longrightarrow & H^3(A,k^\times)\\ & & \downarrow{\scriptstyle \mathrm{res}_B} & & \downarrow{\scriptstyle \mathrm{res}_B}\\ \mathrm{Hom}(B^{\otimes 2},k^\times) & \longrightarrow & H^3_{ab}(B,k^\times) & \longrightarrow & H^3(B,k^\times)\end{array} \tag{67}$$

with commutative square and the bottom row exact in the middle term. (Abelian cohomology groups were defined in Example 2.2.) Let q be a quadratic form on A, identified with an element of $H^3_{ab}(A,k^\times)$. It follows from diagram (67) that q is in the kernel of the composition

$$H^3_{ab}(A,k^\times)\to H^3(A,k^\times)\to H^3(B,k^\times)$$

if and only if the restriction of q to B can be represented by some bimultiplicative $\beta : B^{\otimes 2}\to k^\times$. This proves surjectivity of (66). □

Remark 5.3. Note that the condition (65) along with identity (12) imply

$$\beta(x,\,y)\beta(y,\,x)=\sigma(x,\,y),\quad x,\,y\in B. \tag{68}$$

By $\mathcal{M}(B,\,\beta)$ we will denote a module category corresponding to the pair $(B,\,\beta)$ under the bijection from Corollary 5.2.

The following lemma is a special case of the result proved in [Naidu 2007]:

Lemma 5.4. *Let $\mathcal{M} = \mathcal{M}(B, \beta)$ be a $\mathcal{C}(A, q)$-module category. Then the group $\mathrm{Aut}_{\mathcal{C}}(\mathcal{M})$ of isomorphism classes of $\mathcal{C}$-module autoequivalences of $\mathcal{M}$ fits into a short exact sequence*:

$$1 \longrightarrow \hat{B} \longrightarrow \mathrm{Aut}_{\mathcal{C}}(\mathcal{M}) \longrightarrow A/B \longrightarrow 1$$

Proof. The homomorphism $\mathrm{Aut}_{\mathcal{C}}(\mathcal{M}) \to A/B$ assigns the effect of a $\mathcal{C}$-equivalence on the set A/B of simple objects of $\mathcal{M}$. It is clear that this homomorphism is surjective (it is enough to look at the images of α-inductions).

The kernel of the homomorphism $\mathrm{Aut}_{\mathcal{C}}(\mathcal{M}) \to A/B$ consists of isomorphism classes of $\mathcal{C}$-equivalences isomorphic to the identity functor. With a choice of simple object $m \in \mathcal{M}$ a $\mathcal{C}$-module structure on the identity functor on $\mathcal{M}$ gives rise to a character $\psi \in \hat{B}$

$$\psi(b)\mathrm{id}_m : m = b * m \to b * m = m.$$

It follows from Shapiro's lemma that the character determines the $\mathcal{C}$-module structure. □

Proposition 5.5. *The $\mathcal{C}(A, q)$-module category $\mathcal{M}(B, \beta)$ is invertible if and only if the form $\beta : B \times B \to k^{\times}$ is nondegenerate.*

Proof. Note that $\mathcal{M} = \mathcal{M}(B, \beta)$ is invertible if and only if the α-inductions

$$\alpha^{\pm}_{\mathcal{M}} : \mathcal{C} \to \mathrm{End}_{\mathcal{C}}(\mathcal{M})$$

from Section 2I induce isomorphisms of groups $A \to \mathrm{Aut}_{\mathcal{C}}(\mathcal{M})$ on the level of isomorphism classes of objects. We can see that α-inductions give morphisms of short exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B & \longrightarrow & A & \longrightarrow & A/B & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \alpha^{\pm}_{\mathcal{M}}} & & \| & & \\
0 & \longrightarrow & \hat{B} & \longrightarrow & \mathrm{Aut}_{\mathcal{C}}(\mathcal{M}) & \longrightarrow & A/B & \longrightarrow & 0.
\end{array}$$

The homomorphisms $B \to \hat{B}$ can be recovered from the $\mathcal{C}$-module functor structures of $\alpha^{\pm}_{\mathcal{M}}(a)$ for $a \in A$. The $\mathcal{C}$-module functor structure for $\alpha^{+}_{\mathcal{M}}(a)$ is given by the diagram

$$\begin{array}{ccc}
a(bm) & \xrightarrow{\alpha^{+}_{\mathcal{M}}(a)_{b,m}} & b(am) \\
{\scriptstyle \gamma(a,b)}\downarrow & & \downarrow{\scriptstyle \gamma(b,a)} \\
(ab)m & \xrightarrow{c(a,b)} & (ba)m
\end{array}$$

so that $\alpha^{+}_{\mathcal{M}}(a)_{b,m} = \beta(a, b)$ for $a, b \in B$. Here m is a simple object of $\mathcal{M}$. Thus, the corresponding homomorphism $B \to \hat{B}$ has the form $b \to \beta(b, -)$.

Similarly, the $\mathcal{C}$-structure for $\alpha^-_{\mathcal{M}}(a)$ is defined by

$$\begin{array}{ccc} a(bm) & \xrightarrow{\alpha^-_{\mathcal{M}}(a)_{b,m}} & b(am) \\ {\scriptstyle \gamma(a,b)}\downarrow & & \downarrow{\scriptstyle \gamma(b,a)} \\ (ab)m & \xrightarrow{c(b,a)^{-1}} & (ba)m. \end{array}$$

Hence, $\alpha^-_{\mathcal{M}}(a)_{b,m} = \beta(b,a)^{-1}$ for $a, b \in B$ and the corresponding homomorphism $B \to \hat{B}$ has a form $b \to \beta(-,b)^{-1}$. □

From the proof of Proposition 5.5 we have the following:

Corollary 5.6. *The homomorphism $\partial : \mathrm{Pic}(\mathcal{C}(A,q)) \to \mathrm{Aut}^{\mathrm{br}}(A,q)$ sends the class of $\mathcal{M}(B,\beta)$ into the unique automorphism $g \in O(A,q)$ such that*

- $g(B) \subset B$,
- *g induces the identity on A/B, and*
- $\beta(b, g(c)) = \beta(c,b)^{-1}$ *for all* $b, c \in B$.

Remark 5.7. It follows from (68) that the last condition in Corollary 5.6 can be written as $\beta(b, g(c) - c) = \sigma(b,c)^{-1}$ for all $b, c \in B$. This gives an alternative description of g (compare [Davydov et al. 2011]; the graph of $-g$ is the Lagrangian subgroup $\Gamma(B,\beta) \subset (A \oplus A, q \oplus q^{-1})$ there):

- $g(a) - a \in B$ for any $a \in A$ and
- $\beta(b, g(a) - a) = \sigma(b,a)^{-1}$ for all $b \in B$.

In accordance with the crossed module axiom (36) the map

$$\partial : \mathrm{Pic}(\mathcal{C}(A,q)) \to O(A,q)$$

is $O(A,q)$-equivariant: $\partial(h(B,\beta)) = h \circ \partial(B,\beta) \circ h^{-1}$ for $h \in O(A,q)$. Here $h(B,\beta) = (h(B), h(\beta))$ with $h(\beta)(a,b) = \beta(h^{-1}(a), h^{-1}(b))$ and ${}^h\mathcal{M}(B,\beta) \simeq \mathcal{M}(h(B,\beta))$.

This gives a description of the map ∂ for the Picard crossed module $\mathfrak{P}(\mathcal{C}(A,q))$. The part which is unclear in this presentation is the group structure of $\mathrm{Pic}(\mathcal{C}(A,q))$. It appears that the group operation is more accessible on the level of the autoequivalence crossed module $\mathfrak{A}(\mathcal{C}(A,q))$ (recall that $\mathfrak{A}(\mathcal{C}(A,q)) \simeq \mathfrak{P}(\mathcal{C}(A,q))$ by Corollary 4.9). In the remaining sections we compute this crossed module.

5B. ***The center of a pointed braided fusion category.*** Let $\mathcal{C} = \mathcal{C}(A,q)$ be a pointed braided fusion category. The following fact is no doubt known to experts but we were unable to locate a reference in the literature:

Proposition 5.8. *The center $\mathcal{Z}(\mathcal{C})$ is pointed and $\mathcal{Z}(\mathcal{C}) \simeq \mathcal{C}(A \oplus \hat{A}, Q)$, where*

$$Q(a,\phi) = \langle \phi, a \rangle q(a). \tag{69}$$

Proof. For any $a \in A$ and $\phi \in \hat{A}$ there is an invertible object $Z_{a,\phi}$ in $\mathcal{Z}(\mathcal{C})$ which is equal to a as an object of $\mathcal{C}$ and has a half-braiding given by

$$c(x,a)\langle \phi, x\rangle \mathrm{id}_{a+x} : x \otimes Z_{a,\phi} \xrightarrow{\simeq} Z_{a,\phi} \otimes x, \tag{70}$$

where $c : A^{\times 2} \to k^\times$ is the function (6) determining the braiding of $\mathcal{C}$. That the morphism (70) is indeed a central structure on a (that is, satisfies necessary coherence conditions) follows from identities (7) and (8).

Thus, $\mathcal{Z}(\mathcal{C})$ contains $|A|^2$ nonisomorphic invertible simple objects. Since the dimension of $\mathcal{Z}(\mathcal{C})$ is $\dim(\mathcal{C})^2 = |A|^2$, the category $\mathcal{Z}(\mathcal{C})$ is pointed. Furthermore, $Z_{a,\phi} \otimes Z_{a',\phi'} = Z_{aa',\phi\phi'}$, $a, a' \in A$, $\phi, \phi' \in \hat{A}$, that is, the group of invertible objects of $\mathcal{Z}(\mathcal{C})$ is $A \oplus \hat{A}$. Finally, from (70) we see that the braiding on $Z_{a,\phi} \otimes Z_{a,\phi}$ is given by the scalar $\langle \phi, a\rangle q(a)$. □

Remark 5.9. Let

$$\sigma(a,b) := \frac{q(a+b)}{q(a)q(b)}, \quad x, y \in A \tag{71}$$

be the bimultiplicative form corresponding to the quadratic form $q : A \to k^\times$. Then the bimultiplicative form corresponding to the form Q defined in (69) is

$$\begin{aligned} B((a,\phi),(a',\phi')) &= \frac{Q(a+a',\phi+\phi')}{Q(a,\phi)Q(a',\phi')} \\ &= \langle \phi', a\rangle\langle \phi, a'\rangle \sigma(a,a'), \quad a, a' \in A, \phi, \phi' \in \hat{A}. \end{aligned}$$

Remark 5.10. Note that in general the category $\mathcal{Z}(\mathrm{Vec}_A^\omega)$, where A is an abelian group and $\omega \in Z^3(A, k^\times)$, is not pointed, see [Goff et al. 2007].

Let $\sigma : A \times A \to k^\times$ be the symmetric bimultiplicative form (71). For any $a \in A$ define a homomorphism $\tilde{\sigma} : A \to \hat{A}$ by

$$\langle \tilde{\sigma}(a), x\rangle = \sigma(a,x) \quad \text{for all } x \in A.$$

The embeddings $\mathcal{C}(A,q), \mathcal{C}(A,q)^{\mathrm{rev}} \hookrightarrow \mathcal{Z}(\mathcal{C}(A,q))$ defined in (4) are given by injective orthogonal homomorphisms

$$\begin{aligned} (A,q) &\to (A \oplus \hat{A}, Q) : a \mapsto (a,0), \\ (A,q^{-1}) &\to (A \oplus \hat{A}, Q) : a \mapsto (a, -\tilde{\sigma}(a)). \end{aligned}$$

5C. ***The Picard group of*** $\mathcal{C}(A,q)$**.** By Theorem 4.3 any invertible $\mathcal{C}(A,q)$-module category corresponds to an orthogonal automorphism $\alpha \in O(A \oplus \hat{A}, Q)$ such that $\alpha(a,0) = (a,0)$ for all $a \in A$.

Proposition 5.11. *Let $f : \hat{A} \to A$ be a group homomorphism satisfying the following conditions*:

(i) $\mathrm{id}_{\hat{A}} - \tilde{\sigma} f$ *is invertible*;

(ii) $\langle \phi, f(\phi)\rangle = q(f(\phi))$ *for all* $\phi \in \hat{A}$.

Then the map

$$\alpha_f(a,\phi) = \big(a + f(\phi), \phi - \tilde{\sigma} f(\phi)\big), \quad a \in A, \phi \in \hat{A} \tag{72}$$

is an orthogonal automorphism of $(A \oplus \hat{A}, Q)$ *that restricts to the identity on* A.

Conversely, any orthogonal automorphism with this property is of the form (72) *for a unique homomorphism* $f : \hat{A} \to A$ *satisfying conditions* (*i*) *and* (*ii*).

Proof. Suppose a group homomorphism $f : \hat{A} \to A$ is given. Clearly, α_f is a homomorphism and its restriction to A is the identity. Condition (i) in the statement of the proposition is equivalent to α_f being invertible. Let us explore the property of α_f being orthogonal. We compute

$$\begin{aligned} Q(\alpha_f(a,\phi)) &= Q\big(a + f(\phi), \phi - \tilde{\sigma} f(\phi)\big) \\ &= Q(a,\phi) Q\big(f(\phi), -\tilde{\sigma} f(\phi)\big) B\big((a,\phi), (f(\phi), -\tilde{\sigma} f(\phi))\big) \\ &= Q(a,\phi)\sigma\big(f(\phi), f(\phi)\big)^{-1} q(f(\phi))\langle \phi, f(\phi)\rangle \\ &= Q(a,\phi) q(f(\phi))^{-1}\langle \phi, f(\phi)\rangle, \end{aligned}$$

whence α_f is orthogonal if and only if condition (ii) is satisfied.

Let us prove the converse statement. Let $\alpha \in O(A \oplus \hat{A}, Q)$ be such that α restricts to the identity on A. Let $f : \hat{A} \to A$ and $g : \hat{A} \to \hat{A}$ be homomorphisms such that $\alpha(0,\phi) = (f(\phi), g(\phi))$ for all $\phi \in \hat{A}$. Since α preserves the quadratic form Q, the condition $Q(0,\phi) = 1$ implies $Q(f(\phi), g(\phi)) = 1$, which is equivalent to

$$\langle g(\phi), f(\phi)\rangle q(f(\phi)) = 1. \tag{73}$$

Next, for arbitrary $a \in A$ and $\phi \in \hat{A}$ we have

$$\alpha(a,\phi) = (a + f(\phi), g(\phi)). \tag{74}$$

We have $Q(\alpha(a,\phi)) = Q(a,\phi) = \langle \phi, a\rangle q(a)$. On the other hand, we compute

$$\begin{aligned} Q(\alpha(a,\phi)) &= Q\big(a + f(\phi), g(\phi)\big) \\ &= Q(a,1) Q\big(f(\phi), g(\phi)\big)\langle g(\phi), a\rangle \sigma(a, f(\phi)) \\ &= q(a)\langle g(\phi), a\rangle \sigma(f(\phi), a) \\ &= q(a)\langle g(\phi) + \tilde{\sigma} f(\phi), a\rangle. \end{aligned}$$

Comparing two expressions we obtain

$$g(\phi) = \phi - \tilde{\sigma} f(\phi) \quad \text{for all } \phi \in \hat{A}. \tag{75}$$

This along with (74) yields (72).

Substituting (75) into (73) we obtain

$$\langle \phi, f(\phi)\rangle q(f(\phi)) = \langle \tilde{\sigma} f(\phi), f(\phi)\rangle = \sigma(f(\phi), f(\phi)) = q(f(\phi))^2,$$

whence $\langle \phi, f(\phi)\rangle = q(f(\phi))$ as required. □

Let $P(A, q)$ be the set of group homomorphisms $f : \hat{A} \to A$ satisfying conditions (i) and (ii) of Proposition 5.11, that is,

$$P(A,\ q) := \left\{ \begin{array}{c} \text{homomorphisms } f : \hat{A} \to A \text{ such that} \\ \mathrm{id}_{\hat{A}} - \tilde{\sigma} \circ f \text{ is invertible and} \\ \langle \phi,\ f(\phi)\rangle = q(f(\phi)) \text{ for all } \phi \in \hat{A} \end{array} \right\}. \tag{76}$$

Endow the set $P(A, q)$ with the binary operation

$$f \diamond g = f + g - f \circ \tilde{\sigma} \circ g, \quad f, g \in P(A, q). \tag{77}$$

Proposition 5.12. *The set $P(A, q)$ with the operation $\diamond$ defined in (77) is a group. Furthermore, the map*

$$f \mapsto \alpha_f : P(A, q) \to \mathrm{Aut}^{\mathrm{br}}\big(\mathfrak{Z}(\mathcal{C}(A, q)), \mathcal{C}(A, q)\big), \tag{78}$$

where $\alpha_f \in \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C}(A, q)))$ is defined in (72), is a group isomorphism.

Proof. By Proposition 5.11 the assignment (78) is a bijection. Since

$$\alpha_f \circ \alpha_g = \alpha_{f \diamond g} \quad \text{for all } f, g \in P(A, q),$$

we see that $P(A, q)$ is a group and the assignment (78) is a group isomorphism. □

Remark 5.13. Clearly, the identity element of $P(A, q)$ is the zero homomorphism. Let us describe the inverse of $f \in P(A, q)$.

It is immediate from (77) that the inverse of f is given by the formula

$$f^{-1} = (f \circ \tilde{\sigma} - \mathrm{id}_A)^{-1} \circ f. \tag{79}$$

Let $f^* : \hat{A} \to A$ denote the homomorphism dual to f. We claim that $f^* \in P(A, q)$ and that f^* is the inverse of f with respect to the multiplication $\diamond$. Indeed, equality of quadratic forms in condition (ii) of Proposition 5.11 implies equality of the corresponding bilinear forms

$$\langle f + f^*(\phi), \psi\rangle = \sigma(f(\phi), f(\psi)), \quad \phi, \psi \in \hat{A},$$

whence $f + f^* = f^* \circ \tilde{\sigma} \circ f$, that is, f^* coincides with the right hand side of (79).

Corollary 5.14. *There is a group isomorphism $P(A, q) \cong \mathrm{Pic}(\mathcal{C}(A, q))$.*

Proof. This follows from Proposition 5.12 and Theorem 4.3. □

Remark 5.15. We have two parametrizations for the group $\mathrm{Pic}(\mathcal{C}(A,q))$. The first one is given in terms of pairs (B,β), where $B\subset A$ is a subgroup and $\beta: B\times B\to k^\times$ is a nondegenerate bimultiplicative map such that $\beta(x,x)=q(x)$ for all $x\in B$, see Corollary 5.2 and Proposition 5.5. The second one is given in terms of the set $P(A,q)$ consisting of homomorphisms $f:\hat{A}\to A$ satisfying conditions listed in (76).

Let us establish a bijection between these parametrizations. Let $\mathcal{M}=\mathcal{M}(B,\beta)$ denote the invertible $\mathcal{C}(A,q)$-module category corresponding to a pair (B,β) as above. Let $\Phi(\mathcal{M})$ denote the corresponding braided autoequivalence of $\mathcal{Z}(\mathcal{C}(A,q)$ defined as in (44). By Proposition 5.11 $\Phi(\mathcal{M})=\alpha_f$ for a unique $f\in P(A,q)$. Let $\phi\in\hat{A}$ and let $b=f(\phi)$. Then b is uniquely determined by the condition

$$\Phi(\mathcal{M})(Z_{0,\phi})=Z_{b,\psi}\quad \text{for some } \psi\in\hat{A}.$$

Equivalently,

$$a_{\mathcal{M}}(Z_{0,\phi})=b_{\mathcal{M}}(Z_{b,\psi}),$$

where $a_{\mathcal{M}}$ and $b_{\mathcal{M}}$ are functors defined in (37) and (41). Note that $b\in B$ since the functor $a_{\mathcal{M}}(Z_{0,\phi})$ is identical on the classes of isomorphic objects of $\mathcal{M}$.

Take $x\in B$ and compare isomorphisms

$$x\otimes a_{\mathcal{M}}(Z_{0,\phi})(?)\xrightarrow{\simeq} a_{\mathcal{M}}(Z_{0,\phi})(x\otimes ?) \tag{80}$$

and

$$x\otimes b_{\mathcal{M}}(Z_{b,\psi})(?)\xrightarrow{\simeq} b_{\mathcal{M}}(Z_{b,\psi})(x\otimes ?) \tag{81}$$

coming from left $\mathcal{C}(A,q)$-module functor structures of $a_{\mathcal{M}}(Z_{0,\phi})$ and $b_{\mathcal{M}}(Z_{0,\phi})$.

Using Equations (50) and (70) we see that the isomorphism (80) is given by

$$x\otimes(Z_{0,\phi}\otimes ?)\xrightarrow{\langle\phi,x\rangle} Z_{0,\phi}\otimes(x\otimes ?). \tag{82}$$

On the other hand, using (52) we see that the isomorphism (81) is given by

$$\begin{aligned} x\otimes(Z_{b,\psi}\otimes ?)&\xrightarrow{\gamma(x,b)}(x\otimes Z_{b,\psi})\otimes ?\\ &\xrightarrow{c(x,b)}(Z_{b,\psi}\otimes x)\otimes ?\xrightarrow{\gamma(b,x)^{-1}} Z_{b,\psi}\otimes(x\otimes ?), \end{aligned} \tag{83}$$

where $\gamma: B\times B\to k^\times$ is the function that determines the module associativity of $\mathcal{M}(B,\beta)$ — see (63) — and $c: A\times A\to k^\times$ is the braiding of $\mathcal{C}(A,q)$. From (64) we see that the product of scalars in the composition (83) is equal to $\beta(x,b)$. Since β is nondegenerate it follows that $b=f(\phi)$ is completely determined by the condition

$$\langle\phi,x\rangle=\beta(x,b).$$

Thus, the homomorphism $f : \hat{A} \to A$ corresponding to (B, β) is given by the composition

$$f : \hat{A} \to \hat{B} \xrightarrow{\hat{\beta}} B \hookrightarrow A, \tag{84}$$

where $\hat{A} \to \hat{B}$ is the surjection dual to the embedding $B \hookrightarrow A$ and $\hat{\beta} : \hat{B} \xrightarrow{\sim} B$ is the isomorphism induced by β.

Example 5.16. (i) Suppose q is nondegenerate (that is, the category $\mathcal{C}(A, q)$ is nondegenerate). Then $\tilde{\sigma} : A \to \hat{A}$ is an isomorphism and the map

$$P(A, q) \to O(A, q) \quad \text{given by} \quad f \mapsto \mathrm{id}_A - f \circ \tilde{\sigma}$$

is an isomorphism.

(ii) Suppose $q = 1$ (that is, the category $\mathcal{C}(A, q)$ is tannakian). Then

$$P(A, q) = \{\phi : \hat{A} \to A \mid \langle \phi, f(\phi) \rangle = 1\}.$$

Thus, elements of $P(A, q)$ are identified with alternating bimultiplicative maps $\hat{A} \times \hat{A} \to k^\times$ and

$$P(A, q) \cong \bigwedge\nolimits^2 A \cong H^2(\hat{A}, k^\times);$$

see [Etingof et al. 2010, Corollary 3.17].

(iii) Suppose that $\sigma = 1$ but $q \neq 1$ (that is, the category $\mathcal{C}(A, q)$ is symmetric but not tannakian). In this case $q \in \hat{A}$ is a character of order 2. Let $\langle q \rangle$ denote the subgroup of $\hat{A}$ generated by q. We have

$$P(A, q) \cong \begin{cases} H^2(\hat{A}, k^\times) & \text{if } \langle q \rangle \text{ is a direct summand in } \hat{A}, \\ H^2(\hat{A}, k^\times) \times \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

This agrees with the result of [Carnovale 2006] in the case of semisimple Hopf algebras.

5D. ***Description of the Picard crossed module of*** $\mathcal{C}(A, q)$**.** Let $\mathcal{C}(A, q)$ be a pointed braided fusion category. By Corollary 4.9 the Picard crossed module of $\mathcal{C}$ is isomorphic to the autoequivalence crossed module

$$\mathfrak{A}(\mathcal{C}(A, q)) = \big(\mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C}(A, q)); \mathcal{C}(A, q)), \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}(A, q))\big) \cong \big(P(A, q), O(A, q)\big)$$

introduced in Section 3D.

By Lemma 4.4 the structural homomorphism

$$\partial : \mathrm{Pic}(\mathcal{C}(A, q)) \cong \mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C}(A, q)); \mathcal{C}(A, q)) \to \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}(A, q)) \tag{85}$$

is given by restriction of the autoequivalences in $\mathrm{Aut}^{\mathrm{br}}(\mathfrak{Z}(\mathcal{C}(A, q)); \mathcal{C}(A, q))$ to $\mathcal{C}(A, q)^{\mathrm{rev}} \subset \mathfrak{Z}(\mathcal{C}(A, q))$.

Let us describe ∂ explicitly. We already observed that the tensor subcategory $\mathcal{C}(A,q)^{\mathrm{rev}} \subset \mathcal{Z}(\mathcal{C}(A,q))$ corresponds to the subgroup $\{(a,-\hat{a}) \mid a \in A\} \subset A \oplus \hat{A}$. Given $f \in P(A,q)$ we have

$$\alpha_f(a, -\tilde{\sigma}(a)) = (a - f\tilde{\sigma}(a), -(\tilde{\sigma}(a) - \tilde{\sigma} f \tilde{\sigma}(a)).$$

Hence,

$$\partial(f) = \mathrm{id}_A - f \circ \tilde{\sigma}, \quad f \in P(A,q). \tag{86}$$

Next, for any $g \in O(A,q)$ let $\tilde{g} \in O(A \oplus \hat{A}, Q)$ be the orthogonal automorphism induced by g, that is, $\tilde{g}(a,\phi) = (g(a), \phi \circ g^{-1})$. It is straightforward to check the identity

$$\tilde{g} \circ \alpha_f \circ \tilde{g}^{-1} = \alpha_{({}^g f)},$$

where

$${}^g f = g \circ f \circ g^{-1}, \quad g \in O(A,q),\ f \in P(A,q). \tag{87}$$

Thus, the autoequivalence crossed module of $\mathcal{C}(A,q)$ is

$$\mathfrak{A}(\mathcal{C}(A,q)) \simeq (P(A,q), O(A,q))$$

with structural operations (86) and (87).

5E. ***Invariants of*** $\mathfrak{P}(\mathcal{C}(A,q))$**.** The kernel and the cokernel of the homomorphism ∂ are important invariants of a crossed module. Below, we compute the kernel of ∂ for the crossed module $\mathfrak{P}(\mathcal{C}(A,q))$. We also describe the cokernel of ∂ for the crossed module $\mathfrak{P}(\mathcal{C}(A,q))$ when $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C}(A,q))$ is tannakian.

As before, let $A^\perp \subset A$ denote the kernel of σ. Note that $\mathcal{C}(A^\perp, q|_{A^\perp}) = \mathcal{Z}_{\mathrm{sym}}(\mathcal{C}(A,q))$ is a symmetric fusion category.

Proposition 5.17. *The group homomorphism* (61)

$$j : \mathrm{Pic}(\mathcal{C}(A^\perp, q|_{A^\perp})) \to \ker(\partial)$$

is an isomorphism.

Proof. The homomorphism j can be explicitly described as follows. For g in $P(A^\perp, q|_{A^\perp})$ the image $j(g) \in P(A,q)$ is the composition

$$j(g) : \hat{A} \to \widehat{A^\perp} \xrightarrow{g} A^\perp \hookrightarrow A,$$

where the first arrow is the restriction of a character and the last arrow is the embedding.

We will construct the inverse homomorphisms

$$i : \mathrm{Ker}(\partial) \to \mathrm{Pic}(\mathcal{C}(A^\perp, q|_{A^\perp}))$$

to j. Let $f \in \mathrm{Ker}(\partial)$. Then $f \circ \tilde{\sigma} = 0$; that is, $f|_{\widehat{A/A^\perp}} = 0$. By Remark 5.13 we also have $f^* \in \mathrm{Ker}(\partial)$, and hence $f^* \circ \tilde{\sigma} = 0$. Taking the dual we get $\tilde{\sigma} \circ f = 0$, that is, $f(\hat{A}) \subset A^\perp$. Hence f descends to a homomorphism

$$i(f) : \widehat{A^\perp} \cong \hat{A}/(\widehat{A/A^\perp}) \to A^\perp,$$

which is easily seen to be in $P(A^\perp, q|_{A^\perp})$. □

Now let $\mathcal{C}(A, q))$ be a pointed category whose symmetric center $\mathcal{Z}_{\mathrm{sym}}(\mathcal{C}(A, q))$ is tannakian. In other words let $q|_{A^\perp} = 1$. Note that in this case the form q descends to $A/A^\perp$ (we denote the descendent form by $\tilde{q}$). Below, we describe the kernel of the homomorphism (62) for $\mathcal{C}(A, q)$.

Proposition 5.18. *Let $q|_{A^\perp} = 1$. Then the kernel of the canonical homomorphism (62)*

$$\mathrm{coker}\big(\mathrm{Pic}(\mathcal{C}(A, q)) \xrightarrow{\partial} \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}(A, q))\big) \to \mathrm{Aut}(A^\perp)$$

is isomorphic to the abelian group $\mathrm{Hom}(A/A^\perp, A^\perp)$. *In other words, the cokernel* $C = \mathrm{coker}\big(\mathrm{Pic}(\mathcal{C}(A, q)) \xrightarrow{\partial} \mathrm{Aut}^{\mathrm{br}}(\mathcal{C}(A, q))\big)$ *fits into an exact sequence*

$$0 \longrightarrow \mathrm{Hom}(A/A^\perp, A^\perp) \longrightarrow C \longrightarrow \mathrm{Aut}(A^\perp)\ . \tag{88}$$

Proof. From the commutativity of the diagram

$$\begin{array}{ccc} P(A, q) & \xrightarrow{\partial} & O(A, q) \\ \downarrow & & \downarrow \\ P(A/A^\perp, \tilde{q}) & \xrightarrow[\partial]{\simeq} & O(A/A^\perp, \tilde{q}) \end{array}$$

it follows that $\mathrm{coker}\big(P(A, q) \xrightarrow{\partial} O(A, q)\big)$ coincides with

$$\ker\big(O(A, q) \to O(A/A^\perp, \tilde{q})\big)/\mathrm{im}(\partial) \cap \ker\big(O(A, q) \to O(A/A^\perp, \tilde{q})\big).$$

Now $\ker\big(O(A, q) \to O(A/A^\perp, \tilde{q})\big)$ consists of automorphisms of the form $\mathrm{id}_A + \phi$ for $\phi \in \mathrm{Hom}(A, A^\perp)$. Indeed any element of $\ker\big(O(A, q) \to O(A/A^\perp, \tilde{q})\big)$ must have this form and conversely any automorphisms of this form preserves q:

$$q(a + \phi(a)) = q(a)q(\phi(a))\sigma(a, \phi(a)) = q(a).$$

Note that composition of automorphisms induces the following group operation on $\mathrm{Hom}(A, A^\perp)$:

$$\phi * \psi = \phi + \psi + \phi \circ \psi.$$

It is straightforward that $C = \{\phi \in \mathrm{Hom}(A, A^\perp) \mid \mathrm{id}_A + \phi \text{ is invertible}\}$ with the group operation $*$ fits into an exact sequence (88).

All we need to show now is that the intersection of $\mathrm{im}(\partial)$ with the kernel of $O(A,q) \to O(A/A^\perp, \tilde{q})$ is trivial. Assume that $\partial(f) = \mathrm{id}_A + \phi$ for ϕ in $\mathrm{Hom}(A, A^\perp)$. Then $\phi = -f \circ \tilde{\sigma}$ so that $\mathrm{im}(f) \subset A^\perp$. We also have $\partial(f^*) = \mathrm{id}_A + \psi$ for $\psi \in \mathrm{Hom}(A, A^\perp)$, which implies that $\mathrm{im}(f^*) \subset A^\perp$. Then

$$\phi = -f \circ \tilde{\sigma} = -(\tilde{\sigma} \circ f^*)^* = 0. \qquad \square$$

Acknowledgments

We are deeply grateful to V. Drinfeld. The statements of Theorems 3.10 and 4.3 are due to him. We also thank J. Cuadra, V. Ostrik and the anonymous referee for valuable comments.

References

[Bakalov and Kirillov 2001] B. Bakalov and A. Kirillov, Jr., *Lectures on tensor categories and modular functors*, University Lecture Series **21**, American Mathematical Society, Providence, RI, 2001. MR 2002d:18003 Zbl 0965.18002

[Böckenhauer et al. 2001] J. Böckenhauer, D. E. Evans, and Y. Kawahigashi, "Longo–Rehren subfactors arising from α-induction", *Publ. Res. Inst. Math. Sci.* **37**:1 (2001), 1–35. MR 2002d:46053 Zbl 1090.46047

[Carnovale 2006] G. Carnovale, "The Brauer group of modified supergroup algebras", *J. Algebra* **305**:2 (2006), 993–1036. MR 2008d:16055 Zbl 1135.16043

[Davydov et al. 2011] A. Davydov, L. Kong, and I. Runkel, "Invertible defects and isomorphisms of rational CFTs", *Adv. Theor. Math. Phys.* **15**:1 (2011), 43–69. MR 2888007 Zbl 1246.81319

[Davydov et al. 2013] A. Davydov, D. Nikshych, and V. Ostrik, "On the structure of the Witt group of braided fusion categories", *Selecta Math.* (*N.S.*) **19**:1 (2013), 237–269. MR 3022755

[Deligne 2002] P. Deligne, "Catégories tensorielles", *Mosc. Math. J.* **2**:2 (2002), 227–248. MR 2003k:18010 Zbl 1005.18009

[Drinfeld et al. 2010] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, "On braided fusion categories, I", *Selecta Math.* (*N.S.*) **16**:1 (2010), 1–119. MR 2011e:18015 Zbl 1201.18005

[Eilenberg and Mac Lane 1953] S. Eilenberg and S. Mac Lane, "On the groups $H(\Pi, n)$, I", *Ann. of Math.* (2) **58** (1953), 55–106. MR 15,54b Zbl 0050.39304

[Eilenberg and Mac Lane 1954] S. Eilenberg and S. Mac Lane, "On the groups $H(\Pi, n)$, II: Methods of computation", *Ann. of Math.* (2) **60** (1954), 49–139. MR 16,391a Zbl 0055.41704

[Etingof and Ostrik 2004] P. Etingof and V. Ostrik, "Finite tensor categories", *Mosc. Math. J.* **4**:3 (2004), 627–654. MR 2005j:18006 Zbl 1077.18005

[Etingof et al. 2010] P. Etingof, D. Nikshych, and V. Ostrik, "Fusion categories and homotopy theory", *Quantum Topol.* **1**:3 (2010), 209–273. MR 2011h:18007 Zbl 1214.18007

[Goff et al. 2007] C. Goff, G. Mason, and S.-H. Ng, "On the gauge equivalence of twisted quantum doubles of elementary abelian and extra-special 2-groups", *J. Algebra* **312**:2 (2007), 849–875. MR 2008d:16057 Zbl 1171.16021

[Janelidze and Kelly 2001] G. Janelidze and G. M. Kelly, "A note on actions of a monoidal category", *Theory Appl. Categ.* **9** (2001), 61–91. MR 2003f:18007 Zbl 1009.18005

[Joyal and Street 1993] A. Joyal and R. Street, "Braided tensor categories", *Adv. Math.* **102**:1 (1993), 20–78. MR 94m:18008 Zbl 0817.18007

[Müger 2003] M. Müger, "On the structure of modular categories", *Proc. London Math. Soc.* (3) **87**:2 (2003), 291–308. MR 2004g:18009 Zbl 1037.18005

[Naidu 2007] D. Naidu, "Categorical Morita equivalence for group-theoretical categories", *Comm. Algebra* **35**:11 (2007), 3544–3565. MR 2008j:18007 Zbl 1143.18009

[Ostrik 2003a] V. Ostrik, "Module categories over the Drinfeld double of a finite group", *Int. Math. Res. Not.* **2003**:27 (2003), 1507–1520. MR 2004h:18005 Zbl 1044.18005

[Ostrik 2003b] V. Ostrik, "Module categories, weak Hopf algebras and modular invariants", *Transform. Groups* **8**:2 (2003), 177–206. MR 2004h:18006 Zbl 1044.18004

[Quillen 1973] D. Quillen, "Higher algebraic K-theory, I", pp. 85–147 in *Algebraic K-theory, I: Higher K-theories* (Seattle, WA, 1972), edited by H. Bass, Lecture Notes in Math. **341**, Springer, Berlin, 1973. MR 49 #2895 Zbl 0292.18004

[Van Oystaeyen and Zhang 1998] F. Van Oystaeyen and Y. Zhang, "The Brauer group of a braided monoidal category", *J. Algebra* **202**:1 (1998), 96–128. MR 99c:18006 Zbl 0909.18005

Communicated by Susan Montgomery
Received 2012-02-06 Revised 2012-11-08 Accepted 2012-11-20

alexei1davydov@gmail.com *Department of Mathematics, Ohio University, Athens, OH 45701, United States*

nikshych@math.unh.edu *Department of Mathematics, University of New Hampshire, Durham, NH 03824, United States*

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1405

A Gross–Zagier formula for quaternion algebras over totally real fields

Eyal Z. Goren and Kristin E. Lauter

We prove a higher dimensional generalization of Gross and Zagier's theorem on the factorization of differences of singular moduli. Their result is proved by giving a counting formula for the number of isomorphisms between elliptic curves with complex multiplication by two different imaginary quadratic fields K and K' when the curves are reduced modulo a supersingular prime and its powers. Equivalently, the Gross–Zagier formula counts optimal embeddings of the ring of integers of an imaginary quadratic field into particular maximal orders in $B_{p,\infty}$, the definite quaternion algebra over $\mathbb{Q}$ ramified only at p and infinity. Our work gives an analogous counting formula for the number of simultaneous embeddings of the rings of integers of primitive CM fields into superspecial orders in definite quaternion algebras over totally real fields of strict class number 1. Our results can also be viewed as a counting formula for the number of isomorphisms modulo $\mathfrak{p} \mid p$ between abelian varieties with CM by different fields. Our counting formula can also be used to determine which superspecial primes appear in the factorizations of differences of values of Siegel modular functions at CM points associated to two different CM fields and to give a bound on those supersingular primes that can appear. In the special case of Jacobians of genus-2 curves, this provides information about the factorizations of numerators of Igusa invariants and so is also relevant to the problem of constructing genus-2 curves for use in cryptography.

1. Introduction

The celebrated theorem of Gross and Zagier [1985] gives a factorization of norms of differences of singular moduli: values of the modular j-function evaluated at CM points associated to imaginary quadratic fields. Let K and K' be two imaginary quadratic fields with relatively prime fundamental discriminants d and d'. For τ and τ' running through equivalence classes of imaginary quadratic integers in the upper half-plane modulo $\mathrm{SL}_2(\mathbb{Z})$ with $\mathrm{disc}(\tau) = d$, $\mathrm{disc}(\tau') = d'$, and w and w'

MSC2010: primary 11G15, 11G16; secondary 11G18, 11R27.
Keywords: CM abelian varieties, singular moduli, quaternion algebras, superspecial orders.

equal to the number of roots of unity in K and K', respectively, define

$$J(d,d') = \left(\prod_{[\tau],[\tau']} (j(\tau) - j(\tau')) \right)^{4/(ww')}.$$

Then the Gross–Zagier thereom states that if λ is a prime of $\mathbb{O}_K$ of characteristic p,

$$\operatorname{ord}_\lambda J(d,d') = \frac{1}{2} \sum_{x\in\mathbb{Z}} \sum_{n\geq 1} \delta(x) R\left(\frac{dd'-x^2}{4p^n} \right),$$

where $R(m)$ is the number of ideals of $\mathbb{O}_K$ of norm m and $\delta(x) = 1$ unless x is divisible by d, in which case it is 2. Their results can also be viewed as a counting formula for the number of isomorphisms between the reductions modulo primes and their powers of elliptic curves with complex multiplication by two different imaginary quadratic fields K and K'. This in turn is equivalent to counting optimal embeddings of the ring of integers of an imaginary quadratic field into particular maximal orders in $B_{p,\infty}$, the definite quaternion algebra over $\mathbb{Q}$ ramified only at p and infinity. Gross and Zagier gave an algebraic proof of this result under the additional assumption that d is prime, and the algebraic proof of the theorem was extended to arbitrary fundamental, relatively prime discriminants in a series of papers by Dorman [1988; 1989a; 1989b].

In this paper, we prove a generalization to higher dimensions of Gross and Zagier's theorem, which can also be viewed in three ways: (1) a statement about primes in the factorization of differences of values of Siegel modular functions at CM points associated to two different CM fields, (2) a counting formula for isomorphisms modulo p between abelian varieties with CM by different fields, and (3) a counting formula for simultaneous embeddings of the rings of integers of two primitive CM fields into superspecial orders in certain definite quaternion algebras over a totally real field.

First we explain our interest in these three contexts. Assume throughout that K and K' are primitive CM fields with a common totally real subfield $K^+ = K'^+ = L$ and $[L:\mathbb{Q}] = g$, where L has strict class number 1. In the special case of $g = 2$, we are inspired by some concrete calculations of values of certain Siegel modular functions at CM points associated to primitive quartic CM fields. Let C and C' be two genus-2 curves whose Jacobians J and J' have complex multiplication (CM) by K and K'. In analogy with the modular j-invariant for elliptic curves, for genus-2 curves Igusa defined ten modular invariants. Equality of these ten invariants determines whether two curves are isomorphic geometrically, so primes appearing in the factorization of all ten differences correspond to primes where the curves become isomorphic when reduced modulo that prime. Concrete calculations and the tables of van Wamelen [1999] suggest that such primes are "small". An explicit

characterization of such primes gives information about the numerators of Igusa invariants and thus has some value computationally as well.

Thus, we are led to be interested in counting the number of isomorphisms modulo various primes and their powers between abelian varieties with CM by two different CM fields K and K'. The existence of an isomorphism modulo p between abelian varieties with CM by two different CM fields K and K' with $K^+ = K'^+$ implies supersingular reduction modulo p. Fixing an abelian variety A with CM by K, each isomorphism modulo p with an abelian variety A' with CM by K' gives an embedding of $\mathcal{O}_{K'}$ into $\mathrm{End}_{\mathcal{O}_L}(A)$. In the case of superspecial reduction, we can give a very explicit description of the orders $\mathrm{End}_{\mathcal{O}_L}(A)$, which allows us to derive a formula that counts such embeddings.

Nicole introduced the notion of superspecial orders in definite quaternion algebras over totally real fields as a generalization of maximal orders in definite quaternion algebras over $\mathbb{Q}$; see [Nicole 2005; 2008]. These orders were further studied in [Charles et al. 2009a; 2009b; Goren and Lauter 2009], where related Ramanujan graphs were constructed and certain cryptographic applications suggested. Throughout this paper, assume that p is a prime number that is unramified in the totally real field L of degree g and strict class number $h^+(L) = 1$. Under these assumptions, a *superspecial order* in $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$ is an Eichler order of level p. The connection with geometry is given in the thesis of Nicole, where it is shown that $\mathrm{End}_{\mathcal{O}_L}(A)$ is a superspecial order for A a principally polarized superspecial abelian variety with RM over $\bar{\mathbb{F}}_p$. Conversely, every superspecial order arises in this way from such an abelian variety A.

Next we give an overview of the results of the paper. The core of the paper is the generalization of Dorman's work constructing and classifying superspecial orders in $B_{p,L}$ with an optimal embedding of a CM number field K with $K^+ = L$. First, Section 3 is devoted to giving a description of the quaternion algebra $B_{p,L}$ with a fixed embedding of the CM field K for *superspecial primes*, i.e., unramified primes p such that an abelian variety with CM by K has superspecial reduction modulo a prime $\mathfrak{P} \mid p$ in a field of definition of the abelian variety. Sections 4 and 5 establish a classification of superspecial orders with an optimal embedding of K, giving both an explicit construction of all such superspecial orders and a bijection (up to conjugation by elements of $K^\times$) with the class group of K (Theorem 5.7). These three sections together establish the generalization to $g > 1$ of Dorman's work on orders [1989a] and fix several gaps in his proofs.

Section 6 gives a method for counting embeddings by counting elements of the superspecial orders with a prescribed trace and norm in a way that generalizes the Gross–Zagier formula. Our method is very similar to Gross–Zagier's and Dorman's; their results are the special case $g = 1$. To make the link between the algebraic and the geometric sides of the story, we include the determination of endomorphism

rings of superspecial abelian varieties in Section 7. Section 8 connects the counting formula for isomorphisms between CM abelian varieties with the counting formula for embeddings into superspecial orders.

The main result of the paper is an explicitly computable counting formula for the number of isomorphisms modulo $\mathfrak{P} \mid p$ between abelian varieties with CM by two different CM fields K and K' with $K^+ = K'^+$ (Theorems 6.5 and 8.2). This formula can be viewed as an intersection number under the assumption that a reasonable lemma in intersection theory holds (Section 9). Less precisely, we refer to this value as a "coincidence number". It also has an algebraic interpretation as the number of "optimal triples" of embeddings of $\mathbb{O}_K$ and $\mathbb{O}_{K'}$ into superspecial orders (Section 8.4).

For primes of supersingular reduction for CM abelian varieties, a separate computation of the endomorphism rings is given in Section 10. In Section 11, a volume argument such as was used in [Goren and Lauter 2007] is given to establish a bound on primes p of either supersingular or superspecial reduction, where isomorphisms exist modulo p between CM points associated to K and K'. In Section 12, an example of two Galois CM fields is given and all primes dividing the differences of the Igusa invariants are examined and compared with our counting formula.

The authors thank the referee for helpful comments to improve the paper.

2. Preliminaries

2.1. ***Quadratic reciprocity for number fields.*** Let L be a number field and γ and δ prime elements of L that are nonassociates such that $(\gamma\delta, 2) = 1$. Define

$$\left(\frac{\gamma}{\delta}\right) = \begin{cases} 1 & \text{if } \gamma = \square \bmod \delta, \\ -1 & \text{else.} \end{cases}$$

Let $B := \left(\frac{\gamma,\delta}{L}\right)$ be the quaternion algebra over L defined by the elements γ and δ. For any place η of L, including the infinite places, define

$$(\gamma, \delta)_\eta := \begin{cases} 1 & \text{if } B \otimes_L L_\eta \text{ is split,} \\ -1 & \text{else,} \end{cases}$$

and we have the following analogue of quadratic reciprocity for the number field L:

Proposition 2.1. (1) *If η is a finite prime such that $\eta \nmid 2$, then $(\gamma, \delta)_\eta = 1$ if and only if $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution modulo η.*

(2) *If η is complex, then $(\gamma, \delta)_\eta = 1$.*

(3) *If η is real ($\eta : L \to \mathbb{R}$), then $(\gamma, \delta)_\eta = 1$ if and only if $\eta(\gamma) > 0$ or $\eta(\delta) > 0$. That is, $(\gamma, \delta)_\eta = -1$ if and only if both $\eta(\gamma)$ and $\eta(\delta)$ are negative.*

$$\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right) = (-1)^{r(\gamma,\delta)} \cdot \prod_{\eta|2} (\gamma, \delta)_\eta, \tag{4}$$

where $r(\gamma, \delta)$ equals the number of real places η such that both $\eta(\gamma)$ and $\eta(\delta)$ are negative. In particular, if either γ or δ are totally positive, then

$$\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right) = (\gamma, \delta)_2 := \prod_{\eta|2} (\gamma, \delta)_\eta.$$

$$\left(\frac{-1}{\gamma}\right)(-1, \gamma)_2 = (-1)^{r(\gamma)}, \tag{5}$$

where $r(\gamma)$ is the number of real places η such that $\eta(\gamma)$ is negative.

Proof. We prove (1). By [Vignéras 1980, Chapter II, Corollary 1.2], $(\gamma, \delta)_\eta = 1$ if and only if $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution in L_η, where by "nontrivial" we mean a solution where at least one of the variables with nonzero coefficients is nonzero. Suppose that $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution in L_η. By multiplying by a common denominator, we can assume $x, y, z \in \mathbb{O}_{L_\eta}$ and one of them is a unit. Then reducing modulo η, we get a nontrivial solution to $x^2 - \gamma y^2 - \delta z^2 \equiv 0 \bmod \eta$. Conversely, suppose $x^2 - \gamma y^2 - \delta z^2 \equiv 0 \bmod \eta$ has a nontrivial solution. By Hensel's lemma, we can lift the solution to $\mathbb{O}_{L_\eta}$.

Part (2) is clear, and (3) follows from loc. cit. because $x^2 - \eta(\gamma) y^2 - \eta(\delta) z^2 = 0$ has a nontrivial solution in $\mathbb{R}^3$ if and only if either $\eta(\gamma) > 0$ or $\eta(\delta) > 0$.

To prove (4), first note that $(\gamma, \delta)_\gamma = 1$ if and only if $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution modulo γ if and only if $\delta = (x/z)^2$ for some nonzero $x, z \in \mathbb{O}_L/(\gamma)$ if and only if $\left(\frac{\delta}{\gamma}\right) = 1$. By the product formula,

$$1 = \prod_\eta (\gamma, \delta)_\eta = (-1)^{r(\gamma,\delta)} (\gamma, \delta)_2 \left(\frac{\delta}{\gamma}\right)\left(\frac{\gamma}{\delta}\right) \prod_{\substack{\eta \text{ finite} \\ \eta \nmid 2\gamma\delta}} (\gamma, \delta)_\eta.$$

But for $\eta \nmid 2\gamma\delta$, $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution modulo η, so $(\gamma, \delta)_\eta = 1$.

Similarly for (5), for any real place η, $\eta(\gamma) > 0$ if and only if $(-1, \gamma)_\eta = 1$, so it follows from the product formula that

$$1 = \prod_\eta (-1, \gamma)_\eta = (-1)^{r(\gamma)} \left(\frac{-1}{\gamma}\right)(-1, \gamma)_2. \qquad \square$$

2.2. ***The ring of integers in CM fields.*** Let K be a CM field with a totally real subfield $K^+ = L$. Assume that L has strict class number 1. Let $\mathfrak{D}_{K/L}$ be the different of the extension, and let η denote a prime ideal of $\mathbb{O}_L$.

Lemma 2.2. (1) $\mathbb{O}_K = \mathbb{O}_L[t]$, *where $t^2 + at + b = 0$ for some $a, b \in \mathbb{O}_L$, and $\mathfrak{D}_{K/L}^{-1} = (1/\sqrt{d})$ with $d = a^2 - 4b$ a totally negative element of $\mathbb{O}_L$.*

(2) *Assume for $\eta|2$ that if $\eta|a$ then b is not a square modulo η. Then $(d,2)=1$, and d is square-free.*

Proof. Part (1) is proved in [Goren and Lauter 2006, Lemma 3.1].

We now prove (2). Since $\mathbb{O}_K = \mathbb{O}_L[t]/(t^2+at+b)$, the prime decomposition of every prime η is determined by the prime factorization of $t^2+at+b \bmod \eta$. If η is ramified, that implies that $t^2+at+b \equiv (t-c)^2 \bmod \eta$ for some $c \in \mathbb{O}_L/(\eta)$. But since $\eta|2$, we have

$$(t-c)^2 \equiv t^2-c^2 \equiv t^2+c^2 \bmod \eta,$$

so

$$t^2+at+b \equiv (t-c)^2 \bmod \eta \iff \eta|a \text{ and } b = \square \bmod \eta.$$

Thus, our condition implies that $\mathbb{O}_K$ is unramified over all primes $\eta|2$. It follows that $(d,2)=1$.

Next we prove that d is square-free. Let η be a prime of $\mathbb{O}_L$ not dividing 2. For $\eta|d$, we have $\mathbb{O}_K \otimes_{\mathbb{O}_L} \mathbb{O}_{L_\eta} = \mathbb{O}_{L_\eta}[\sqrt{d}]$ because $\mathbb{O}_K = \mathbb{O}_L[(-a+\sqrt{d})/2]$. Write $\mathbb{O}_{L_\eta}[\sqrt{d}] = \mathbb{O}_{L_\eta}[\sqrt{u\cdot\alpha_\eta^r}]$, where u is a unit at η and $\alpha_\eta^r|d$. If $r>1$, then

$$\mathbb{O}_{L_\eta}\big[\sqrt{u\cdot\alpha_\eta^r}\big] = \mathbb{O}_{L_\eta} + \mathbb{O}_{L_\eta}\cdot\sqrt{u\cdot\alpha_\eta^r}$$

has no element of valuation 1, which is not possible. Indeed, if π is a uniformizer of $\mathbb{O}_{K_\eta}$ with valuation normalized so that $\mathrm{val}_\eta(\mathbb{O}_{L_\eta}) = \mathbb{Z}_{\geq 0}$, then for $x \in \mathbb{O}_{L_\eta}$, $\mathrm{val}_\pi(x) = 2\,\mathrm{val}_\eta(x) \in 2\mathbb{Z}_{\geq 0}$, and

$$\mathrm{val}_\pi\big(\sqrt{u\cdot\alpha_\eta^r}\big) = \tfrac{1}{2}\,\mathrm{val}_\pi(u\cdot\alpha_\eta^r) = \mathrm{val}_\eta(u\cdot\alpha_\eta^r) = r.$$

In other words, we have shown that discriminants of quadratic extensions of p-adic fields are square-free when $p \neq 2$. □

Lemma 2.3. *We have $\mathbb{O}_K = \mathbb{O}_L[(a'+\sqrt{d})/2]$ exactly for the $a' \in \mathbb{O}_L$ such that $a' \equiv a \bmod 2\mathbb{O}_L$. Such a' satisfy $(a')^2 \equiv d \bmod 4\mathbb{O}_L$. Conversely, given $a' \in \mathbb{O}_L$ such that $(a')^2 \equiv d \bmod 4\mathbb{O}_L$, we have $\mathbb{O}_K = \mathbb{O}_L[(a'+\sqrt{d})/2]$.*

Proof. If $a' \equiv a \bmod 2\mathbb{O}_L$, we have $\mathbb{O}_K = \mathbb{O}_L[t] = \mathbb{O}_L[(a+\sqrt{d})/2] = \mathbb{O}_L[(a'+\sqrt{d})/2]$ if $a' \equiv a \bmod 2\mathbb{O}_L$. We have $d = a^2 - 4b \equiv a^2 \bmod 4\mathbb{O}_L$. Then also $(a')^2 = (a+2y)^2 = a^2+4ay+4y^2 \equiv d \bmod 4\mathbb{O}_L$.

If $\mathbb{O}_L[(a+\sqrt{d})/2] = \mathbb{O}_L[(a'+\sqrt{d})/2]$, then

$$\frac{a+\sqrt{d}}{2} = u + v\Big(\frac{a'+\sqrt{d}}{2}\Big),$$

which implies that

$$a+\sqrt{d} = 2u + va' + v\sqrt{d},$$

and so

$$v = 1 \quad \text{and} \quad a = 2u + a' \Longrightarrow a \equiv a' \bmod 2\mathbb{O}_L.$$

Finally, suppose $a' \in \mathbb{O}_L$ satisfies $(a')^2 \equiv d \bmod 4\mathbb{O}_L$. Then $(a' + \sqrt{d})/2$ is integral. Therefore, we get successively

$$\frac{a'+\sqrt{d}}{2} = u + v \cdot \left(\frac{a+\sqrt{d}}{2}\right),$$

from which we get successively

$$a' + \sqrt{d} = 2u + va + v\sqrt{d}, \quad v = 1, \quad a \equiv a' \bmod 2\mathbb{O}_L. \qquad \square$$

2.3. ***CM points on Hilbert modular varieties.*** Assume that L is a totally real field, $[L : \mathbb{Q}] = g$, and L has strict class number 1; we write $h_L^+ = 1$. This implies that $(\mathbb{O}_L{}^\times)^+ = (\mathbb{O}_L{}^\times)^2$. In this case, the Hilbert modular variety $\mathscr{H}_L$ associated to L is geometrically irreducible and affords the following description. It is the moduli space for triples $(A, \iota : \mathbb{O}_L \to \mathrm{End}(A), \eta)$, where A is a complex abelian variety of dimension g, ι is a ring embedding, and η is a principal $\mathbb{O}_L$-polarization or, equivalently, η is a principal polarization and the associated Rosati involution fixes $\mathbb{O}_L$ elementwise. We have $\mathscr{H}_L \cong \mathrm{SL}_2(\mathbb{O}_L) \setminus \mathfrak{H}^g$; see [Goren 2002, Chapter 2, §2]. Our interest is in the parametrization of CM points on $\mathscr{H}_L$.

2.3.1. *Abelian varieties with CM.* Let K be a CM field such that $K^+ = L$. We consider triples

$$(A, \iota : \mathbb{O}_K \to \mathrm{End}(A), \eta) \tag{2-1}$$

such that A is a g-dimensional complex abelian variety, ι is a ring homomorphism, and η is a principal $\mathbb{O}_K$-polarization, by which we mean a principal polarization whose associated Rosati involution induces complex conjugation on K.

Such datum produces a point on $\mathscr{H}_L$, namely, the point parametrizing $(A, \iota|_{\mathbb{O}_L}, \eta)$. This will be examined later. First we want to classify triples (A, ι, η) as in (2-1) up to isomorphism.

To a triple (A, ι, η), we may associate a CM type Φ that records the induced action of K on $T_{A,0}$, the tangent space to A at the origin. The theory of complex multiplication then asserts the existence of a fractional ideal $\mathfrak{a}$ of K such that

$$(A, \iota) \cong (\mathbb{C}^g / \Phi(\mathfrak{a}), \iota_{\mathrm{can}}),$$

where $\Phi(\mathfrak{a})$ is the lattice $\{(\varphi_1(a), \ldots, \varphi_g(a)) : a \in \mathfrak{a}\}$ and $\Phi = \{\varphi_1, \ldots, \varphi_g\}$; ι_{can} is the canonical action of $\mathbb{O}_K$ on that abelian variety obtained by extending the natural action on $\Phi(\mathfrak{a})$. Furthermore, the principal polarization η is induced from a paring on K of the form

$$(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(ax\bar{y})$$

for some $a \in K$. The conditions on a ensuring the associated polarization, say η_a, is principal are these:

(1) $(a) = (\mathfrak{D}_K \mathfrak{a}\bar{\mathfrak{a}})^{-1}$.

(2) $\bar{a} = -a$.

(3) $\mathrm{Im}(\varphi_i(a)) > 0$ for $i = 1, \ldots, g$.

It follows easily that for every $\lambda \in K^\times$, the principally polarized abelian variety associated to $(\Phi, \mathfrak{a}, a)$ in the manner above is isomorphic to that associated to $(\Phi, \lambda\mathfrak{a}, (\lambda\bar{\lambda})^{-1}a)$. Furthermore, any isomorphism of principally polarized abelian varieties $(A, \iota, \eta) \cong (A', \iota', \eta')$ as in (2-1) arises that way.

Now, given a fractional ideal $\mathfrak{a}$ of K, the ideal $\mathfrak{a}\bar{\mathfrak{a}}$ is of the form $\mathfrak{b}\mathbb{O}_K$ for some fractional ideal $\mathfrak{b}$ of L, and since $h_L = 1$, we can write $(\mathfrak{a}\bar{\mathfrak{a}})^{-1} = \lambda\mathbb{O}_K$ for a suitable $\lambda \in L$. The fractional ideal $\mathfrak{D}_K^{-1}$ is of the form $d^{-1/2}\mathbb{O}_K$, where d is a totally negative element of L. Thus,

$$(\mathfrak{D}_K \mathfrak{a}\bar{\mathfrak{a}})^{-1} = (\lambda d^{-1/2}),$$

and $\overline{\lambda d^{-1/2}} = -\lambda d^{-1/2}$. We are free to change λ by any unit $\epsilon \in {\mathbb{O}_L}^\times$. Since $({\mathbb{O}_L}^\times)^+ = ({\mathbb{O}_L}^\times)^2$, it follows easily that for any choice of signs $s_1, \ldots, s_g$ in $\{\pm 1\}$, there is a unit $\epsilon \in {\mathbb{O}_L}^\times$ such that the sign of $\varphi_i(\epsilon)$ is s_i. Since

$$\mathrm{Im}\big(\varphi_i\big(\epsilon\lambda\sqrt{d}^{-1}\big)\big) = \varphi_i(\epsilon)\,\mathrm{Im}\big(\varphi_i\big(\lambda\sqrt{d}^{-1}\big)\big),$$

by choosing ϵ properly we may arrange $\mathrm{Im}(\varphi_i(\epsilon\lambda\sqrt{d}^{-1})) > 0$ for all $i = 1, \ldots, g$. We have thus shown that for every fractional ideal $\mathfrak{a}$ of K, there is a suitable a such that $(\Phi, \mathfrak{a}, a)$ gives a principally polarized abelian variety with CM by K.

Our discussion so far shows that the isomorphism classes of principally polarized abelian varieties with CM by $\mathbb{O}_K$ are in bijection with equivalence classes of the set

$$\{(\Phi, \mathfrak{a}, a) : \Phi \text{ is a CM type, } a \text{ satisfies (1)–(3) above relative to } (\Phi, \mathfrak{a})\}.$$

The equivalence relation is $(\Phi, \mathfrak{a}, a) \sim (\Phi, \lambda\mathfrak{a}, \lambda\bar{\lambda}a)$ for $\lambda \in K^\times$ and, further, that every pair $(\Phi, \mathfrak{a})$, where Φ is a CM type and $\mathfrak{a}$ is a fractional ideal, appears in a suitable triple $(\Phi, \mathfrak{a}, a)$.

Given $(\Phi, \mathfrak{a}, a)$ and $(\Phi, \mathfrak{a}, b)$, there is a unit $\epsilon_1 \in {\mathbb{O}_K}^\times$ such that $b = \epsilon_1 a$ because both a and b generate the ideal $(\mathfrak{D}_K \mathfrak{a}\bar{\mathfrak{a}})^{-1}$. Since $\bar{a} = -a$ and $\bar{b} = -b$, it follows that $\epsilon_1 \in {\mathbb{O}_L}^\times$, and since $\mathrm{Im}(\varphi(a)) > 0$ and $\mathrm{Im}(\varphi(b)) > 0$, it follows that $\epsilon_1 \in {\mathbb{O}_L}^{\times,+}$. Using that ${\mathbb{O}_L}^{\times,+} = {\mathbb{O}_L}^{\times,2}$, we conclude that there is an $\epsilon \in \mathbb{O}_L$ such that $\epsilon_1 = \epsilon^2 = \epsilon\bar{\epsilon}$. That is, $(\Phi, \mathfrak{a}, a) \sim (\Phi, \mathfrak{a}, b)$. We therefore conclude that, in the strict class number 1 case, isomorphism classes of principally polarized abelian varieties with CM by K and a fixed CM type are parametrized by the ideal classes of K.

2.3.2. *CM points on $\mathscr{H}_L$.* Let $(A, \iota : \mathbb{O}_K \to \mathrm{End}(A))$ be a complex abelian variety with CM by K (so $[K : \mathbb{Q}] = 2\dim(A)$). Since $h_L^+ = 1$, it carries a unique principal polarization up to isomorphism. Consider $\mathrm{End}_{\mathbb{O}_L}(A)$. We use [Chai 1995, Lemma 6, p. 464]. In the notation of that lemma since A has CM, only cases III(a) and IV

can arise. But since we are working over the complex numbers, in fact only case IV can arise, and according to which, $A \sim B^n$, where B is of dimension g/n and has CM by a CM field K_0 whose totally real subfield L_0 is contained in L and satisfies $[L : L_0] = n$. One has $\mathrm{End}_L^0(A) = L \otimes_{L_0} K_0$, which is a CM field according to that lemma. It follows, because K is primitive, that $\mathrm{End}_L^0(A) = K$. As a consequence, once a RM structure is specified on A, there are precisely two CM structures extending it; if $\iota : \mathbb{O}_K \to \mathrm{End}(A)$ is one of them, the other is $\bar{\iota} := \iota \circ \tau$, where τ is complex conjugation on K. If ι has CM type Φ, then $\bar{\iota}$ has CM type $\bar{\Phi}$. Let $\mathscr{F}$ be the set of CM types for K.

Proposition 2.4. *Let* $(\Phi, [\mathfrak{a}]) \sim (\bar{\Phi}, [\bar{\mathfrak{a}}])$ $(= (\bar{\Phi}, [\mathfrak{a}^{-1}]))$ *define an equivalence relation* $\sim$ *on* $\mathscr{F} \times \mathrm{Cl}(K)$. *Then the set* $\mathscr{F} \times \mathrm{Cl}(K)/\sim$ *has* $2^{g-1} \times \#\mathrm{Cl}(K)$ *elements and is in a natural bijection with the* K*-CM points on* $\mathscr{H}_L$, *that is, with the points* $(A, \iota : \mathbb{O}_L \to \mathrm{End}(A), \eta)$ *for which we can extend* ι *to an embedding* $\mathbb{O}_K \to \mathrm{End}(A)$ *whose image is fixed* (*as a set*) *by the Rosati involution associated to* η.

3. Quaternion algebras over totally real fields

Let L be a totally real number field of degree g and strict class number 1. Let p be a prime number unramified in L, and let

$$B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L,$$

where $B_{p,\infty}$ is the rational quaternion algebra ramified at p and ∞ alone. Let

$$S := \{\mathfrak{p} \lhd \mathbb{O}_L : \mathfrak{p} \mid p\}$$

be the set of prime ideals of L above p, and let

$$S_0 = \{\mathfrak{p} \in S : f(\mathfrak{p}/p) \equiv 1 \bmod 2\}$$

be those with odd residue degree. The algebra $B_{p,L}$ is ramified precisely at all infinite places and at the primes $\mathfrak{p} \in S_0$.

The rest of this section and Sections 4 and 5 are devoted to giving a description of the quaternion algebra $B_{p,L}$ and a classification of some particular orders under the assumptions that all primes $\mathfrak{p} \in S \setminus S_0$ split in K and all primes $\mathfrak{p} \in S_0$ are inert in K. First we prove that this assumption is satisfied when p is an unramified prime of superspecial reduction for an abelian variety with CM by K.

3.1. *Splitting behavior in the case of superspecial reduction.*

Proposition 3.1. *Let* p *be a rational prime unramified in* K. *Let* A *be an abelian variety with CM by* $\mathbb{O}_K$ *defined over a number field* M *with good reduction at a prime ideal* $\mathfrak{p}_M$ *of* M *dividing the rational prime* p. *Assume that* A *has supersingular reduction modulo* $\mathfrak{p}_M$. *Then every prime in* S_0 *is inert in* K. *Assume further that* A *has superspecial reduction*; *then every prime in* $S \setminus S_0$ *is split in* K.

Proof. Since A has supersingular reduction, say $\bar{A}$, $\mathrm{End}_L^0(\bar{A}) \cong B_{p,L} = B_{p,\infty} \otimes_{\mathbb{Q}} L$ [Chai 1995, Lemma 6], and so

$$K \hookrightarrow B_{p,L}.$$

Thus, at every prime $\mathfrak{P}$ of K above a prime $\mathfrak{p}$ of L, the field $K_{\mathfrak{P}}$ splits the quaternion algebra $B_{p,L} \otimes_L L_{\mathfrak{p}}$. The quaternion algebra $B_{p,L}$ is ramified precisely at the primes in S_0 and at infinity, so if $\mathfrak{p} \in S_0$, we find that each $K_{\mathfrak{P}}$ is a quadratic field extension of $L_{\mathfrak{p}}$; that is, since p is unramified in K, all the primes in S_0 are inert in K.

Assume now that there is a prime $\mathfrak{p} \in S \setminus S_0$ that is inert in K, and let $\mathfrak{P}$ be the prime of K above $\mathfrak{p}$. Let us denote the embedding of $\mathbb{O}_L$ into $W(\bar{\mathbb{F}}_p)$ associated to $\mathfrak{p}$ $\{\varphi_1, \ldots, \varphi_f\}$ and $f = f(\mathfrak{p}/p)$, where we may order the embeddings so that $\sigma \circ \varphi_i = \varphi_{i+1}$ and σ denotes the Frobenius automorphism. Each embedding φ_i is the restriction of two embeddings of $\mathbb{O}_K$ into $W(\bar{\mathbb{F}}_p)$ that we denote ψ_i^1 and ψ_i^2, where one is the composition of the other with complex conjugation. Since $\mathfrak{P}$ is inert over $\mathfrak{p}$, σ still acts transitively on the set $\{\psi_i^j : i = 1, \ldots, f, j = 1, 2\}$.

The Dieudonné module of $\bar{A}$ decomposes as $D = \bigoplus_{\mathfrak{p}\,|\,p} D(\mathfrak{p})$ relative to the $\mathbb{O}_L$ structure. Let $H := D(\mathfrak{p})$. Then H decomposes further as

$$H = \bigoplus_{i=1}^{f} H(\varphi_i) = \bigoplus_{i=1}^{f} (H(\psi_i^1) \oplus H(\psi_i^2)),$$

where $H(\varphi_i)$ is a free $W(\bar{\mathbb{F}}_p)$-module of rank 2 on which $\mathbb{O}_L$ acts via φ_i, and it decomposes into a direct sum of two free $W(\bar{\mathbb{F}}_p)$-modules of rank 1, $H(\psi_i^1)$ and $H(\psi_i^2)$, on which $\mathbb{O}_K$ acts by ψ_i^1 and ψ_i^2, respectively. Now, the transitivity of the action of σ on the ψ_i^j means that we can order them so that

$$\begin{aligned}
&\sigma \circ \psi_i^1 = \psi_{i+1}^1, \quad && i = 1, 2, \ldots, f-1,\\
&\sigma \circ \psi_f^1 = \psi_1^2, &&\\
&\sigma \circ \psi_i^2 = \psi_{i+1}^2, \quad && i = 1, 2, \ldots, f-1,\\
&\sigma \circ \psi_f^2 = \psi_1^1. &&
\end{aligned}$$

Let us choose a basis $\{e_i^j : i = 1, 2, \ldots, f, j = 1, 2\}$ for H such that e_i^j spans $H(\psi_i^j)$. Note that the kernel of Frobenius on $\overline{H} := H \bmod p$ is an $\mathbb{O}_K$-module and is one-dimensional in every $H(\varphi_i)$ because $\bar{A}$ satisfies the Rapoport condition or, alternately, for each i, precisely one of $\{\psi_i^1, \psi_i^2\}$ belongs to the CM type. Suppose, without loss of generality, that e_1^1 spans the kernel of Frobenius in $\overline{H}(\varphi_1)$; then we must have that $\mathrm{Fr}(e_1^2)$, which is equal up to a unit to e_2^2, spans the kernel of Frobenius in $\overline{H}(\varphi_2)$ (this is where "superspecial" is being used), and by the same rationale, we find that the kernel of Frobenius in $\overline{H}(\varphi_i)$ is spanned by e_i^1 for i odd and by e_i^2 for i even. In particular, the kernel of Frobenius in $\overline{H}(\varphi_f)$ is spanned by e_f^2 because f is

even. Now, by the same rationale, $\mathrm{Fr}(e_f^1)$ spans the kernel of Frobenius in $\overline{H}(\varphi_1)$, and it lies in $\overline{H}(\psi_1^2)$ because $\sigma \circ \psi_f^1 = \psi_1^2$. This is a contradiction. □

3.2. ***A description of $B_{p,L}$.*** Next we give a description of the quaternion algebra $B_{p,L}$ in terms of a CM field K for a certain set of primes p, which according to Proposition 3.1 includes the superspecial primes of K. This description generalizes the approach of Gross and Zagier.

Notation. If $\mathfrak{q}$ is a prime ideal of L, let $\alpha_\mathfrak{q}$ denote a totally positive generator of $\mathfrak{q}$. It is unique up to an element of ${\mathbb{O}_L}^{\times +} = {\mathbb{O}_L}^{\times,2}$. Write $p = \prod_{\mathfrak{p}\in S} \alpha_\mathfrak{p}$.

Proposition 3.2. *Let K be a CM field and $K^+ = L$. Assume p is odd and unramified in L and that all primes $\mathfrak{p} \in S \setminus S_0$ split in K and all primes $\mathfrak{p} \in S_0$ are inert in K. These conditions imply that K embeds in $B_{p,L}$. Assume that the discriminant $\mathfrak{d}_{K/L} = (d)$ satisfies $(d, 2p) = 1$. Then there is a totally negative prime element $\alpha_0 \in \mathbb{O}_L$ such that $(\alpha_0, 2pd) = 1$, the ideal (α_0) is split in K, and*

$$B_{p,L} \cong \left(\frac{d, \alpha_0 p}{L}\right).$$

Proof. We first need a lemma.

Lemma 3.3 (Primes in arithmetic progressions). *Let L be a number field, and let $\nu_1, \ldots, \nu_t$ be some of L's embeddings into $\mathbb{R}$. Let $\mathfrak{r} \lhd \mathbb{O}_L$ be an integral ideal and $r \in \mathbb{O}_L$ an element such that $(r, \mathfrak{r}) = 1$. Then there is a prime element $\alpha \in \mathbb{O}_L$ such that $\alpha \equiv r \mod \mathfrak{r}$ and $\nu_i(\alpha) > 0$ for $i = 1, \ldots, t$.*

Proof. We may assume $\nu_i(r) > 0$ for $i = 1, \ldots, t$. Indeed, one may replace r by $r + n$ for any element $n \in \mathfrak{r}$. Since $\mathfrak{r} \otimes \mathbb{Q} = L$, for any $c \in \mathbb{R}$, $\mathfrak{r}$ contains elements n such that $\nu(n) > c$ for every real place ν of L. Taking $C = \max\{|\nu_i(r)| : \nu_i(r) < 0\}$ and a suitable element $n \in \mathfrak{r}$, we get $\nu_i(r + n) > 0$ for $i = 1, \ldots, t$.

Consider the modulus $\mathfrak{r}\nu_1\nu_2 \cdots \nu_t = \mathfrak{m}$ and the ray class group modulo $\mathfrak{m}$, $I(\mathfrak{m})/P(\mathfrak{m})$. Here $I(\mathfrak{m})$ is the multiplicative group of fractional ideals prime to $\mathfrak{m}$ and $P(\mathfrak{m})$ is the subgroup of principal ideals having a generator β such that $\beta \equiv 1 \mod \mathfrak{m}$ and $\nu_i(\beta) > 0$ for $i = 1, \ldots, t$. Let $L(\mathfrak{m})$ be the corresponding class field with $\mathrm{Gal}(L(\mathfrak{m})/L) \cong I(\mathfrak{m})/P(\mathfrak{m})$. The ideal (r) is an element of $I(\mathfrak{m})/P(\mathfrak{m})$. Let

$$\sigma := ((r), L(\mathfrak{m})/L) \in \mathrm{Gal}(L(\mathfrak{m})/L)$$

be the Artin symbol. By Chebotarev, there is a prime ideal $\mathfrak{p}$ such that $(\mathfrak{p}, \mathfrak{m}) = 1$ and

$$\sigma = \sigma_\mathfrak{p} = (\mathfrak{p}, L(\mathfrak{m})/L).$$

Also, $\mathfrak{p}$ is equivalent to (r) modulo $P(\mathfrak{m})$ and hence also principal. Indeed,

$$\sigma_\mathfrak{p}|_{H_L} = \sigma|_{H_L} = ((r), L(\mathfrak{m})/L)|_{H_L} = 1.$$

Since $\mathrm{Gal}(H_L/L) \cong I/P$, we must have that $\mathfrak{p}$ is principal. Let $(\alpha_1) = \mathfrak{p}$. By construction, $(\alpha_1) = (r)$ in $I(\mathfrak{m})/P(\mathfrak{m})$. That means that the ideal $(\alpha_1 r^{-1})$ has a generator $u\alpha_1 r^{-1}$, $u \in {\mathbb{O}_L}^\times$, such that

$$u\alpha_1 r^{-1} \equiv 1 \bmod \mathfrak{m}.$$

Let $\alpha = u\alpha_1$. Then $\alpha \equiv r \bmod \mathfrak{m}$, meaning $\alpha \equiv r \bmod \mathfrak{r}$, and for every $i = 1, \ldots, t$, $v_i(\alpha)$ has the same sign as $v_i(r)$, i.e., is positive. □

According to Lemma 3.3, we can choose $\alpha_0 \in \mathbb{O}_L$ satisfying these conditions:

(1) α_0 is a totally negative prime element of $\mathbb{O}_L$.

(2) $\alpha_0 \equiv p \bmod \eta^N$ for each $\eta \mid 2$ and some $N \gg 0$ (for the choice of N, see below).

(3) $\alpha_0 \equiv p \bmod \mathfrak{q}$ for each $\mathfrak{q} \mid d$.

(4) $\alpha_0 \equiv 1 \bmod p$.

Since $x^2 - dy^2 - \alpha_0 p z^2 \equiv 0 \bmod \eta^N$ has a nontrivial solution and N is large enough, by Hensel's lemma there is a p-adic solution. We therefore have

$$(d, \alpha_0 p)_\eta = 1 \quad \text{for all } \eta \mid 2, \qquad \left(\frac{\alpha_0}{\mathfrak{q}}\right) = \left(\frac{p}{\mathfrak{q}}\right) \quad \text{for all } \mathfrak{q} \mid d \tag{3-1}$$

and $(\alpha_0, 2pd) = 1$.

To show that $B_{p,L} \cong \left(\frac{d, \alpha_0 p}{L}\right)$, we need to check the following:

1. $(d, \alpha_0 p)_\eta = 1$ for all $\eta \mid 2$. This follows from (3-1).
2. $(d, \alpha_0 p)_\eta = 1$ for all finite η with $\eta \nmid d\alpha_0 p$. This is because $x^2 - dy^2 - \alpha_0 p z^2 \equiv 0 \bmod \eta$ has a nontrivial solution.
3. $(d, \alpha_0 p)_\eta = 1$ for all finite η such that $\eta \mid d$. This is so because $x^2 - \alpha_0 p z^2 \equiv 0 \bmod \eta$ has a nontrivial solution if and only if $\left(\frac{\alpha_0 p}{\eta}\right) = 1$, which is true by (3).
4. $(d, \alpha_0 p)_\eta = 1$ for all $\eta \in S \setminus S_0$. Indeed, $x^2 - dy^2 \equiv 0 \bmod \eta$ has a nontrivial solution if and only if $d = \square \bmod \eta$, which holds if and only if η splits in K.
5. $(d, \alpha_0 p)_\eta = 1$ if $\eta = \alpha_0$. This is so because the congruence $x^2 - dy^2 \equiv 0 \bmod \alpha_0$ has a nontrivial solution if and only if $\left(\frac{d}{\alpha_0}\right) = 1$. We will examine this below.
6. $(d, \alpha_0 p)_\eta = -1$ for all $\eta \in S_0$. Indeed, $x^2 - dy^2 \equiv 0 \bmod \eta$ has only the trivial solution if and only if $d \neq \square \bmod \eta$, which holds if and only if η is inert in K.
7. $(d, \alpha_0 p)_\eta = -1$ for all η real. This is so because $x^2 - dy^2 - \alpha_0 p z^2 = 0$ in $\mathbb{R}$ has only the trivial solution (since $-d$ and $-\alpha_0 p$ are both positive).

So it remains to prove only that $\left(\frac{d}{\alpha_0}\right) = 1$.

Write $d = (-1) \cdot \prod_{\mathfrak{q}|d} \alpha_{\mathfrak{q}}$ and $p = \prod_{\mathfrak{p}|p} \alpha_{\mathfrak{p}}$. Then

$$\begin{aligned}
\left(\frac{d}{\alpha_0}\right) &= \left(\frac{-1}{\alpha_0}\right) \prod_{\mathfrak{q}|d} \left(\frac{\alpha_{\mathfrak{q}}}{\alpha_0}\right) \\
&= \left(\frac{-1}{\alpha_0}\right) \prod_{\mathfrak{q}|d} \left(\left(\frac{\alpha_0}{\alpha_{\mathfrak{q}}}\right)(\alpha_0, \alpha_{\mathfrak{q}})_2\right) && \text{(by quadratic reciprocity)} \\
&= \left(\frac{-1}{\alpha_0}\right) \prod_{\mathfrak{q}|d} \left(\prod_{\mathfrak{p}|p} \left(\frac{\alpha_{\mathfrak{p}}}{\alpha_{\mathfrak{q}}}\right)\right)(\alpha_0, \alpha_{\mathfrak{q}})_2 && \left(\text{since } \left(\tfrac{\alpha_0}{\mathfrak{q}}\right) = \left(\tfrac{p}{\mathfrak{q}}\right)\right) \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -d)_2 \prod_{\mathfrak{q}|d,\, \mathfrak{p}|p} \left(\frac{\alpha_{\mathfrak{p}}}{\alpha_{\mathfrak{q}}}\right) \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -d)_2 \prod_{\mathfrak{q}|d,\, \mathfrak{p}|p} \left(\frac{\alpha_{\mathfrak{q}}}{\alpha_{\mathfrak{p}}}\right)(\alpha_{\mathfrak{p}}, \alpha_{\mathfrak{q}})_2 && \text{(by quadratic reciprocity)} \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -d)_2 \prod_{\mathfrak{p}|p} \left(\frac{-d}{\alpha_{\mathfrak{p}}}\right)(-d, \alpha_{\mathfrak{p}})_2 \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -1)_2(\alpha_0, d)_2 \prod_{\mathfrak{p}|p} \left(\frac{-1}{\alpha_{\mathfrak{p}}}\right)(\alpha_{\mathfrak{p}}, -1)_2(\alpha_{\mathfrak{p}}, d)_2 \left(\frac{d}{\alpha_{\mathfrak{p}}}\right) \\
&= (-1)^g (\alpha_0, d)_2 \prod_{\mathfrak{p}|p} (\alpha_{\mathfrak{p}}, d)_2 \left(\frac{d}{\alpha_{\mathfrak{p}}}\right) && \text{(by Proposition 2.1(5))} \\
&= (-1)^g (\alpha_0 p, d)_2 (-1)^{\#S_0} && \text{(by our assumptions on } K\text{).}
\end{aligned}$$

This equals $(-1)^{g+\#S_0}$ since $(\alpha_0 p, d)_\eta = 1$ for all $\eta | 2$; but the exponent, being the number of ramified primes of $B_{p,L}$, is necessarily even. This concludes the proof. □

3.3. *Another description of the quaternion algebra $B_{p,L}$.*

Definition 3.4. For $\alpha, \beta \in K$, define

$$[\alpha, \beta] := \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \in M_2(K).$$

Lemma 3.5. *With assumptions as in Proposition 3.2, $B_{p,L} \cong \{[\alpha, \beta] : \alpha, \beta \in K\}$.*

Proof. Proposition 3.2 implies that $B_{p,L} = L \oplus Li \oplus Lj \oplus Lij$ with $i^2 = d$, $j^2 = \alpha_0 p$, and $ij = -ji$. We can write this as $K \oplus Kj$ with the multiplicative structure such that, for $x, y \in K$, we have $x(yj) = (xy)j$, $j^2 = \alpha_0 p$, and

$$xj = (x_1 + x_2 i)j = x_1 j + x_2 ij = jx_1 - jix_2 = j(x_1 - ix_2) = j\bar{x}.$$

So for the isomorphism $x + yj \to [x, y]$ to respect the multiplicative structure, it is enough to check the following:

(1) $[\alpha, 0][0, \beta] = [0, \alpha\beta]$, so

$$\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \begin{pmatrix} 0 & \beta \\ \alpha_0 p\bar{\beta} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha\beta \\ \alpha_0 p\overline{\alpha\beta} & 0 \end{pmatrix},$$

(2) $[0, 1]^2 = [\alpha_0 p, 0]$, so

$$\begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} = \begin{pmatrix} \alpha_0 p & 0 \\ 0 & \alpha_0 p \end{pmatrix},$$

(3) $[\alpha, 0][0, 1] = [0, 1][\bar{\alpha}, 0]$, so

$$\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha \\ \alpha_0 p\bar{\alpha} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} \begin{pmatrix} \bar{\alpha} & 0 \\ 0 & \alpha \end{pmatrix}.$$ □

4. Orders in the quaternion algebra $B_{p,L}$

By Proposition 3.2, the ideal $\alpha_0\mathbb{O}_L$ splits in K. Write

$$\alpha_0\mathbb{O}_K = \mathscr{A} \cdot \bar{\mathscr{A}},$$

and let $\mathscr{D} = \mathscr{D}_{K/L} = (\sqrt{d})$ be the different ideal of K/L.

Definition 4.1. Let $\mathfrak{a}$ be an integral ideal of $\mathbb{O}_K$. For each $\mathfrak{q}|d$, fix a solution $\lambda_\mathfrak{q}$ to

$$x^2 \equiv \alpha_0 p \bmod \mathfrak{q}.$$

Let $\varepsilon(\mathfrak{a}, \mathfrak{q}) \in \{\pm 1\}$ be a choice of sign for each $\mathfrak{q}|d$ and $\lambda \in L$, $(\lambda, d) = 1$, such that

(1) $\lambda \equiv \varepsilon(\mathfrak{a}, \mathfrak{q})\lambda_\mathfrak{q} \bmod \mathfrak{q}$, $\forall \mathfrak{q}|d$ and

(2) $\lambda\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ is an integral ideal of $\mathbb{O}_K$.

This is possible by the Chinese remainder theorem and using $(\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}, d) = 1$.

We shall denote $\epsilon(\mathfrak{a})$ the vector of signs $\{\epsilon(\mathfrak{a}, \mathfrak{q}) : \mathfrak{q}|d\}$. When we need to emphasize the dependence of λ on the choice of signs, we shall write $\lambda_{\epsilon(\mathfrak{a})}$ instead of λ. For example, one particular choice of signs that we will often make is $\varepsilon(\mathfrak{a}, \mathfrak{q}) = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})}$, where $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ is an ideal such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$, and we denote $\lambda_\mathfrak{a}$ the corresponding λ.

Let $l \in \mathbb{O}_L$ be any nonzero element such that $(l, \alpha_0 d\mathfrak{a}^{-1}\bar{\mathfrak{a}}) = 1$ and l is split in K/L. In particular, l could be a power of p. Now define

$$R := R(\mathfrak{a}, \lambda, l) = \left\{[\alpha, \beta] : \alpha \in \mathscr{D}^{-1}, \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}l\mathfrak{a}^{-1}\bar{\mathfrak{a}}, \alpha \equiv \lambda\beta \bmod \mathbb{O}_K\right\}.$$

Proposition 4.2. *Apply assumptions as in Proposition 3.2. In particular, K is a CM field such that $K^+ = L$ has strict class number 1, the discriminant of K/L is prime to 2 and thus square-free, and p is odd and unramified in K. All primes $\mathfrak{p} \in S \setminus S_0$ split in K, and all primes $\mathfrak{p} \in S_0$ are inert in K. Then*:

(1) *R is an order of $B_{p,L}$ containing $\mathbb{O}_K$.*

(2) *R has discriminant $p \cdot l$.*

(3) *R does not depend on the choice of λ as long as λ satisfies the same local sign conditions.*

Proof. (1) It should be clear that R is a finitely generated $\mathbb{O}_L$-module containing $\mathbb{O}_K = \{[\alpha, 0] : \alpha \in \mathbb{O}_K\}$. We need to show that R is closed under multiplication. The multiplication formula is

$$[x, y][z, w] = [xz + \alpha_0 py\overline{w}, xw + y\overline{z}],$$

and we need to show that, for $[x, y], [z, w] \in R$, also $[x, y][z, w] \in R$.

Step 1: *Show that $xz + \alpha_0 py\overline{w} \in \mathcal{D}^{-1}$.*

A priori, $xz \in \mathcal{D}^{-2}$, and

$$\alpha_0 py\overline{w} \in \alpha_0 p\mathcal{D}^{-1}\mathcal{A}^{-1} l\mathfrak{a}^{-1}\bar{\mathfrak{a}}\overline{\mathcal{D}^{-1}\mathcal{A}^{-1} l\mathfrak{a}^{-1}\bar{\mathfrak{a}}}$$
$$= \alpha_0 p\mathcal{D}^{-2}(\mathcal{A}\overline{\mathcal{A}})^{-1} l^2 = p\mathcal{D}^{-2} l^2 \subseteq \mathcal{D}^{-2} m,$$

so it is enough to show that $\mathrm{val}_{\tilde{\mathfrak{q}}}(xz + \alpha_0 py\overline{w}) \geq -1$ for all $\tilde{\mathfrak{q}} | \mathcal{D}$. Let $\mathfrak{q} = \tilde{\mathfrak{q}} \cap \mathbb{O}_L$. Then $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$. We will work $\mathfrak{q}$-adically. Let $\pi \in \mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$ be a uniformizer such that $\overline{\pi} = -\pi$ (the extension of complex conjugation from K to $K_{\tilde{\mathfrak{q}}}$).

Lemma 4.3. *Such a π exists.*

Proof. Choose a uniformizer π_0 of $\mathbb{O}_{L_\mathfrak{q}}$, and let $K_1 = L_\mathfrak{q}(\sqrt{\pi_0})$. Then for K_1 there exists such a uniformizer. So it is enough to show that if $\mathfrak{q} | q$ and $q \neq 2$ then any q-adic field L_1 has a unique quadratic ramified extension. By local class field theory, ramified quadratic extensions are in bijection with subgroups of index 2 of $\mathbb{O}_{L_1}^\times$. There is a unique subgroup of index 2 of $\mathbb{O}_{L_1}^\times$ since it contains $\mathbb{O}_{L_1}^{\times 2}$ and $\mathbb{O}_{L_1}^\times / \mathbb{O}_{L_1}^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$. □

Note that $\mathcal{D}^{-1}\mathcal{A}^{-1} l\mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathbb{O}_{K_{\tilde{\mathfrak{q}}}} = (1/\pi)\mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$ since $(\mathcal{A}, \tilde{\mathfrak{q}}) = 1$, $(l, \tilde{\mathfrak{q}}) = 1$, and $(\mathfrak{a}^{-1}\bar{\mathfrak{a}}, \tilde{\mathfrak{q}}) = 1$ because $\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ has no ramified or inert primes. Write then $x = x_0/\pi$, $y = y_0/\pi$, $z = z_0/\pi$, and $w = w_0/\pi$ with $x_0, y_0, z_0, w_0 \in \mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$. So

$$x \equiv \lambda y \bmod \mathbb{O}_K \Longrightarrow x_0 - \lambda y_0 \in (\pi) \quad \text{and} \quad z \equiv \lambda w \bmod \mathbb{O}_K \Longrightarrow z_0 - \lambda w_0 \in (\pi).$$

Now

$$xz + \alpha_0 py\overline{w} = \frac{1}{\pi^2}(x_0 z_0 - \alpha_0 p y_0 \overline{w_0}),$$

so it is enough to show $\mathrm{val}_{\tilde{\mathfrak{q}}}(x_0z_0 - \alpha_0 p y_0 \overline{w_0}) \geq 1$. But

$$\begin{aligned} x_0z_0 - \alpha_0 p y_0 \overline{w_0} &\equiv \lambda y_0 \lambda w_0 - \alpha_0 p y_0 \overline{w_0} \bmod (\pi) \\ &\equiv \lambda^2 y_0 w_0 - \alpha_0 p y_0 w_0 \bmod (\pi) \end{aligned}$$

because conjugation is trivial mod (π)

$$\begin{aligned} &\equiv (\lambda^2 - \alpha_0 p) y_0 w_0 \\ &\equiv (\lambda_{\mathfrak{q}}^2 - \alpha_0 p) y_0 w_0 \\ &\equiv 0 \bmod (\pi). \end{aligned}$$

Step 2: *Show that* $xw + y\bar{z} \in \mathscr{D}^{-1}\mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}$.

A priori, xw, $y\bar{z} \in \mathscr{D}^{-2}\mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}$, so we just need to show $\mathrm{val}_{\tilde{\mathfrak{q}}}(xw + y\bar{z}) \geq -1$ at all primes $\tilde{\mathfrak{q}} | \mathscr{D}$. We need to show $\mathrm{val}_{\tilde{\mathfrak{q}}}(x_0w_0 - y_0\overline{z_0}) \geq 1$, using the same notation as in 1. We have, modulo (π), $x_0w_0 - y_0\overline{z_0} = x_0w_0 - y_0z_0 = \lambda y_0 w_0 - \lambda y_0 w_0 = 0$.

Step 3: *Show that* $xz + \alpha_0 p y \bar{w} - \lambda(xw + y\bar{z}) \in \mathbb{O}_K$.

A priori, by steps 1 and 2, $xz + \alpha_0 p y \bar{w} \in \mathscr{D}^{-1}$ and

$$\lambda(xw + y\bar{z}) \in \mathscr{D}^{-1} l \lambda \mathscr{A}^{-1} \mathfrak{a}^{-1} \bar{\mathfrak{a}} \subset \mathscr{D}^{-1} l \subset \mathscr{D}^{-1}$$

since $\lambda \mathscr{A}^{-1} \mathfrak{a}^{-1} \bar{\mathfrak{a}} \subseteq \mathbb{O}_K$. Therefore, we just need to show that for all $\tilde{\mathfrak{q}} | \mathscr{D}$,

$$\mathrm{val}_{\tilde{\mathfrak{q}}}(xz + \alpha_0 p y \bar{w} - \lambda(xw + y\bar{z})) \geq 0.$$

Using the same notation as above, this is equivalent to

$$\mathrm{val}_{\tilde{\mathfrak{q}}}(x_0z_0 - \alpha_0 p y_0 \overline{w_0} - \lambda(x_0w_0 - y_0\overline{z_0})) \geq 2.$$

Write $x_0 = \lambda y_0 + \pi x_1$ and $z_0 = \lambda w_0 + \pi z_1$. Then

$$\begin{aligned} &(\lambda y_0 + \pi x_1)(\lambda w_0 + \pi z_1) - \alpha_0 p y_0 \overline{w_0} - \lambda(\lambda y_0 + \pi x_1) w_0 + \lambda y_0(\lambda \overline{w_0} - \pi \overline{z_1}) \\ &\qquad = (\lambda^2 - \alpha_0 p) y_0 \overline{w_0} + \lambda \pi y_0 (z_1 - \overline{z_1}) \equiv 0 \bmod \pi^2 \end{aligned}$$

since $(z_1 - \overline{z_1}) \in (\pi)$ and $(\lambda^2 - \alpha_0 p) \in \mathfrak{q}\mathbb{O}_{L_{\mathfrak{q}}} \subset (\pi^2)$. This proves conclusion (1) of the proposition.

(2) We need to compute the discriminant of

$$R = R(\mathfrak{a}, \lambda, l) = \left\{ [\alpha, \beta] : \alpha \in \mathscr{D}^{-1}, \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}, \alpha \equiv \lambda\beta \bmod \mathbb{O}_K \right\}.$$

Let

$$R' := \{ [\alpha, \beta] : \alpha \in \mathbb{O}_K, \beta \in l \mathfrak{a}^{-1} \bar{\mathfrak{a}} \}.$$

Then R' is an $\mathbb{O}_L$-module of rank 4.

Lemma 4.4. *We have* $\mathrm{disc}(R') = (l \alpha_0 p d)^2$.

Proof. The quadratic form on R' is $\det[\alpha,\beta]=\alpha\bar{\alpha}-\alpha_0 p\beta\bar{\beta}=:q([\alpha,\beta])$. Note this quadratic form coincides with the norm form on the quaternion algebra $B_{p,L}$; writing

$$[\alpha,\beta]=[\alpha,0]+[0,\beta][0,1]=(\alpha_1+\alpha_2 i)+(\beta_1+\beta_2 i)j,$$

where $i^2=d$ and $j^2=\alpha_0 p$, we have

$$\begin{aligned}\mathrm{Norm}(\alpha_1+\alpha_2 i+\beta_1 j+\beta_2 ij)&=\alpha_1^2-\alpha_2^2 d-\beta_1^2\alpha_0 p+\beta_2^2 d\alpha_0 p\\&=(\alpha_1+\alpha_2 i)(\alpha_1-\alpha_2 i)-\alpha_0 p(\beta_1+\beta_2 i)(\beta_1-\beta_2 i)\\&=\alpha\bar{\alpha}-\alpha_0 p\beta\bar{\beta}.\end{aligned}$$

The associated bilinear form is

$$\langle[\alpha,\beta],[\gamma,\delta]\rangle=\alpha\bar{\gamma}+\bar{\alpha}\gamma-\alpha_0 p(\beta\bar{\delta}+\bar{\beta}\delta),$$

where $\frac{1}{2}\langle x,x\rangle=q(x)$. Note that $\langle[\alpha,0],[0,\delta]\rangle=0$,

$$\langle[\alpha_1,0],[\alpha_2,0]\rangle=\alpha_1\bar{\alpha}_2+\bar{\alpha}_1\alpha_2=\mathrm{Tr}_{K/L}\,\alpha_1\bar{\alpha}_2,$$

$$\langle[0,\beta_1],[0,\beta_2]\rangle=-\alpha_0 p(\beta_1\bar{\beta}_2+\bar{\beta}_1\beta_2)=-\alpha_0 p\,\mathrm{Tr}_{K/L}\,\beta_1\bar{\beta}_2.$$

To compute the discriminant of R' with respect to the bilinear form, we need to compute the determinant of the matrix $(\langle x_i,x_j\rangle)$ for $\{x_i\}$ a basis for R'. Choose a basis $\{w_1,w_2\}$ for $\mathbb{O}_K$ as an $\mathbb{O}_L$-module (for example, $\{1,t\}$). Choose a basis $\{w_3,w_4\}$ for $l\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ as an $\mathbb{O}_L$-module. By the above calculations, we see that

$$\det(\langle w_i,w_j\rangle)=\det(M_1)\det(M_2),$$

where

$$M_1=\begin{pmatrix}2w_1\overline{w_1} & w_1\overline{w_2}+w_2\overline{w_1}\\ w_1\overline{w_2}+w_2\overline{w_1} & 2w_2\overline{w_2}\end{pmatrix}=(\mathrm{Tr}(w_i\overline{w_j})),\quad i,j=1,2,$$

$$M_2=-\alpha_0 p\begin{pmatrix}2w_3\overline{w_3} & w_3\overline{w_4}+w_4\overline{w_3}\\ w_3\overline{w_4}+w_4\overline{w_3} & 2w_4\overline{w_2}\end{pmatrix}=-\alpha_0 p(\mathrm{Tr}(w_i\overline{w_j})),\quad i,j=3,4.$$

We have

$$\det(M_1)=-\operatorname{disc}_{K/L}(\mathbb{O}_K)\quad\text{and}\quad\det(M_2)=-(\alpha_0 p)\operatorname{disc}_{K/L}(l\mathfrak{a}^{-1}\bar{\mathfrak{a}}).$$

For any $\mathbb{O}_K$-ideal $\mathfrak{b}$, $\operatorname{disc}_{K/L}(\mathfrak{b})=\operatorname{disc}_{K/L}(\mathbb{O}_K)\,\mathrm{Norm}_{K/L}(\mathfrak{b})^2$ [Lang 1986, Proposition 13, p. 66], so

$$\operatorname{disc}(R')=\operatorname{disc}_{K/L}(\mathbb{O}_K)^2\,\mathrm{Norm}_{K/L}(l\mathfrak{a}^{-1}\bar{\mathfrak{a}})^2(\alpha_0 p)^2=(l\alpha_0 pd)^2.$$

We remark that this uses that l is split in K/L. In a typical application, l will be a prime lying above p. If p is inert in L, then it will automatically be split in K/L according to the hypotheses of Proposition 3.2. If l is not split in K/L, we get a higher power of l in the final answer. □

In order to show that R has discriminant $p \cdot l$, the following lemma is needed:

Lemma 4.5. *The following sequence is exact*:

$$0 \to R' \hookrightarrow R \xrightarrow{\psi} \mathcal{D}^{-1}\mathcal{A}^{-1}/\mathcal{O}_K \to 0,$$

where

$$[\alpha, \beta] \mapsto \beta \in \frac{\mathcal{D}^{-1}\mathcal{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}}{l\mathfrak{a}^{-1}\bar{\mathfrak{a}}} \cong \mathcal{D}^{-1}\mathcal{A}^{-1}/\mathcal{O}_K.$$

Proof. First, $R' \subseteq R$ because $\alpha \in \mathcal{O}_K$ and $\lambda\beta \in \lambda l \mathfrak{a}^{-1}\bar{\mathfrak{a}} = (\lambda\mathfrak{a}^{-1}\bar{\mathfrak{a}})l \subseteq \mathcal{O}_K l \subseteq \mathcal{O}_K$. Since $\lambda\beta \in \mathcal{O}_K$, clearly $\alpha \equiv \lambda\beta \bmod \mathcal{O}_K$. Now:

- Exactness at R: Clearly $R' \subseteq \mathrm{Ker}(\psi)$. Now suppose $[\alpha, \beta] \in \mathrm{Ker}(\psi)$. Then $\beta \in l\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, and so $\alpha \in \mathcal{O}_K$ because $\lambda\beta \in \mathcal{O}_K$ by the definition of λ and $\alpha \equiv \lambda\beta \bmod \mathcal{O}_K$. So $[\alpha, \beta] \in R'$.
- Surjectivity of ψ: Let $\beta \in \mathcal{D}^{-1}\mathcal{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}$. Then we have $[\lambda\beta, \beta] \in R$ because $\lambda\beta \in \mathcal{D}^{-1} l(\lambda\mathcal{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}) \subseteq \mathcal{D}^{-1} l \mathcal{O}_K \subseteq \mathcal{D}^{-1}$. □

Thus, $\mathrm{disc}_{K/L}(R) = \mathrm{disc}_{K/L}(R')/\mathrm{Norm}_{K/L}(\mathcal{D}\mathcal{A})^2 = (l\alpha_0 pd)^2/(\alpha_0 d)^2 = l^2p^2$, so the discriminant of R as an order of $B_{p,L}$ is lp. This proves conclusion (2).

(3) Finally, R is independent of the choice of λ assuming λ satisfies the same local sign conditions. Suppose both λ and λ' satisfy the conditions of Definition 4.1. Let $[\alpha, \beta] \in R(\mathfrak{a}, \lambda, l)$, so $\alpha \in \mathcal{D}^{-1}$, $\beta \in \mathcal{D}^{-1}\mathcal{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}$, and $\alpha \equiv \lambda\beta \bmod \mathcal{O}_K$. Then

$$\alpha - \lambda\beta \in \mathcal{O}_K \Longrightarrow (\sqrt{d}\alpha) - \lambda(\sqrt{d}\beta) \in (\sqrt{d}),$$

and

$$(\sqrt{d}\alpha) - \lambda'(\sqrt{d}\beta) - (\lambda - \lambda')(\sqrt{d}\beta) \in (\sqrt{d}).$$

Now, because d is square-free and for all $\mathfrak{q} | d$ we have $\lambda' = e(\mathfrak{a}, \mathfrak{q})\lambda_{\mathfrak{q}} \equiv \lambda \bmod \mathfrak{q}$, it follows that $\lambda - \lambda' \in (d)$. But

$$\lambda - \lambda' \in (d) \Longrightarrow (\lambda - \lambda')\sqrt{d}\beta \in dl\mathcal{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$$

and

$$\lambda\sqrt{d}\beta - \lambda'\sqrt{d}\beta \in \mathcal{O}_K$$

by the definitions of λ and λ', so

$$(\lambda - \lambda')\sqrt{d}\beta \in \mathcal{O}_K \cap dl\mathcal{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq (d).$$

It follows that $(\sqrt{d}\alpha) - \lambda'(\sqrt{d}\beta) \in (\sqrt{d})$, so $\alpha \equiv \lambda'\beta \bmod \mathcal{O}_K$. □

5. Classification of superspecial orders of $B_{p,L}$ in which $\mathbb{O}_K$ embeds, having chosen an embedding $K \hookrightarrow B_{p,L}$

By a superspecial order in $B_{p,L}$, we mean an order of discriminant $p\mathbb{O}_L$. An example is $R \otimes_{\mathbb{Z}} \mathbb{O}_L$ for a maximal order R of $B_{p,\infty}$. Let K be a primitive CM field such that $K^+ = L$. As before, d will denote a totally negative generator of the relative different ideal $\mathscr{D}_{K/L}$. In this section, we classify the superspecial orders in which $\mathbb{O}_K$ embeds, relying on the results in Section 4 and making the particular choice of local signs $\varepsilon(\mathfrak{a}, \mathfrak{q}) = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})}$, where $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ is an ideal such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$, and we denote $\lambda_{\mathfrak{a}}$ the corresponding λ. We shall prove that, once the embedding $K \hookrightarrow B_{p,L}$ has been fixed, the isomorphism classes of the superspecial orders in which $\mathbb{O}_K$ embeds are in bijection with the ideal class group of K (Theorem 5.7). Our classification of these orders will be achieved through a series of lemmas:

Lemma 5.1. *Let R_1 and R_2 be two superspecial orders in $B_{p,L}$. Then $R_1 \cong R_2$ over K if and only if there exists $\mu \in K$ such that $R_1 = \mu R_2 \mu^{-1}$.*

Proof. By Skolem–Noether, $R_1 \cong R_2$ if and only if there exists $\mu \in B_{p,L}^{\times}$ such that $R_1 = \mu R_2 \mu^{-1}$. This is a K-automorphism if and only if $\mu \in \mathrm{Cent}_{B_{p,L}}(K) = K$. □

Lemma 5.2. *Given $\mathfrak{a}$ and λ as in Definition 4.1, there exists $\mathfrak{c} \mid d$ such that we have $R(\mathfrak{a}, \lambda) = R(\mathfrak{ac}, \lambda_{\mathfrak{ac}})$.*

Proof. We have $R(\mathfrak{ac}, \lambda_{\mathfrak{ac}}, l) = R(\mathfrak{a}, \lambda_{\mathfrak{a}} \cdot \lambda_{(-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{c})}}, l)$ because

$$\lambda_{\mathfrak{ac}} \equiv (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{ac})} \lambda_{\mathfrak{q}} \bmod \mathfrak{q} \quad \text{for all } \mathfrak{q} \mid d,$$

so

$$\lambda_{\mathfrak{ac}} \equiv \lambda_{\mathfrak{a}} (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{c})} \bmod \mathfrak{q} \quad \text{for all } \mathfrak{q} \mid d.$$

So as $\mathfrak{c}$ ranges over the ideals dividing d, we get all sign vectors $\varepsilon(\mathfrak{a})$ that appear in the left-hand side and each one once. □

Lemma 5.3. *Fix $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$ representatives for the class group of K and the choice of local signs as above. Then every $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ is isomorphic to $R(\mathfrak{b}, \lambda_{\mathfrak{b}})$ for some $\mathfrak{b} \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$.*

Proof. Let $\mu \in K^{\times}$ be such that $\mathfrak{b} = \mu\mathfrak{a}$ for some (unique) $\mathfrak{b} \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$. Then

$$\begin{aligned}
&\mu^{-1} R(\mathfrak{a}, \lambda_{\mathfrak{a}}) \mu \\
&= \left\{ \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \bar{\mu}^{-1} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & \bar{\mu} \end{pmatrix} \right. \\
&\qquad \left. : \alpha \in \mathscr{D}^{-1},\ \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}},\ \alpha \equiv \lambda_{\mathfrak{a}}\beta \bmod \mathbb{O}_K \right\} \\
&= \left\{ \begin{pmatrix} \alpha & (\bar{\mu}/\mu)\beta \\ \alpha_0 p \overline{((\bar{\mu}/\mu)\beta)} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathscr{D}^{-1},\ \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}},\ \alpha \equiv \lambda_{\mathfrak{a}}\beta \bmod \mathbb{O}_K \right\}.
\end{aligned}$$

By setting $b = \frac{\overline{\mu}}{\mu}\beta$, this is equal to

$$\left\{ \begin{pmatrix} \alpha & b \\ \alpha_0 p\bar{b} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathscr{D}^{-1},\ b \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}},\ \alpha \equiv \lambda_{\mathfrak{a}}\frac{\mu}{\overline{\mu}}b \bmod \mathbb{O}_K \right\}$$

because $\mathfrak{b} = \mu\mathfrak{a}$,

$$\frac{\overline{\mu}}{\mu}\beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}\frac{\overline{\mu}}{\mu} = \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}},$$

and $\alpha \equiv \lambda_{\mathfrak{a}}(\mu/\overline{\mu})(\overline{\mu}/\mu)\beta = \lambda_{\mathfrak{a}}(\mu/\overline{\mu})b \bmod \mathbb{O}_K$.

Now it remains to show $\alpha \equiv \lambda_{\mathfrak{a}}(\mu/\overline{\mu})b \bmod \mathbb{O}_K$ if and only if $\alpha \equiv \lambda_{\mathfrak{b}}b \bmod \mathbb{O}_K$. In other words, we must show that the following two conditions are equivalent:

$$(\sqrt{d}\alpha) \equiv \lambda_{\mathfrak{a}}\frac{\mu}{\overline{\mu}}(\sqrt{d}b) \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} \mid \sqrt{d}\mathbb{O}_K,$$

$$(\sqrt{d}\alpha) \equiv \lambda_{\mathfrak{b}}(\sqrt{d}b) \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} \mid \sqrt{d}\mathbb{O}_K.$$

This can be checked in $\mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$ for every $\tilde{\mathfrak{q}}$. The point is that $(-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{b})} = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})} \cdot (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mu)}$, and so it is enough to show that $\mu/\overline{\mu} \equiv (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mu)} \bmod \tilde{\mathfrak{q}}$. This follows from the fact that $\mathbb{O}_{K_{\tilde{\mathfrak{q}}}} = \mathbb{O}_{L_{\mathfrak{q}}}[\pi]$ with $\overline{\pi} = -\pi$, so writing $\mu = \pi^r \cdot u$ with $u \in \mathbb{O}_{K_{\tilde{\mathfrak{q}}}}^{\times}$, we have $\bar{u} = u \bmod \tilde{\mathfrak{q}}$ and

$$\frac{\mu}{\overline{\mu}} = (-1)^r\frac{u}{\bar{u}} \equiv (-1)^r \bmod \tilde{\mathfrak{q}}.$$

Thus, we have proved that $\mu^{-1}R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mu = R(\mu\mathfrak{a}, \lambda_{\mu\mathfrak{a}})$. □

Lemma 5.4. *We have* $R(\mathfrak{a}, \lambda_{\mathfrak{a}}) = R(\mathfrak{b}, \lambda_{\mathfrak{b}})$ *if and only if* $\mathfrak{a}^{-1}\bar{\mathfrak{a}} = \mathfrak{b}^{-1}\bar{\mathfrak{b}}$ *and* $\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a}) \equiv \mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{b}) \bmod 2$ *for all* $\tilde{\mathfrak{q}} \mid d$.

Proof. ($\Leftarrow$) This is obvious.

($\Rightarrow$) Let $\beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ and $\alpha := \lambda_{\mathfrak{a}}\beta$. Since $\lambda_{\mathfrak{a}}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq \mathbb{O}_K$, it follows that $\alpha \in \mathscr{D}^{-1}$. Therefore, $[\alpha, \beta] \in R(\mathfrak{a}, \lambda_{\mathfrak{a}}) = R(\mathfrak{b}, \lambda_{\mathfrak{b}})$, so $\beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}$. Therefore, $\mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}$. By symmetry, we have equality.

Furthermore, since $[\lambda_{\mathfrak{a}}\beta, \beta] \in R(\mathfrak{b}, \lambda_{\mathfrak{b}})$, we have

$$\lambda_{\mathfrak{a}}\beta \equiv \lambda_{\mathfrak{b}}\beta \bmod \mathbb{O}_K \quad \text{for all } \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}.$$

Otherwise said,

$$\beta(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{b}}) \equiv 0 \bmod \mathbb{O}_K \quad \text{for all } \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}},$$

and this implies

$$\lambda_{\mathfrak{a}} \equiv \lambda_{\mathfrak{b}} \bmod \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}.$$

We conclude that

$$\lambda_{\mathfrak{a}} \equiv \lambda_{\mathfrak{b}} \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} \mid d \quad (\text{because } (\mathscr{D}, \mathscr{A}\mathfrak{a}\bar{\mathfrak{a}}^{-1}) = 1).$$

It follows that

$$(-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})} = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{b})} \quad \text{for all } \tilde{\mathfrak{q}} \mid d. \qquad \square$$

Lemma 5.5. *For* $\mathfrak{b}, \mathfrak{b}' \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$, $R(\mathfrak{b}, \lambda_{\mathfrak{b}}) \sim R(\mathfrak{b}', \lambda_{\mathfrak{b}'})$ *if and only if* $\mathfrak{b} = \mathfrak{b}'$.

Proof. ($\Leftarrow$) This is obvious.

($\Rightarrow$) Suppose $R(\mathfrak{b}, \lambda_{\mathfrak{b}}) = \mu^{-1} R(\mathfrak{b}', \lambda_{\mathfrak{b}'})\mu = R(\mu\mathfrak{b}', \lambda_{\mu\mathfrak{b}'})$ (this second equality was proved in Lemma 5.3 above). By Lemma 5.4, this implies

$$\mathfrak{b}^{-1}\bar{\mathfrak{b}} = \mathfrak{b}'^{-1}\bar{\mathfrak{b}}'\frac{\bar{\mu}}{\mu} \quad \text{or} \quad \mathfrak{b}'\mathfrak{b}^{-1}\mu = \overline{\mathfrak{b}'\mathfrak{b}^{-1}\mu}.$$

An ideal $\mathfrak{f} \lhd \mathbb{O}_K$ satisfies $\mathfrak{f} = \bar{\mathfrak{f}}$ if and only if $\mathfrak{f} = j \cdot \prod_{\tilde{\mathfrak{q}} \mid d} \tilde{\mathfrak{q}}^{s(\tilde{\mathfrak{q}})}$ for $j \in L$. Indeed, write $\mathfrak{f}$ as a product of inert, split, and ramified prime ideals. Inert prime ideals are generated by elements of L. Split prime ideals must appear in the factorization to the same power as their complex conjugate because of the condition $\mathfrak{f} = \bar{\mathfrak{f}}$. Thus, it is actually some power of their norm that appears, and that is also generated by an element of L. What remains is a product of some ramified primes.

Applying this to the ideal $\mathfrak{f} = \mathfrak{b}'\mathfrak{b}^{-1}\mu$, we find that

$$\mu\mathfrak{b}' = j \cdot \prod_{\tilde{\mathfrak{q}} \mid d} \tilde{\mathfrak{q}}^{s(\tilde{\mathfrak{q}})} \cdot \mathfrak{b}.$$

Note that $R(\mu\mathfrak{b}', \lambda_{\mu\mathfrak{b}'}) = R((\mu/j)\mathfrak{b}', \lambda_{(\mu/j)\mathfrak{b}'})$, so we can replace μ by μ/j to obtain $R(\mathfrak{b}, \lambda_{\mathfrak{b}}) = R(\mu\mathfrak{b}', \lambda_{\mu\mathfrak{b}'})$ with $\mu\mathfrak{b}'$ of the form

$$\mu\mathfrak{b}' = \prod_{\tilde{\mathfrak{q}} \mid d} \tilde{\mathfrak{q}}^{s(\tilde{\mathfrak{q}})} \cdot \mathfrak{b}.$$

Now $\lambda_{\mathfrak{b}} = \lambda_{\mu\mathfrak{b}'}$ implies that each $s(\tilde{\mathfrak{q}})$ is even, so $\mu\mathfrak{b}' = k\mathfrak{b}$ for some $k \in K$. Thus, $\mathfrak{b}' = \mathfrak{b}$ because they are already representatives for the class group. $\square$

Lemma 5.6. *Any superspecial order* $R \supseteq \mathbb{O}_K$ *is isomorphic to some* $R(\mathfrak{a}, \lambda)$.

Proof. Let $\mathfrak{c}$ be a prime ideal of L. For any ideal $\mathfrak{a}$ of $K_{\mathfrak{c}}$, define orders $R^{\mathfrak{c}}(\mathfrak{a}, \lambda_{\mathfrak{a}})$ of $(B_{p,L})_{\mathfrak{c}}$ exactly the same way as for $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$. The orders have the same properties that were proved for the $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ in Proposition 4.2: independent of the choice of λ and conductor $p\mathbb{O}_{L_{\mathfrak{c}}}$.

Then for an ideal $\mathfrak{a}$ of K, we have $R(\mathfrak{a}, \lambda_{\mathfrak{a}})_{\mathfrak{c}} = R^{\mathfrak{c}}(\mathfrak{a}_{\mathfrak{c}}, \lambda_{\mathfrak{a}_{\mathfrak{c}}})$. Let R be an order of $B_{p,L}$ that contains $\mathbb{O}_K$ of discriminant $p\mathbb{O}_L$. For every $\mathfrak{c}$, the order $R_{\mathfrak{c}}$ is an Eichler order of discriminant $p\mathbb{O}_{L_{\mathfrak{c}}}$ as is the order $R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}}$, where $\mathbb{O}$ represents the trivial ideal class. For every $\mathfrak{c}$, there is a $\mu_{\mathfrak{c}} \in (B_{p,L})_{\mathfrak{c}}^{\times}$ such that

$$R_{\mathfrak{c}} = \mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}}$$

because Eichler orders of the same discriminant are locally conjugate. Furthermore,

$$R_{\mathfrak{c}} = \mathrm{M}_2(\mathbb{O}_{L_{\mathfrak{c}}}) \subseteq (B_{p,L})_{\mathfrak{c}} = \mathrm{M}_2(L_{\mathfrak{c}})$$

for almost all $\mathfrak{c}$, and the same holds for $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$. Now it is enough to show that we can choose $\mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}$ for all $\mathfrak{c}$ because in that case

$$R_{\mathfrak{c}} = \mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}} = R^{\mathfrak{c}}((\mu_{\mathfrak{c}}), \lambda_{(\mu_{\mathfrak{c}})})$$

for a collection of elements

$$\{\mu_{\mathfrak{c}} : \mathfrak{c} \lhd \mathbb{O}_L \text{ prime}, \mu_{\mathfrak{c}} = 1 \text{ for almost all } \mathfrak{c}, \mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}\}.$$

Therefore, there is an ideal $\mathfrak{a}$ of K such that, for all $\mathfrak{c}$, $\mathfrak{a}_{\mathfrak{c}} = (\mu_{\mathfrak{c}})$. The two orders R and $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ are equal because they are equal locally everywhere, and we are done.

To show that we may choose $\mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}$ for all $\mathfrak{c}$, we use [Vignéras 1980, Theorems 3.1 and 3.2, pages 43–44] to produce an element $\nu_{\mathfrak{c}}$ such that

(1) $\nu_{\mathfrak{c}}^{-1}(\mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}})\nu_{\mathfrak{c}} = \mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}} = R_{\mathfrak{c}}$ and

(2) the embedding of $\mathbb{O}_{K_{\mathfrak{c}}}$ into $R_{\mathfrak{c}}$ is the embedding of $\mathbb{O}_{K_{\mathfrak{c}}}$ into $R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}}$ conjugated by $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}}$.

Since conjugation by $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}}$ fixes $K_{\mathfrak{c}}$ pointwise, this implies $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}}$ commutes with $K_{\mathfrak{c}}$, and so $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}$. □

Our conclusion is that isomorphism classes of superspecial orders of $B_{p,L}$ in which $\mathbb{O}_K$ embeds are the isomorphism classes of $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$. Thus, we have proved the following theorem:

Theorem 5.7. *Fix an embedding of $K \hookrightarrow B_{p,L}$. The isomorphism classes of the superspecial orders in which $\mathbb{O}_K$ embeds are in bijection with the ideal class group of K via the map*

$$[\mathfrak{a}] \mapsto R(\mathfrak{a}, \lambda_{\mathfrak{a}}).$$

Remark 5.8. In the case $L = \mathbb{Q}$, Theorem 5.7 provides a different proof for the main theorems of Dorman's paper [1989a] on global orders in definite quaternion algebras and corrects several minor errors and gaps in the proofs there. For example, we correct the missing condition on the integrality for $\lambda\mathfrak{D}^{-1}\mathfrak{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ and the resulting mistake in the proof of Proposition 2, and we give a different proof of the one-to-one correspondence.

6. Main theorems on counting formulas

6.1. ***Assumptions and notation.*** Let L be a totally real field of degree g of strict class number 1, p a rational prime that is unramified in L, and K a primitive CM field with $K^+ = L$. Using the same notation as in Lemma 2.2, write the ring of

integers of K, $\mathbb{O}_K = \mathbb{O}_L[t]$, where $t^2 + at + b = 0$ for some $a, b \in \mathbb{O}_L$, and the different $\mathfrak{D} = \mathfrak{D}_{K/L} = (\sqrt{d})$ with $d = a^2 - 4b$ a totally negative element of $\mathbb{O}_L$.

Assume as in Proposition 3.2 that all primes $\mathfrak{p} \in S \setminus S_0$ split in K and all primes $\mathfrak{p} \in S_0$ are inert in K and that the discriminant $\mathfrak{d}_{K/L} = (d)$ satisfies $(d, 2) = 1$ and $(d, p) = 1$. Let $\alpha_0 \in \mathbb{O}_L$ be a totally negative prime element such that

$$B_{p,L} \cong \left(\frac{d, \alpha_0 p}{L}\right),$$

where $(\alpha_0, 2pd) = 1$, $\alpha_0 \equiv p \mod \mathfrak{q}$ for each $\mathfrak{q} \mid d$, $\alpha_0 \equiv 1 \mod p$, and $\alpha_0 \mathbb{O}_K = \mathscr{A} \cdot \bar{\mathscr{A}}$.

For $l \in \mathbb{O}_L$ such that $(l, \alpha_0 d \mathfrak{a}^{-1} \bar{\mathfrak{a}}) = 1$, let

$$R := R(\mathfrak{a}, \lambda, l) = \left\{[\alpha, \beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{D}^{-1} \mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}, \alpha \equiv \lambda\beta \mod \mathbb{O}_K\right\}.$$

6.2. ***Counting simultaneous embeddings.*** Let K' be another CM field that has $\mathbb{O}_{K'} = \mathbb{O}_L[w]$ and

$$\operatorname{disc}_{K'/L} = (\operatorname{Tr}(w)^2 - 4 \operatorname{Norm}(w)) = (d')$$

generated by a totally negative element d' of L.

Now we are assuming we are in the situation where an abelian variety A with CM by K has superspecial reduction modulo p, and we fix an isomorphism

$$\operatorname{End}_{\mathbb{O}_L}(A) \cong R(\mathfrak{a}, \lambda)$$

for some unique $\mathfrak{a} \lhd \mathbb{O}_K$ (Lemma 5.6, Theorem 5.7). Then, to count simultaneous embeddings of $\mathbb{O}_{K'} = \mathbb{O}_L[\omega]$, i.e., embeddings $\mathbb{O}_{K'} \to \operatorname{End}_{\mathbb{O}_L}(A)$, we count elements $[\alpha, \beta] \in R(\mathfrak{a}, \lambda)$ with trace equal to $\operatorname{Tr}(\omega)$ and with norm equal to $\operatorname{Norm}(\omega)$, that is, elements of the set $S(\mathfrak{a}, \lambda, 1)$, where

$$S(\mathfrak{a}, \lambda, l) = \left\{[\alpha, \beta] = \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \in R(\mathfrak{a}, \lambda, l) \right. \\ \left. : \operatorname{Tr}[\alpha, \beta] = \operatorname{Tr}(w), \operatorname{Norm}[\alpha, \beta] = \operatorname{Norm}(w)\right\}.$$

Let $[\alpha, \beta]$ be an element of this set. Since

$$\mathbb{O}_K = \mathbb{O}_L + \mathbb{O}_L \cdot \frac{a + \sqrt{d}}{2} = \left\{\frac{2l_1 + l_2(a + \sqrt{d})}{2} : l_1, l_2 \in \mathbb{O}_L\right\} \\ = \left\{\frac{l_3 + l_4\sqrt{d}}{2} : l_3, l_4 \in \mathbb{O}_L, l_3 - a l_4 \equiv 0 \mod 2\mathbb{O}_L\right\},$$

we can write $\alpha \in \mathfrak{D}^{-1}$ in the form $\alpha = (l_3 + l_4\sqrt{d})/2\sqrt{d}$, where $l_3, l_4 \in \mathbb{O}_L$ with $l_3 - a l_4 \equiv 0 \mod 2\mathbb{O}_L$, and in this notation, $\operatorname{Tr}(\alpha) = \operatorname{Tr}([\alpha, \beta]) = l_4$. So

$$\alpha = \frac{x + \operatorname{Tr}(w)\sqrt{d}}{2\sqrt{d}}, \quad x \in \mathbb{O}_L,\ x - a \operatorname{Tr}(w) \equiv 0 \mod 2\mathbb{O}_L,$$

where $a = -\mathrm{Tr}(t)$ and

$$\beta = \frac{l}{\sqrt{d}}\gamma, \quad \gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}.$$

Since

$$\begin{aligned}\mathrm{Norm}[\alpha,\beta] &= \det[\alpha,\beta] = \alpha\bar{\alpha} - \alpha_0 p\beta\bar{\beta} \\ &= \frac{x + \mathrm{Tr}(w)\sqrt{d}}{2\sqrt{d}} \cdot \frac{x - \mathrm{Tr}(w)\sqrt{d}}{-2\sqrt{d}} - \alpha_0 p \frac{l^2}{-d}\gamma\bar{\gamma} \\ &= \frac{1}{-4d}(x^2 - \mathrm{Tr}(w)^2 d - 4\alpha_0 p l^2 \gamma\bar{\gamma}),\end{aligned}$$

it follows that

$$-d\left(4\,\mathrm{Norm}(w) - \mathrm{Tr}(w)^2\right) = x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma}.$$

So an element $[\alpha,\beta]$ of the set $S(\mathfrak{a},\lambda,l)$ gives rise to a solution (x,γ) to

$$dd' = x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma}$$

with $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, $x \in \mathbb{O}_L$, and $x \equiv a\,\mathrm{Tr}(w) \bmod 2\mathbb{O}_L$, where $x^2 - dd'$ is a totally negative element of $\mathbb{O}_L$ because α_0 is. Call this set of conditions on x conditions **C**.

Our analysis allows us to define a function $\phi : S(\mathfrak{a},\lambda,l) \to S_1(\mathfrak{a},x,l)$ that sends $[\alpha,\beta] \mapsto \gamma$ (it is used in the proof of Theorem 6.5 below), where the set $S_1(\mathfrak{a},x,l)$ is defined for an integral ideal $\mathfrak{a}$ and x satisfying conditions **C** by

$$S_1(\mathfrak{a},x,l) := \left\{\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} : \mathrm{Norm}(\gamma) = \gamma\bar{\gamma} = \frac{x^2 - dd'}{4\alpha_0 p l^2}\right\}.$$

For $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, the ideal generated by γ can be written as $(\gamma) = \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \cdot \mathfrak{b}$ for $\mathfrak{b}$ an ideal of $\mathbb{O}_K$, and $\mathrm{Norm}(\mathfrak{b}) = \alpha_0\,\mathrm{Norm}(\gamma)$. We let $S_2(\mathfrak{a},x,l)$ be the set

$$S_2(\mathfrak{a},x,l) := \left\{\mathfrak{b} \lhd \mathbb{O}_K : \mathrm{Norm}(\mathfrak{b}) = \frac{x^2 - dd'}{4pl^2},\ \mathfrak{b} \sim \mathfrak{a}^2\mathscr{A}\right\}.$$

Proposition 6.1. *The map $S_1(\mathfrak{a},x,l) \to S_2(\mathfrak{a},x,l)$ that sends $\gamma \mapsto \mathfrak{b}_\gamma = (\gamma)\mathscr{A}\mathfrak{a}\bar{\mathfrak{a}}^{-1}$ is a surjective $[w_K : 1]$-map, where w_K equals the number of roots of unity in K.*

Proof. To show that the map is $[w_K : 1]$, we first show $\mathfrak{b}_\gamma = \mathfrak{b}_\delta$ if and only if $\gamma = \mu\delta$, where μ is a root of unity in K. Since $\mathfrak{b}_\gamma$ depends only on (γ), the "only if" part is clear. Now if $\mathfrak{b}_\gamma = \mathfrak{b}_\delta$, then $(\gamma) = (\delta)$, so $\gamma = \mu\delta$ for some $\mu \in \mathbb{O}_K{}^\times$, but also $\mathrm{Norm}(\gamma) = \mathrm{Norm}(\delta) = \mathrm{Norm}(\mu)\cdot\mathrm{Norm}(\gamma)$ implies $\mathrm{Norm}(\mu) = 1$ implies $\mu \in \mu_K$.

Next we show that the map is surjective. Given $\mathfrak{b} \in S_2(\mathfrak{a},x,l)$, let γ be a generator of $\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathfrak{b}$. Then $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, and

$$(\mathrm{Norm}(\gamma)) = (\gamma\bar{\gamma}) = \left(\frac{x^2 - dd'}{4\alpha_0 p l^2}\right).$$

Hence, there exists a totally positive unit $\epsilon' \in {\mathbb{O}_L}^{\times +} = {\mathbb{O}_L}^{\times 2}$ with $\epsilon' = \epsilon^2$ such that

$$\epsilon' \gamma \bar{\gamma} = \frac{x^2 - dd'}{4\alpha_0 p l^2}.$$

Changing γ to $\epsilon\gamma$,

$$\gamma \bar{\gamma} = \frac{x^2 - dd'}{4\alpha_0 p l^2}.$$

So $\gamma \in S_1(\mathfrak{a}, x, l)$, and since it is still true that $(\gamma) = \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathfrak{b}$, we have $\mathfrak{b}_\gamma = \mathfrak{b}$. □

Now given an element γ of $S_1(\mathfrak{a}, x, l)$, we can construct elements of $S(\mathfrak{a}, \lambda, l)$ as follows. Let

$$\alpha = \frac{x + \mathrm{Tr}(w)\sqrt{d}}{2\sqrt{d}} \quad \text{and} \quad \beta = \frac{l}{\sqrt{d}}\gamma.$$

First, we note that $\alpha \in \mathscr{D}^{-1}$ if and only if $(x + \mathrm{Tr}(w)\sqrt{d})/2 \in \mathbb{O}_K$ if and only if $x \in \mathbb{O}_L$ and $x \equiv a\,\mathrm{Tr}(w) \bmod 2\mathbb{O}_L$, which holds because x satisfies conditions **C**.

Next, note that $\beta = (l/\sqrt{d})\gamma \in \mathscr{D}^{-1}\mathscr{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}$ if and only if $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, which holds by the definition of the set $S_1(\mathfrak{a}, x)$.

It remains to check that the congruence $\alpha \equiv \lambda\beta \bmod \mathbb{O}_K$ is satisfied. Since $\gamma \in S_1(\mathfrak{a}, x, l)$,

$$x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma} = dd' \equiv 0 \bmod d.$$

Next, the congruence $\lambda^2 \equiv \alpha_0 p \bmod d$ implies that

$$x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma} + 4l^2\gamma\bar{\gamma}(\alpha_0 p - \lambda^2) \equiv 0 \bmod d,$$

and so

$$x^2 - 4\lambda^2 l^2 \gamma\bar{\gamma} \equiv 0 \bmod d.$$

Therefore,

$$(x + \mathrm{Tr}(w)\sqrt{d})(x - \mathrm{Tr}(w)\sqrt{d}) - 4\lambda^2 l^2 \gamma\bar{\gamma} \equiv 0 \bmod d.$$

Using $x + \mathrm{Tr}(w)\sqrt{d} = 2\sqrt{d}\alpha$ and $l\gamma = \sqrt{d}\beta$, we get

$$-4d(\alpha\bar{\alpha} - \lambda^2\beta\bar{\beta}) \equiv 0 \bmod d.$$

Since $(d, 2) = 1$, it follows that $\alpha\bar{\alpha} \equiv \lambda^2\beta\bar{\beta} \bmod \mathbb{O}_K$. Now, α and $\lambda\beta$ belong to $\mathscr{D}^{-1} = (1/\sqrt{d})\mathbb{O}_K$, and hence,

$$\alpha_1 := \sqrt{d}\alpha \quad \text{and} \quad \beta_1 := \sqrt{d}\lambda\beta$$

are in $\mathbb{O}_K$, and we have $\alpha_1\bar{\alpha}_1 \equiv \beta_1\bar{\beta}_1 \bmod d$. Equivalently, this relation holds modulo all ideals $\mathfrak{q}$ of $\mathbb{O}_L$ dividing d:

$$\alpha_1\bar{\alpha}_1 \equiv \beta_1\bar{\beta}_1 \bmod \mathfrak{q} \quad \text{for all } \mathfrak{q} \mid d, \mathfrak{q} \lhd \mathbb{O}_L. \tag{6-1}$$

Let $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ be a prime such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$. Then $\mathbb{O}_K/\tilde{\mathfrak{q}} \cong \mathbb{O}_L/\mathfrak{q}$, and complex conjugation hence acts trivially modulo $\tilde{\mathfrak{q}}$. So (6-1) is equivalent to

$$\alpha_1^2 \equiv \beta_1^2 \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} | d\mathbb{O}_K, \tilde{\mathfrak{q}} \lhd \mathbb{O}_K,$$

which is equivalent to

$$\alpha_1 \equiv \pm\beta_1 \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} | d\mathbb{O}_K, \tilde{\mathfrak{q}} \lhd \mathbb{O}_K.$$

So this shows that there exists a choice of signs $\varepsilon(\mathfrak{a}, \mathfrak{q})$ and a λ depending on this choice for which the congruence condition is satisfied, and $[\alpha, \beta] \in S(\mathfrak{a}, \lambda, l)$. However, for any ideal $\mathfrak{q}$ for which $x \equiv 0 \bmod \mathfrak{q}$, both signs will work. This motivates the following definitions and theorem:

Definition 6.2. (1) For $x \in \mathbb{O}_L$, let $\delta(x) := 2^{\#\{\mathfrak{q} | d : x \equiv 0 \bmod \mathfrak{q}\}}$.

(2) Let $\tau := \#\{\mathfrak{q} | d\}$.

For clarity, we also repeat previous definitions.

Definition 6.3 (conditions **C**). We say that $x \in \mathbb{O}_L$ *satisfies* **C** if $x \equiv a\,\mathrm{Tr}(w) \bmod 2\mathbb{O}_L$, $x^2 - dd'$ is totally negative, and $(x^2 - dd')/4pl^2 \in \mathbb{O}_L$.

Definition 6.4. We write $\lambda_{\epsilon(\mathfrak{a})}$ to emphasize the dependence of λ on the choice of signs. For example, for $\mathfrak{a} \lhd \mathbb{O}_K$, let $\lambda_{\mathfrak{a}} = \lambda_{\varepsilon(\mathfrak{a})}$, where $\varepsilon(\mathfrak{a}, \mathfrak{q}) = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})}$ and $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ is an ideal such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$.

Theorem 6.5.

(1)
$$\sum_{\varepsilon(\mathfrak{a})} \#S(\mathfrak{a}, \lambda_{\varepsilon(\mathfrak{a})}, l) = \sum_{x \text{ satisfies } \mathbf{C}} \delta(x) \cdot \#S_1(\mathfrak{a}, x, l)$$
$$= w_K \sum_{x \text{ satisfies } \mathbf{C}} \delta(x) \cdot \#S_2(\mathfrak{a}, x, l).$$

(2)
$$\sum_{\varepsilon(\mathfrak{a})} \#S(\mathfrak{a}, \lambda_{\varepsilon(\mathfrak{a})}, l) = \sum_{\substack{\mathfrak{c} | d \\ \mathfrak{c} \lhd \mathbb{O}_K}} \#S(\mathfrak{a}\mathfrak{c}, \lambda_{\mathfrak{a}\mathfrak{c}}, l).$$

Proof. To avoid confusion, we remark that in (1), the first summation is a sum over 2^τ elements, one of them being $\#S(\mathfrak{a}, \lambda_{\mathfrak{a}}, l)$. The second equality of (1) follows from Proposition 6.1. To prove the first equality in (1), we refer to the construction given above of the map $\phi : S(\mathfrak{a}, \lambda, l) \to S_1(\mathfrak{a}, x, l)$. It can be extended to a map

$$\phi : \coprod_{\varepsilon(\mathfrak{a})} S(\mathfrak{a}, \lambda_{\varepsilon(\mathfrak{a})}, l) \to \coprod_{x \text{ satisfies } \mathbf{C}} S_1(\mathfrak{a}, x, l).$$

We claim that ϕ is a surjective map that is $[\delta(x) : 1]$. Given an element γ of $S_1(\mathfrak{a}, x, l)$, we constructed above, for some possible choice of signs $\epsilon(\mathfrak{a})$ determining

λ, an element of $S(\mathfrak{a}, \lambda, l)$

$$\alpha = \frac{x + \mathrm{Tr}(w)\sqrt{d}}{2\sqrt{d}} \quad \text{and} \quad \beta = \frac{l}{\sqrt{d}}\gamma.$$

For any ideal $\tilde{\mathfrak{q}} \mid d$, let $\mu(x, \gamma) \in \{\pm 1\}$ be such that $\alpha_1 \equiv \mu(x, \gamma)\beta_1 \bmod \tilde{\mathfrak{q}}$, where $\alpha_1 = \sqrt{d}\alpha$ and $\beta_1 = \sqrt{d}\lambda\beta$. Given $\varepsilon(\mathfrak{a})$, we have $\alpha \equiv \lambda_{\varepsilon(\mathfrak{a})}\beta \bmod \mathbb{O}_K$ if and only if, for all $\tilde{\mathfrak{q}} \mid d$, either $\alpha_1 \equiv \beta_1 \equiv 0 \bmod \tilde{\mathfrak{q}}$ or $\beta_1 \not\equiv 0 \bmod \tilde{\mathfrak{q}}$ and $\varepsilon(\mathfrak{a}, \mathfrak{q}) \equiv \mu(x, \gamma) \bmod \tilde{\mathfrak{q}}$. It follows that for a given (x, γ), the number of sign vectors $\varepsilon(\mathfrak{a})$ such that we have $\alpha \equiv \lambda_{\varepsilon(\mathfrak{a})}\beta \bmod \mathbb{O}_K$ is equal to

$$2^{\#\{\tilde{\mathfrak{q}} \mid d : \sqrt{d}\alpha \equiv 0 \bmod \tilde{\mathfrak{q}}\}}.$$

Now since $\mathrm{val}_{\tilde{\mathfrak{q}}}(\sqrt{d}\alpha) = \mathrm{val}_{\tilde{\mathfrak{q}}}(x + \mathrm{Tr}(w)\sqrt{d}) \geq \min\{\mathrm{val}_{\tilde{\mathfrak{q}}}(x), \mathrm{val}_{\tilde{\mathfrak{q}}}(\mathrm{Tr}(w)\sqrt{d})\}$, it follows that

$$\mathrm{val}_{\tilde{\mathfrak{q}}}(\sqrt{d}\alpha) > 0 \iff \mathrm{val}_{\tilde{\mathfrak{q}}}(x) > 0 \iff \mathrm{val}_{\tilde{\mathfrak{q}}}(x) > 0,$$

so the number of sign vectors $\varepsilon(\mathfrak{a})$ such that $\alpha \equiv \lambda_{\varepsilon(\mathfrak{a})}\beta \bmod \mathbb{O}_K$ is equal to $2^{\#\{\mathfrak{q} \mid d : x \equiv 0 \bmod \mathfrak{q}\}}$.

The second assertion in the theorem follows from the same argument given in the proof of Lemma 5.2. □

7. Endomorphism rings of abelian surfaces with complex multiplication

Let K be a primitive CM field of degree 4 over the rational numbers. Let $W = W(\bar{\mathbb{F}}_p)$ be the Witt ring, and let

$$(A, \iota : \mathbb{O}_K \to \mathrm{End}_W(A))$$

be an abelian scheme over W of relative dimension 2 such that $A \pmod p$ is superspecial. Assume also that p is unramified in K. Then $R := \mathrm{End}_{\mathbb{O}_L}(A \pmod p)$ is a superspecial order of the quaternion algebra $B_{p,L}$ [Nicole 2008, Proposition 4.1].

Theorem 7.1. *One has*

$$\mathrm{End}_{\mathbb{O}_L, W/(p^n)}(A \pmod{p^n}) = \mathbb{O}_K + p^{n-1}R.$$

This theorem is a generalization of a theorem of Gross that deals with the case of elliptic curves [1986], but our method of proof is different; it is based on crystalline deformation theory.

Proof. Consider $A \pmod{p^n}$. We have an identification

$$\mathbb{H}^1_{dR}(A \pmod{p^n}) \cong H^1_{\mathrm{Crys}}(A \pmod p / W) \otimes W/(p^n).$$

Using that $W/(p^{n+1}) \to W/(p^n)$ has canonical divided power structure, we know the deformations of $A \pmod{p^n}$ to an abelian scheme B over $W/(p^{n+1})$ are in functorial correspondence with direct summands of $H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^{n+1})$ such that the following diagram commutes:

$$\begin{array}{ccc} M & \subseteq & H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^{n+1}) \\ \downarrow{\scriptstyle \bmod p^n} & & \downarrow{\scriptstyle \bmod p^n} \\ \underline{\omega}_{A \pmod{p^n}} & \subseteq & H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^n) \end{array}$$

where $\underline{\omega}_{A \pmod{p^n}}$ are the relative differentials at the origin of $A \pmod{p^n}$.

We shall show that there exists a unique such B to which the $\mathbb{O}_K$-action extends, namely, a unique M fixed under the $\mathbb{O}_K$ action on $H^1_{\mathrm{Crys}}(A \pmod p/W)$. We may conclude then that for that M there is an isomorphism

$$\begin{aligned}\mathrm{End}_{\mathbb{O}_L}(A \pmod{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathbb{O}_L}\left(M \subset H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^{n+1})\right) \\ \cap \mathrm{End}_{\mathbb{O}_L}(A \pmod{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p. \quad (7\text{-}1)\end{aligned}$$

We then calculate the right-hand side and find that it is equal to $(\mathbb{O}_K + p^n R) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Since we know a priori that $\mathrm{End}_{\mathbb{O}_L}(A \pmod{p^{n+1}})$ has index equal to a power of p in R [Goren and Lauter 2012, Proposition 6.1], our theorem will follow.

First, the uniqueness of M is easy to establish. We have an isomorphism of $\mathbb{O}_K \otimes_{\mathbb{Z}} W$ modules

$$H^1_{\mathrm{Crys}}(A \pmod p/W) \cong \bigoplus_{\varphi \in \mathrm{Emb}(\mathbb{O}_K, W)} W(\varphi),$$

where $W(\varphi)$ is just W with the $\mathbb{O}_K$ action given by φ. Since p is unramified, for all $n \geq 1$, $W(\varphi) \ncong W(\varphi') \pmod{p^n}$ as $\mathbb{O}_K$-modules for any distinct $\varphi, \varphi' \in \mathrm{Emb}(\mathbb{O}_K, W)$. If Φ is the CM-type of A, it follows that if M is a direct summand of rank g, which is an $\mathbb{O}_K$-submodule, then M must be $\bigoplus_{\varphi \in \Phi} W(\varphi) \pmod{p^{n+1}}$.

Let $R_n := \mathrm{End}_{\mathbb{O}_L, W/(p^n)}(A \pmod{p^n})$. We prove by induction on n that

$$R_n = \mathbb{O}_K + p^{n-1} R.$$

As remarked, it is enough to prove that after p-adic completion, and in fact, we actually calculate the right-hand side of (7-1). The case $n = 1$ is tautological.

Since we assumed that $A \pmod p$ is superspecial and p is unramified in K, there are, according to [Goren and Lauter 2012, Tables 3.3.1(ii), 3.4.1(iii) and (iv), and 3.5.1(iii) and (vi)] and the results of Yu [2004], precisely two possibilities for $H^1_{\mathrm{Crys}}(A \pmod p/W)$, equivalently for the Dieudonné module of $A \pmod p$, as an $\mathbb{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module. Our calculations are done separately according to these cases.

Case 1: In this case, the completions at p of the rings are

$$\mathcal{O}_{L,p} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \quad \text{and} \quad \mathcal{O}_{K,p} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2},$$

where we write $\mathbb{Z}_{p^2}$ for $W(\mathbb{F}_{p^2})$. The Dieudonné module $\mathbb{D}$ is a direct sum of Dieudonné modules

$$\mathbb{D} = \mathbb{D}_1 \oplus \mathbb{D}_2,$$

where for $i = 1, 2$, $\mathbb{D}_i$ has a basis relative to which Frobenius is given by the matrix

$$\begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix},$$

and the ith copy of $\mathbb{Z}_{p^2}$ in $\mathcal{O}_{K,p}$ acts on $\mathbb{D}_i$ by

$$a \mapsto \begin{pmatrix} a & \\ & a^\sigma \end{pmatrix}$$

and $\mathbb{D}_{i+1 \pmod 2}$ by zero. (Here σ is the Frobenius automorphism of $\mathbb{Z}_{p^2}$.) Clearly,

$$\mathrm{End}_{\mathcal{O}_L}(\mathbb{D}) = \mathrm{End}(\mathbb{D}_1) \times \mathrm{End}(\mathbb{D}_2),$$

and, as one can easily check,

$$\mathrm{End}(\mathbb{D}_i) = \left\{ \begin{pmatrix} \alpha & p\beta \\ \beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in W(\mathbb{F}_{p^2}) \right\}.$$

(The restriction on the entries $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ comes from the identity

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^\sigma & b^\sigma \\ c^\sigma & d^\sigma \end{pmatrix}$$

that an endomorphism of the Dieudonné module must satisfy.)

Now, for every n, $\underline{\omega}_{A \pmod{p^n}} = \mathrm{Span}_{W/(p^n)}\{(0\ \ 1)^{\mathrm{T}}\} \oplus \mathrm{Span}_{W/(p^n)}\{(0\ \ 1)^{\mathrm{T}}\}$ in the decomposition $\mathbb{D} = \mathbb{D}_1 \oplus \mathbb{D}_2$. By induction, the endomorphisms in $\mathrm{End}_{\mathcal{O}_L}(\mathbb{D})$ preserving $\underline{\omega}_{A \pmod{p^n}}$ are

$$(\mathcal{O}_K + p^{n-1}R) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \left\{ \left(\begin{pmatrix} \alpha & p^n\beta \\ p^{n-1}\beta^\sigma & \alpha^\sigma \end{pmatrix}, \begin{pmatrix} \gamma & p^n\delta \\ p^{n-1}\delta^\sigma & \gamma^\sigma \end{pmatrix} \right) : \alpha, \beta, \gamma, \delta \in W(\mathbb{F}_{p^2}) \right\}.$$

The condition for such an endomorphism to preserve $\underline{\omega}_{A \pmod{p^{n+1}}}$ is that the vectors

$$\begin{pmatrix} \alpha & p^n\beta \\ p^{n-1}\beta^\sigma & \alpha^\sigma \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \gamma & p^n\delta \\ p^{n-1}\delta^\sigma & \gamma^\sigma \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

are multiples of $(0\ \ 1)^{\mathrm{T}}$ modulo p^{n+1}. This is the case precisely when β and δ, respectively, are in pW. Thus, $\mathrm{End}(A \pmod{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p = (\mathbb{O}_K + p^n R) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and the proof is complete in Case 1.

Case 2: In this case, the completions at p of the rings are

$$\mathbb{O}_{L,p} \cong \mathbb{Z}_{p^2} \quad \text{and} \quad \mathbb{O}_{K,p} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2},$$

where $\mathbb{Z}_{p^2}$ is embedded diagonally in $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$. The Dieudonné module has a basis $\{e_1, e_2, e_3, e_4\}$ relative to which

$$\mathrm{Fr} = \begin{pmatrix} 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \end{pmatrix}.$$

The element $(a, b) \in \mathbb{O}_{K,p}$ acts by the diagonal matrix $\mathrm{diag}(a, b, a^\sigma, b^\sigma)$, and so $a \in \mathbb{O}_{L,p}$ acts by $\mathrm{diag}(a, a, a^\sigma, a^\sigma)$. Change the order of the basis elements to get a new basis $\{e_1, e_4, e_3, e_2\}$. Then Frobenius is given by

$$\begin{pmatrix} 0 & pI_2 \\ I_2 & 0 \end{pmatrix},$$

and $(a, b) \in \mathbb{O}_{K,p}$ acts by the diagonal matrix $\mathrm{diag}(a, b^\sigma, a^\sigma, b)$, and so $a \in \mathbb{O}_{L,p}$ acts by $\mathrm{diag}(a, a^\sigma, a^\sigma, a)$.

The condition for a matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_4(W)$$

to be in $\mathrm{End}(\mathbb{D})$ is

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & pI_2 \\ I_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & pI_2 \\ I_2 & 0 \end{pmatrix} \begin{pmatrix} A^\sigma & B^\sigma \\ C^\sigma & D^\sigma \end{pmatrix},$$

and so we find

$$\mathrm{End}(\mathbb{D}) = \left\{ \begin{pmatrix} A & pC^\sigma \\ C & A^\sigma \end{pmatrix} : A, C \in M_2(W(\mathbb{F}_{p^2})) \right\}.$$

For such a matrix to be in $\mathrm{End}_{\mathbb{O}_L}(\mathbb{D})$, it must commute with all matrices of the form $\mathrm{diag}(a, a^\sigma, a^\sigma, a)$, where a runs over $W(\mathbb{F}_{p^2})$. An easy computation gives

$$\mathrm{End}_{\mathbb{O}_L}(\mathbb{D}) = \left\{ \begin{pmatrix} A & pC^\sigma \\ C & A^\sigma \end{pmatrix} : \text{diagonal matrices } A, C \in M_2(W(\mathbb{F}_{p^2})) \right\}.$$

We have $\underline{\omega}_{A \pmod{p^n}} = \mathrm{Span}\{e_3, e_2\}$, where e_3 and e_2 are the last two vectors in the current basis. One argues by induction, as before, to prove that the endomorphisms

in $\mathrm{End}_{\mathcal{O}_L}(\mathbb{D})$ preserving $\underline{\omega}_{A\ (\mathrm{mod}\ p^n)}$ are precisely those of the form

$$\left\{\begin{pmatrix} A & p^n C^\sigma \\ p^{n-1}C & A^\sigma \end{pmatrix} : \text{diagonal matrices } A, C \in M_2(W(\mathbb{F}_{p^2}))\right\} \cong (\mathcal{O}_K + p^{n-1}R) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

That completes the proof of Case 2 and hence of the theorem. □

8. Geometric interpretation

Let $W := W(\bar{\mathbb{F}}_p)$ and $Q := W \otimes_{\mathbb{Z}} \mathbb{Q}$; Q is the completion of the maximal unramified extension of $\mathbb{Q}_p$. Assume that p is unramified in K, and consider the functor on W-schemes associating to a W-scheme S the isomorphism classes of triples

$$\underline{A} = (A, \iota, \eta), \tag{8-1}$$

where $A \to S$ is an abelian scheme of relative dimension g, $\iota : \mathcal{O}_K \to \mathrm{End}_S(A)$ is a ring homomorphism, and η is a principal polarization of A inducing complex conjugation on K. Arguments as in [Goren and Lauter 2007] show that this functor is represented by an étale scheme over W whose complex points are in natural bijection with $\mathcal{F} \times \mathrm{Cl}(K)$ as described in Proposition 2.4. In particular, isomorphism classes of $\underline{A}$ over $\bar{\mathbb{F}}_p$ as in (8-1), or more generally of $\underline{A}$ over $W/(p^n)$, are also in bijection with $(\mathcal{F} \times \mathrm{Cl}(K))/\sim$ once we have fixed an identification of $\mathrm{Hom}(K, \mathbb{C})$ with $\mathrm{Hom}(K, \bar{\mathbb{Q}}_p)$. This allows us to speak about the CM type of A over $W/(p^n)$. Of course, this is nothing but the isomorphism class of the representation of $\mathcal{O}_K$ on the Lie algebra of A and is determined by its reduction modulo p.

Consider pairs (A, ι) over $\bar{\mathbb{F}}_p$ such that A is a g-dimensional abelian variety and $\iota : \mathcal{O}_K \to \mathrm{End}(A)$ is a ring homomorphism such that $(A, \iota|_{\mathcal{O}_L})$ satisfies the Rapoport condition. One knows that there exists a principal $\mathcal{O}_L$-polarization η on A, unique up to isomorphism. We claim that η automatically induces complex conjugation on K. This can be verified by case-by-case analysis using [Chai 1995, Lemma 6].

8.1. ***Isomorphisms of CM abelian varieties.*** Now fix a CM field K' whose totally real subfield is L. Consider $(A, \iota_A : \mathcal{O}_K \to \mathrm{End}(A))$ and $(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}(A'))$ over $\bar{\mathbb{F}}_p$, and assume that we are given an isomorphism

$$\alpha : (A, \iota_A|_{\mathcal{O}_L}) \xrightarrow{\sim} (A', \iota_{A'}|_{\mathcal{O}_L}).$$

We then get an embedding

$$j_\alpha : \mathcal{O}_{K'} \to \mathrm{End}(A), \quad j_\alpha(r) = \alpha^{-1} \circ \iota_{A'}(r) \circ \alpha.$$

If $\beta : (A, \iota_A|_{\mathcal{O}_L}) \xrightarrow{\sim} (A', \iota_{A'}|_{\mathcal{O}_L})$ is another isomorphism, then

$$\beta = \gamma \circ \alpha,$$

where

$$\gamma \in \mathrm{Aut}(A', \iota_{A'}|_{\mathcal{O}_L}) \quad \text{and} \quad j_\beta(r) = \alpha^{-1} \circ \gamma^{-1} \circ \iota_{A'}(r) \circ \gamma \circ \alpha.$$

This gives another embedding of $\mathcal{O}_{K'}$ into $\mathrm{End}(A)$. The embeddings are equal if and only if $\gamma^{-1} \circ \iota_{A'}(r) \circ \gamma = \iota_{A'}(r)$ for all $r \in \mathcal{O}_{K'}$. This, in turn is equivalent to $\gamma \in \mathrm{Cent}_{\mathrm{End}^0(A')}(K') \cap \mathrm{Aut}((A', \iota_{A'}|_{\mathcal{O}_L})) = \mathcal{O}_{K'}^\times$. (Here $\mathrm{Cent}_{\mathrm{End}^0(A')}(K')$ denotes the centralizer of K' in $\mathrm{End}^0(A')$.) Thus, each isomorphism class of $(A', \iota_{A'})$ such that $(A, \iota_A|_{\mathcal{O}_L}) \cong (A', \iota_{A'}|_{\mathcal{O}_L})$ gives us

$$\#(\mathrm{Aut}((A', \iota_{A'}|_{\mathcal{O}_L}))/\mathcal{O}_{K'}^\times) = \#(\mathrm{Aut}((A, \iota_A|_{\mathcal{O}_L}))/\mathcal{O}_{K'}^\times)$$

distinct embeddings of $\mathcal{O}_{K'}$ into $\mathrm{End}(A)$.

8.2. ***Counting isomorphisms in the superspecial case.*** Now assume we are in the superspecial reduction situation, and fix an isomorphism

$$\mathrm{End}_{\mathcal{O}_L}(A) \cong R(\mathfrak{a}, \lambda_\mathfrak{a})$$

for some unique $\mathfrak{a} \lhd \mathcal{O}_K$ (Lemma 5.6 and Theorem 5.7). With $\mathcal{O}_{K'} = \mathcal{O}_L[\omega]$ as before, to give an embedding $\mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A)$ is to choose an element $[\alpha, \beta] \in R(\mathfrak{a}, \lambda_\mathfrak{a})$ with trace equal to $\mathrm{Tr}(\omega)$ and norm equal to $\mathrm{Norm}(\omega)$, that is, an element of the set $S(\mathfrak{a}, \lambda_\mathfrak{a}, 1)$. Such an embedding makes $(A, \iota_A|_{\mathcal{O}_L})$ into an abelian variety with CM by $\mathcal{O}_{K'}$, and so the embedding $\mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A)$ arises via a particular isomorphism

$$(A, \iota_A : \mathcal{O}_K \to \mathrm{End}(A)) \xrightarrow{\sim} (A', \iota' : \mathcal{O}_{K'} \to \mathrm{End}(A'))$$

(where, in fact, we may take $A = A'$ and ι' restricts to ι_A on $\mathcal{O}_L$). We conclude that

$$\frac{\#S(\mathfrak{a}, \lambda_\mathfrak{a}, 1)}{\#(R(\mathfrak{a}, \lambda_\mathfrak{a})^\times/\mathcal{O}_{K'}^\times)} = \#\left\{(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A'))/\overline{\mathbb{F}}_p : (A', \iota_{A'}|_{\mathcal{O}_L}) \xrightarrow{\sim} (A, \iota_A|_{\mathcal{O}_L})\right\}$$

(where on the left-hand side we consider $(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A'))$ up to isomorphism with CM by $\mathcal{O}_{K'}$, of course). Exactly the same analysis is valid over $W/(p^n)$, and using $\mathrm{End}_{W/(p^n)}(A, \iota|_{\mathcal{O}_L}) \cong R(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1})$ as follows from Theorem 7.1, we get

$$\frac{\#S(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1})}{\#(R(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1})^\times/\mathcal{O}_{K'}^\times)}$$
$$= \#\left\{(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A'))/W/(p^n) : (A', \iota_{A'}|_{\mathcal{O}_L}) \xrightarrow{\sim} (A, \iota_A|_{\mathcal{O}_L})\right\}. \quad (8\text{-}2)$$

8.3. ***Counting formulas for the number of isomorphisms for superspecial CM types.*** Now fix a superspecial CM type Φ of K, namely, a CM type arising for some superspecial abelian variety. By [Goren and Lauter 2012], then any abelian variety with CM by $\mathcal{O}_K$ of CM type Φ is superspecial.

We consider representatives $\underline{A} = (A, \iota_A : \mathbb{O}_K \to \mathrm{End}(A))$ for the isomorphism classes with CM type Φ. For each such $\underline{A}$, we may choose an isomorphism

$$f_{\underline{A}} : \mathrm{End}_L^0(\underline{A}) \xrightarrow{\sim} B_{p,L}$$

and hence get an embedding

$$f_{\underline{A}} \circ \iota_A : K \to B_{p,L}.$$

By Skolem–Noether, we may conjugate the identifications $f_{\underline{A}}$ so that the embeddings $f_{\underline{A}} \circ \iota_A$ are *the same*, and in fact, this will be the case if $f_{\underline{A}_1}$ and $f_{\underline{A}_2}$ are related by a CM isogeny to begin with. Then for every $\underline{A}$, $f_{\underline{A}}(\mathrm{End}_{\mathbb{O}_L}(\underline{A}))$ is a superspecial order containing $\mathbb{O}_K$. This order is uniquely determined by $\underline{A}$ up to conjugation by $K^\times$.

By our results, the representatives for these orders modulo conjugation by $K^\times$ are precisely the orders $R(\mathfrak{a}, \lambda_\mathfrak{a})$ as $\mathfrak{a}$ ranges over representatives for $\mathrm{Cl}(\mathbb{O}_K)$. We therefore conclude:

Theorem 8.1. *We have* (*where, of course, the* $\underline{A}'$ *are taken up to isomorphism*)

$$\sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1}) = \sum_{\substack{\underline{A}/(W/(p^n)) \\ \text{with CM type } \Phi}} \#\left(\frac{\mathrm{End}_{\mathbb{O}_L, W/(p^n)}(\underline{A})^\times}{\mathbb{O}_{K'}^\times}\right) \cdot \#\left\{\begin{array}{c}\underline{A}' \text{ with CM by } \mathbb{O}_{K'} \text{ such that} \\ (A', \iota_{A'}|_{\mathbb{O}_L}) \cong (A, \iota_A|_{\mathbb{O}_L})\end{array}\right\}. \quad (8\text{-}3)$$

If we wish not to fix a CM type on K, we get the following:

Theorem 8.2. *We have*

$$\#\{\text{superspecial CM types}\} \times \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1}) = \sum_{\substack{\underline{A}/(W/(p^n)) \\ \text{with CM by } \mathbb{O}_K}} \#\left(\frac{\mathrm{End}_{\mathbb{O}_L, W/(p^n)}(\underline{A})^\times}{\mathbb{O}_{K'}^\times}\right) \cdot \#\left\{\begin{array}{c}\underline{A}' \text{ with CM by } \mathbb{O}_{K'} \text{ such that} \\ (A', \iota_{A'}|_{\mathbb{O}_L}) \cong (A, \iota_A|_{\mathbb{O}_L})\end{array}\right\}. \quad (8\text{-}4)$$

8.4. ***Counting formulas for pairs of embeddings into superspecial orders.*** The left-hand side of (8-3), for $n = 1$, has another interpretation. Consider a pair of embeddings $\iota : \mathbb{O}_K \to R$ and $\iota' : \mathbb{O}_{K'} \to R$ into a superspecial order R such that both restrict to a fixed, given embedding of $\mathbb{O}_L$ into R. We call it an optimal triple (ι, ι', R). We say that (ι, ι', R) is conjugate to $(j, j', \tilde{R})$ if there exists $t \in B_{p,L}^\times$ such that $t^{-1}Rt = \tilde{R}$ and $t^{-1}\iota(x)t = j(x)$ for all $x \in {\mathbb{O}_K}^\times$ and $t^{-1}\iota'(x)t = j'(x)$ for all $x \in \mathbb{O}_{K'}^\times$.

To count the number of conjugacy classes of optimal triples, let us fix an embedding $I : K \to B_{p,L}$. Then any optimal triple is conjugate to $(I|_{\mathbb{O}_K}, \iota', R)$, where R is a superspecial order containing $I(\mathbb{O}_K)$. We may still conjugate by $K^\times$ and so assume that $R = R(\mathfrak{a}, \lambda_\mathfrak{a})$ for some $\mathfrak{a}$. We may still conjugate by ${\mathbb{O}_K}^\times$, and if $K \neq K'$, that

induces a faithful action of $\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times$ on the embeddings $\iota' : \mathcal{O}_{K'} \to R(\mathfrak{a}, \lambda_\mathfrak{a})$ if they exist at all. We conclude that

$$\#(\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times)^{-1} \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, 1) = \#\{\text{optimal triples up to conjugation}\}.$$

Corollary 8.3. *The number of optimal triples up to conjugation equals*

$$\begin{aligned}
&\#(\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times)^{-1} \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, 1) \\
&= \sum_{\substack{\underline{A}/(W/(p^n)) \\ \text{with CM type } \Phi}} \#(\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times)^{-1} \#(\mathcal{O}_{K'}^\times/\mathcal{O}_L{}^\times)^{-1} \#\left(\frac{\mathrm{End}_{\mathcal{O}_L, W/(p^n)}(\underline{A})^\times}{\mathcal{O}_L^\times}\right) \\
&\qquad \times \#\left\{ \begin{array}{c} \underline{A}' \text{ with CM by } \mathcal{O}_{K'} \text{ such that} \\ (A', \iota_{A'}|_{\mathcal{O}_L}) \cong (A, \iota_A|_{\mathcal{O}_L}) \end{array} \right\}. \qquad (8\text{-}5)
\end{aligned}$$

If we multiply the whole set of equalities (8-5) above by the number of superspecial types for K, we may be justified in calling the new right-hand side of (8-5) the "coincidence number of K and K' at p" as it counts the number of coincidences between abelian varieties with CM by K and abelian varieties with CM by K' in characteristic p once one considers them as abelian varieties with RM only.

9. The connection to moduli spaces

In their paper [1985], Gross and Zagier give a beautiful formula. Let E_1 and E_2 be two elliptic curves over $W = W(\bar{\mathbb{F}}_p)$. Let j_i be the j-invariant of E_i. Their formula is

$$\mathrm{val}_p(j_1 - j_2) = \frac{1}{2} \sum_{n \geq 1} \#\,\mathrm{Isom}_n(E_1, E_2),$$

where Isom_n denotes the isomorphisms between the reduction of E_i modulo (p^n).

The proof Gross and Zagier provided is through direct manipulations of Weierstrass equations. A more conceptual proof was given by Brian Conrad in [2004]. The proof makes essential use of moduli spaces but uses many features unique to modular curves and hence is not readily amenable to generalization. This result is the basis of interpreting their theorem on $J(d, d')$ and $\mathrm{ord}_\lambda(J(d, d'))$ (cf. Section 1) as an arithmetic intersection number. It thus remains a question of how to give an interpretation for our theorems, Theorem 8.2 for example, as an intersection number of CM points on Shimura varieties.

One possibility is to use Shimura curves associated with quaternion algebras over totally real fields split at exactly one infinite prime. This approach entails using the p-adic, not-quite-canonical models for these Shimura curves, following Morita, Carayol, and Boutot–Carayol. The other possibility is to view these CM 0-cycles as lying on a Hilbert modular variety. This approach is complicated by the

fact that there is no "robust" definition of the arithmetic intersection of 0-cycles (1-cycles on the arithmetic models) once their codimension is bigger than 1. This calls for an ad-hoc approach, and it has its own challenging problems.

For now, we will replace the notion of an intersection number with something less precise and define instead a *coincidence number*, which does not reflect the power to which various primes may appear in the differences of invariants but at least reflects whether a prime appears in the factorizations of the differences of invariants. In Section 12, we will give an example to illustrate the coincidence number in computations.

Let L be a totally real field with strict class number 1 and K_i with $i = 1, 2$ two CM fields containing L as their maximal totally real subfield. Let p be a prime unramified in both K_1 and K_2. For each CM field, we can associate a 0-cycle $\mathrm{CM}(K_i)$ on the generic fiber of the Hilbert modular variety $\mathscr{H}_L$ parametrizing principally polarized abelian varieties with RM by $\mathbb{O}_L$ (Section 2.3). Each point x_η in $\mathrm{CM}(K_i)$ can be extended to a $W(\bar{\mathbb{F}}_p)$-point x on $\mathscr{H}_L$ [Goren and Lauter 2012, Lemma 2.3]. This implicitly depends on a choice of a prime $\mathfrak{p}$ in a common field of definition for all the CM abelian varieties under consideration. We write $\mathrm{CM}(K_1) = \sum_i x_i$ and $\mathrm{CM}(K_2) = \sum_j y_j$. We then define the arithmetic *coincidence number* (for lack of better terminology) of $\mathrm{CM}(K_1)$ and $\mathrm{CM}(K_2)$ as

$$\mathrm{CM}(K_1) \wedge \mathrm{CM}(K_2) = \sum_{ij} x_i \wedge y_j,$$

where $x_i \wedge y_j$ is defined as 1 if x_i and y_j have isomorphic reduction modulo p and as 0 otherwise. In this notation, Theorem 8.2 implies the following:

Corollary 9.1. *The contribution from a prime p of superspecial reduction to $\mathrm{CM}(K_1) \wedge \mathrm{CM}(K_2)$ is equal to $\#\{\text{superspecial CM types}\} \times \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_{\mathfrak{a}}, 1)$.*[1] *This number, and in particular whether it is zero, can be effectively calculated.*

10. Supersingular orders

Theorem 10.1. *Let p be a rational prime and k an algebraically closed field of characteristic p. Let K be a quartic CM field, and let $L = K^+$ be its real subfield. Let A/k be an abelian surface that is supersingular, but not superspecial, with complex multiplication by $\mathbb{O}_K$. Let $\mathbb{O} := \mathrm{End}_{\mathbb{O}_L}(A)$, where the endomorphisms are over k. Let $B_{p,\infty}$ be the quaternion algebra over $\mathbb{Q}$ ramified at only p and ∞, and let $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$. Then $\mathbb{O}$ is an Eichler order of $B_{p,L}$ of discriminant p^2.*

Proof. Let H be a quaternion algebra over a number field F, and let R be an order of H containing $\mathbb{O}_F$. Recall that R is called an Eichler order if it is the intersection of two maximal orders. This is a local property [Vignéras 1980, p. 84]. If F denotes

[1] Likewise, the notion of superspecial CM types depends on the implicit choice of $\mathfrak{p}$.

now a nonarchimedean local field with uniformizer π, then an order of H containing $\mathcal{O}_F$ is Eichler (namely, is the intersection of two maximal orders of H) if and only if it is conjugate to the order

$$M = \begin{pmatrix} \mathcal{O}_F & \mathcal{O}_F \\ \pi^n \mathcal{O}_F & \mathcal{O}_F \end{pmatrix}$$

for some positive integer n [Vignéras 1980, p. 39].

We wish to find the completion of $\mathcal{O}$ at every rational prime ideal $\mathfrak{l}$ of $\mathcal{O}_L$.

First, since there exists an isogeny of degree a power of p between any two supersingular abelian surfaces A and A' with real multiplication respecting the real multiplication structure [Bachmat and Goren 1999], for $\mathfrak{l} \nmid p$, we have that $\mathcal{O}_\mathfrak{l} := \mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O}_{L,\mathfrak{l}} \cong \mathcal{O}'_\mathfrak{l}$, where $\mathcal{O}' = \mathrm{End}_{\mathcal{O}_L}(A')$. We may choose for A' the surface $E \otimes_\mathbb{Z} \mathcal{O}_L$, where E is a supersingular elliptic curve with $R = \mathrm{End}(E)$ a maximal order in $B_{p,\infty}$. Then $\mathcal{O}' = \mathrm{End}(A') = R \otimes_\mathbb{Z} \mathcal{O}_L$, so $\mathcal{O}'$ and $\mathcal{O}$ are maximal orders at $\mathfrak{l}$.

We remark that according to the classification of the reduction of abelian surfaces with CM, the situation we consider occurs if and only if p is inert in K, that is, in the following cases:

(a) $K/\mathbb{Q}$ is cyclic Galois and p inert in K [Goren and Lauter 2012, Table 3, case (iii)], and

(b) $K/\mathbb{Q}$ is non-Galois and p inert in K [Goren and Lauter 2012, Table 5, case (vii)].

Following the conventions of [Goren and Lauter 2012], the Dieudonné module of the p-divisible group of the reduction of A modulo $\mathfrak{p}_L$ is

$$\mathbb{D} \cong \mathbb{W}(1) \oplus \mathbb{W}(y^2) \oplus \mathbb{W}(y) \oplus \mathbb{W}(y^3),$$

where $\mathbb{W}(\alpha)$ denotes the Witt vectors of $\bar{\mathbb{F}}_p$, where $\mathcal{O}_K$ acts through the embedding $\alpha : K \to \bar{\mathbb{Q}}_p$. Let σ denote the Frobenius automorphism of $\mathbb{W}$. Then

(a) $\mathcal{O}_L$ acts on $\mathbb{D}$ by $l \mapsto \mathrm{diag}(l, l, \sigma(l), \sigma(l))$, and

(b) $\mathcal{O}_K$ acts on $\mathbb{D}$ by $k \mapsto \mathrm{diag}(k, \sigma^2(k), \sigma(k), \sigma^3(k))$.

The p-adic CM type is $\{1, y^3\}$ according to our conventions, but since the situation is symmetric, we may assume that the p-adic CM type is $\{1, y\}$, and so Frobenius is given in the standard basis by the matrix

$$\mathrm{Fr} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & p & 0 \\ p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

By a theorem of Tate, $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Z}_p \cong \mathrm{End}(\mathbb{D})$, where on the right the endomorphisms are as Dieudonné modules (cf. [Waterhouse and Milne 1971, Theorem 5]),

namely, in this case, $\mathbb{W}$-linear maps $\mathbb{D} \to \mathbb{D}$ that commute with Frobenius. In the same way,

$$\mathcal{O}_p = \mathrm{End}_{\mathcal{O}_L}(A) \otimes_{\mathcal{O}_L} \mathcal{O}_{L\,p} = \mathrm{End}_{\mathcal{O}_L}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathcal{O}_L}(\mathbb{D}).$$

Since $\mathcal{O}_p$ commutes with $\mathcal{O}_L$, one finds that $\mathcal{O}_p$ is given by block diagonal matrix with blocks of size 2. Writing the general such matrix as

$$M = \begin{pmatrix} m_{11} & m_{12} & & \\ m_{21} & m_{22} & & \\ & & n_{11} & n_{12} \\ & & n_{21} & n_{22} \end{pmatrix},$$

the condition $M \cdot \mathrm{Fr} = \mathrm{Fr} \cdot \sigma(M)$ gives, after a short computation,

$$\mathcal{O}_p = \left\{ \begin{pmatrix} m_{11} & m_{12} & & \\ p^2 m_{12}^{\sigma^2} & m_{11}^{\sigma^2} & & \\ & & m_{11}^{\sigma} & p m_{12}^{\sigma} \\ & & p m_{12}^{\sigma^3} & m_{11}^{\sigma^3} \end{pmatrix} : m_{ij} \in \mathbb{W}(\mathbb{F}_{p^4}) \right\}.$$

Since p is inert in L, the quaternion algebra $B_{p,L}$ is ramified only at the two places at infinity. In particular, $B_{p,L} \otimes_L L_p \cong M_2(\mathbb{Q}_{p^2})$, where $\mathbb{Q}_{p^2} = \mathbb{W}(\mathbb{F}_{p^2}) \otimes_{\mathbb{Z}} \mathbb{Q}$. To determine the nature of $\mathcal{O}_p$, we want to recognize it as a suborder of $M_2(\mathbb{W}(\mathbb{F}_{p^2}))$.

The case $p \neq 2$. Put

$$i := \begin{pmatrix} & 1 \\ p^2 & \end{pmatrix} \quad \text{and} \quad j := \begin{pmatrix} \alpha & \\ & \alpha^{\sigma^2} \end{pmatrix},$$

where α is chosen such that $\mathbb{W}(\mathbb{F}_{p^4}) = \mathbb{W}(\mathbb{F}_{p^2})[\alpha]$ and $\alpha^{\sigma^2} = -\alpha$. We have then

$$i^2 = p^2, \qquad j^2 = \alpha^2, \quad \text{and} \quad k := ij = -ji = \begin{pmatrix} & -\alpha \\ p^2\alpha & \end{pmatrix}.$$

Writing $m_1 = x_1 + y_1\alpha$ and $m_2 = x_2 + y_2\alpha$ with $x_i, y_i \in \mathbb{W}(\mathbb{F}_{p^2})$, we can write

$$\begin{aligned} \begin{pmatrix} m_{11} & m_{12} \\ p^2 m_{12}^{\sigma^2} & m_{11}^{\sigma^2} \end{pmatrix} &= x_1 \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + y_1 \begin{pmatrix} \alpha & \\ & \alpha^{\sigma^2} \end{pmatrix} + x_2 \begin{pmatrix} & 1 \\ p^2 & \end{pmatrix} - y_2 \begin{pmatrix} & -\alpha \\ p^2\alpha & \end{pmatrix} \\ &= x_1 \cdot 1 + y_1 \cdot j + x_2 \cdot i - y_2 \cdot k. \end{aligned}$$

Conversely, for any $x_i, y_i \in \mathbb{W}(\mathbb{F}_{p^2})$, we get an element of $\mathcal{O}_p$. Thus,

$$\mathcal{O}_p = \mathbb{W}(\mathbb{F}_{p^2}) \cdot 1 \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot i \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot j \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot k.$$

Let $I = p^{-1}i$, $J = j$, and $K = IJ = -JI$. Then $I^2 = 1$, $J^2 = \alpha^2$, and $K^2 = -\alpha^2$. The module

$$R = \mathbb{W}(\mathbb{F}_{p^2})[1, I, J, K]$$

is in fact an order of $M_2(\mathbb{Q}_{p^2})$, and it has discriminant 1. It must then be isomorphic to $M_2(\mathbb{W}_{p^2})$, and, indeed, if we send

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \qquad I \mapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \qquad J \mapsto \begin{pmatrix} & \alpha^2 \\ 1 & \end{pmatrix}, \quad \text{and} \quad K \mapsto \begin{pmatrix} & \alpha^2 \\ -1 & \end{pmatrix},$$

we get the isomorphism $R \cong M_2(\mathbb{W}(\mathbb{F}_{p^2}))$. Under this isomorphism, $\mathbb{O}_p$ is mapped isomorphically to the order spanned over $\mathbb{W}(\mathbb{F}_{p^2})$ by the matrices

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \qquad \begin{pmatrix} p & \\ & -p \end{pmatrix}, \qquad \begin{pmatrix} & \alpha^2 \\ 1 & \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} & p\alpha^2 \\ -p & \end{pmatrix},$$

which can be described as

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{W}(\mathbb{F}_{p^2}),\ p \mid (a-d),\ p \mid (b - \alpha^2 c) \right\}.$$

Now conjugate $\mathbb{O}_p$ by the matrix

$$A = \begin{pmatrix} 1 & \alpha \\ \alpha^{-1} & -1 \end{pmatrix}.$$

Using

$$2A^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} A = \begin{pmatrix} a + \alpha^{-1} b + \alpha c + d & \alpha(a-d) + (\alpha^2 c - b) \\ \alpha^{-1}(a-d) + \alpha^{-2}(b - \alpha^2 c) & a - \alpha^{-1} b - \alpha c + d \end{pmatrix},$$

we find that $\mathbb{O}_p$ is conjugate to a suborder of

$$R' = \begin{pmatrix} \mathbb{W}(\mathbb{F}_{p^2}) & p\mathbb{W}(\mathbb{F}_{p^2}) \\ p\mathbb{W}(\mathbb{F}_{p^2}) & \mathbb{W}(\mathbb{F}_{p^2}) \end{pmatrix}.$$

However, comparing the discriminant of $\mathbb{O}_p$, which is p^2, and of R', which is p^2 as well, we conclude that $\mathbb{O}_p$ is isomorphic to R'. Further conjugation by the matrix

$$\begin{pmatrix} & 1/p \\ 1 & \end{pmatrix}$$

shows that $\mathbb{O}_p$ is isomorphic to the order

$$R'' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{W}(\mathbb{F}_{p^2}),\ p^2 \mid c \right\},$$

which is an Eichler order of discriminant p^2.

The case $p = 2$. We may find $\alpha \in \mathbb{W}(\mathbb{F}_{p^2})$ such that $\mathbb{W}(\mathbb{F}_{p^4}) = \mathbb{W}(\mathbb{F}_{p^2})[(1+\alpha)/2]$ and $\alpha^{\sigma^2} = -\alpha$. Indeed, for a suitable $\epsilon \in \mathbb{W}(\mathbb{F}_{p^2})^\times$, we have $\mathbb{W}(\mathbb{F}_{p^4}) = \mathbb{W}(\mathbb{F}_{p^2})[\beta]$, where $\beta^2 + \beta + \epsilon = 0$. Note that β is a unit. Take $\alpha = -(2\beta + 1)$.

To make the analogy with the previous case more visible, we keep using p instead of 2 in most places. As before, we let

$$i = \begin{pmatrix} & 1 \\ p^2 & \end{pmatrix}, \qquad j = \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix}, \quad \text{and} \quad k = ij = -ji = \begin{pmatrix} & -\alpha \\ \alpha p^2 & \end{pmatrix}.$$

Writing $m_1 = x_1 + y_1(1+\alpha)/2$ and $m_2 = x_2 + y_2(1+\alpha)/2$ with $x_i, y_i \in \mathbb{W}(\mathbb{F}_{p^2})$, we can write,

$$\begin{pmatrix} m_{11} & m_{12} \\ p^2 m_{12}^{\sigma^2} & m_{11}^{\sigma^2} \end{pmatrix} = x_1 \cdot 1 + y_1 \cdot \frac{1+j}{2} + x_2 \cdot i + y_2 \cdot \frac{i-k}{2},$$

and one concludes that

$$\mathbb{O}_p = \mathbb{W}(\mathbb{F}_{p^2}) \cdot 1 \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot i \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot \frac{1+j}{2} \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot \frac{i-k}{2}.$$

One can verify directly that the right side is indeed an order and its discriminant is p^2.

The order $\mathbb{O}_p$ contains the order $\mathbb{W}(\mathbb{F}_{p^2})[1, i, j, k] = \mathbb{W}(\mathbb{F}_{p^2})[1, I, J, K]$, where $I = i$, $J = j/\alpha$, and $K = k/\alpha$. Note that $I^2 = p^2$, $J^2 = 1$, $K^2 = -p^2$, and $IJ = -JI = K$. Consider the linear map

$$\mathbb{W}(\mathbb{F}_{p^2})[1, I, J, K] \to M_2(\mathbb{W}(\mathbb{F}_{p^2}))$$

determined by

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \qquad I \mapsto \begin{pmatrix} & 2 \\ 2 & \end{pmatrix}, \qquad J \mapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \quad \text{and} \quad K \mapsto \begin{pmatrix} & -2 \\ 2 & \end{pmatrix}.$$

One checks that this map is a ring homomorphism and verifies that

$$\mathbb{O}_p \cong \mathbb{W}(\mathbb{F}_{p^2})\left[\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} \frac{1+\alpha}{2} & \\ & \frac{1-\alpha}{2} \end{pmatrix}, 2\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, 2\begin{pmatrix} & \frac{1+\alpha}{2} \\ \frac{1-\alpha}{2} & \end{pmatrix}\right].$$

Let $u := (1+\alpha)/(1-\alpha) = \beta^2/\epsilon$. Then u and $1-u = 2+u/\beta$ are units. It follows that

$$\mathbb{O}_p \cong \mathbb{W}(\mathbb{F}_{p^2})\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 2\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 2\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right]$$
$$= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{W}(\mathbb{F}_{p^2}),\ p \mid b,\ p \mid c\right\}.$$

An additional conjugation as in the case $p \neq 2$ shows that this is an Eichler order of discriminant p^2. □

11. A crude version of Gross–Zagier's result on singular moduli

Let A be a g-dimensional abelian variety over a field k. Let L be a totally real field of degree g over $\mathbb{Q}$ of strict class number 1, and let K_i with $i = 1, 2$ be two CM fields contained in some algebraic closure of L such that $K_1^+ = K_2^+ = L$. We allow $K_1 = K_2$. Assume we are given two embeddings

$$\varphi_i : K_i \to \mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$

such that

$$\varphi_1|_L = \varphi_2|_L \quad \text{and} \quad \varphi_1(K) \neq \varphi_2(K).$$

Lemma 11.1. *The field k has positive characteristic p. The abelian variety is supersingular, and $\mathrm{End}^0(A) \cong B_{p,L}$, where $B_{p,L} = B_{p,\infty} \otimes_{\mathbb{Q}} L$ and $B_{p,\infty}$ is "the" quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.*

Proof. This follows easily from the classification of the endomorphism algebras of abelian varieties with real multiplication as in [Chai 1995, Lemma 6]; one observes that under our assumptions, the centralizer of L in $\mathrm{End}_k^0(A)$ is an L-vector space of dimension greater than 2. □

Let $\mathcal{O}_i \subseteq K_i$ be orders containing $\mathcal{O}_L$. The order $\mathcal{O}_i$ is determined by its conductor $\mathfrak{c}_i$, which is an integral ideal of $\mathcal{O}_L$ for which we choose a generator c_i [Goren and Lauter 2009, Lemma 4.1]. In fact, one can write

$$\mathcal{O}_{K_i} = \mathcal{O}_L[\kappa_i],$$

where $-m_i = B_i^2 - 4C_i$ is a totally negative element of $\mathcal{O}_L$ and κ_i satisfies a quadratic equation $x^2 + B_i x + C_i$ for $B_i, C_i \in \mathcal{O}_L$. The relative different ideal $\mathcal{D}_{K_i/L}$ is equal to $\mathcal{O}_{K_i}[1/\sqrt{-m_i}]$ [Goren and Lauter 2006, Lemma 3.1]. We have $\mathcal{O}_{K_i} = \mathcal{O}_L[\kappa_i] \supseteq \mathcal{O}_L[\sqrt{-m_i}] \supseteq \mathcal{O}_L[2\kappa_i]$, and so

$$\mathcal{O}_i = \mathcal{O}_L[c_i\kappa_i] \supseteq \mathcal{O}_L[c_i\sqrt{-m_i}] \supseteq \mathcal{O}_L[2c_i\kappa_i].$$

The discriminant of $\mathcal{O}_i$ relative to $\mathcal{O}_L$, $\mathrm{disc}_{K_i/L}(\mathcal{O}_i)$, is equal to the $\mathcal{O}_L$-ideal generated by $c_i^2 m_i$, and the discriminant of $\mathcal{O}_i$ relative to $\mathbb{Z}$, $\mathrm{disc}(\mathcal{O}_i) = \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_i)$, is equal to $\mathrm{Norm}_{L/\mathbb{Q}}(c_i^2 m_i) \cdot \mathrm{disc}(\mathcal{O}_L)^2$. (In general, we use "disc" to denote absolute discriminant, that is, relative to $\mathbb{Z}$.)

Let B be any totally definite quaternion algebra over L; that is, $B \otimes_{L,\sigma} \mathbb{R}$ is a division algebra for any embedding $\sigma : L \to \mathbb{R}$, and let $\mathfrak{d}$ be its discriminant. Let

$$\varphi_i : K_i \to B$$

be two embeddings such that $\varphi_1|_L = \varphi_2|_L$ and $\varphi_1(K_1) \neq \varphi_2(K_2)$. Let

$$k_i = \varphi_i(c_i\sqrt{-m_i}).$$

Let $\mathbb{O}$ be an order of B, which we assume to contain $\varphi_i(\mathbb{O}_i)$ for $i = 1, 2$ and hence also $\mathbb{O}_L$ (we view φ_i as the identity maps on L). Let $\mathfrak{d}^+$ be the discriminant of $\mathbb{O}$. As in [Goren and Lauter 2007], subject to the assumption $\varphi_1(K_1) \neq \varphi_2(K_2)$, one proves the following lemma:

Lemma 11.2. *The $\mathbb{O}_L$ module $\Lambda = \mathbb{O}_L + \mathbb{O}_L k_1 + \mathbb{O}_L k_2 + \mathbb{O}_L k_1 k_2$ has finite index in $\mathbb{O}$ and is in fact a direct sum $\Lambda = \mathbb{O}_L \oplus \mathbb{O}_L k_1 \oplus \mathbb{O}_L k_2 \oplus \mathbb{O}_L k_1 k_2$.*

Theorem 11.3. *Let $\alpha = \mathrm{Trd}(k_1 k_2)$. We have a divisibility of integral ideals in L:*

$$\mathfrak{d}^+ \mid (4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2) \quad \text{in } \mathbb{O}_L.$$

Furthermore,

$$N_{L/\mathbb{Q}}(\mathfrak{d}^+) \leq 4^g \frac{\mathrm{disc}(\mathbb{O}_1)\cdot\mathrm{disc}(\mathbb{O}_2)}{\mathrm{disc}(\mathbb{O}_L)^4}.$$

Proof. The discriminant of the order Λ relative to L, $\mathrm{disc}_{B/L}(\Lambda)$, is divisible by the discriminant of $\mathbb{O}$; namely, it is an integral ideal of L divisible by $\mathfrak{d}^+$. Using the basis $\{1, k_1, k_2, k_1 k_2\}$ for Λ and putting $\alpha = \mathrm{Trd}(k_1 k_2)$, we find that the discriminant of Λ is the $\mathbb{O}_L$-ideal generated by

$$\det \begin{pmatrix} 2 & 0 & 0 & \alpha \\ 0 & 2\,\mathrm{Nrd}(k_1) & -\alpha & 0 \\ 0 & -\alpha & 2\,\mathrm{Nrd}(k_2) & 0 \\ \alpha & 0 & 0 & 2\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) \end{pmatrix} = (4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2)^2,$$

and so $\mathfrak{d}^+ \mid (4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2)$ in $\mathbb{O}_L$. Thus,

$$N_{L/\mathbb{Q}}(\mathfrak{d}^+) \mid N_{L/\mathbb{Q}}(4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2) \quad \text{in } \mathbb{Z}.$$

Now, $4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2$ is a totally positive element of $\mathbb{O}_L$. Indeed, this is just the Cauchy–Schwartz inequality applied to the bilinear form $\mathrm{Trd}(x\bar{y})$ under every embedding $L \to \mathbb{R}$. We can therefore conclude that

$$N_{L/\mathbb{Q}}(\mathfrak{d}^+) \leq N_{L/\mathbb{Q}}(4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2)).$$

We conclude that

$$\begin{aligned} N_{L/\mathbb{Q}}(\mathfrak{d}^+) &\leq \mathrm{disc}(\mathbb{O}_L)^{-4} 4^{-g} \prod_{i=1}^{2} 4^g\,\mathrm{disc}(\mathbb{O}_L)^2 N_{L/\mathbb{Q}}\,\mathrm{Nrd}(k_i) \\ &\leq \mathrm{disc}(\mathbb{O}_L)^{-4} 4^{-g} \prod_{i=1}^{2} \mathrm{disc}(\mathbb{O}_L[2c_i\kappa_i]) \\ &= \mathrm{disc}(\mathbb{O}_L)^{-4} 4^g \prod_{i=1}^{2} \mathrm{disc}(\mathbb{O}_L[c_i\kappa_i]) = 4^g \frac{\mathrm{disc}(\mathbb{O}_1)\cdot\mathrm{disc}(\mathbb{O}_2)}{\mathrm{disc}(\mathbb{O}_L)^4}. \end{aligned}$$

□

p	Unramified (inert/split)	Inert	Ramified	Ramified
Reduction	ssp	s.sing, not ssp	ssp	ssp
Rapoport?	Yes	Yes	Yes	No
r'	2	4	2	1
Table 3 (K cyclic)	ii, iv, v	iii		vi
Table 4 (K biquadratic)	iii, iv, vii, viii		vi	ix, x, xi
Table 5 (K non-Galois)	iii, vi, viii, ix, x, xi, xiii, xv, xxii, xxiii	vii		xvi, xvii, xviii, xix, xx, xxi, xxiv, xxv, xxvi

Table 1. The case $[L:\mathbb{Q}]=2$. Table numbers refer to [Goren and Lauter 2012]. The column headings refer to the decomposition of p in L. "Reduction" refers to the reduction of the abelian variety modulo $\mathfrak{p}$. The abbreviations "s.sing." and "ssp" mean "supersingular" and "superspecial".

Corollary 11.4. (1) *Let A_i be an abelian variety with CM by $\mathbb{O}_{K_i}$. Choose a common field of definition M for A_1 and A_2 such that M contains the normal closure of both K_1 and K_2 and both A_i have good reduction over M. Let $\mathfrak{p}$ be a prime ideal of M, $(p)=\mathfrak{p}\cap\mathbb{Z}$, and suppose that*

$$A_1 \pmod{\mathfrak{p}} \cong A_2 \pmod{\mathfrak{p}}.$$

Let r be the number of prime ideals $\mathfrak{q}$ in $\mathbb{O}_L$ for which $e(\mathfrak{q}/p)f(\mathfrak{q}/p)$ is odd. If $r>0$, then

$$p \le \left(4^g \frac{\operatorname{disc}_{K_1}\cdot\operatorname{disc}_{K_2}}{\operatorname{disc}(\mathbb{O}_L)^4}\right)^{1/r}.$$

(2) *Suppose that $[L:\mathbb{Q}]=2$ and that A_i are principally polarized abelian surfaces. Then we have the bound*

$$p \le \left(16 \frac{\operatorname{disc}_{K_1}\cdot\operatorname{disc}_{K_2}}{\operatorname{disc}(\mathbb{O}_L)^4}\right)^{1/r'}$$

according to the cases listed in Table 1 (and no other case is possible).

Proof. Since the A_i are principally polarized abelian surfaces, they satisfy the Deligne–Pappas condition and, when p is unramified, even the Rapoport condition. We can therefore use the results of [Bachmat and Goren 1999; Nicole 2005].

If p is split in L, then every supersingular abelian variety is superspecial. In that case, $\operatorname{End}_{\mathbb{O}_L}(A)$ is an order of discriminant $p\mathbb{O}_L$ in $B_{p,L}$, and we apply (1) with $r=2$.

If p is inert, then the reduction is necessarily supersingular by Lemma 11.1 and may or may not be superspecial. If it is superspecial, then, again, $\mathrm{End}_{\mathcal{O}_L}(A)$ is an order of discriminant $p\mathcal{O}_L$ in $B_{p,L}$, and the bound holds with $r' = 2$.

If the reduction is supersingular and not superspecial, then in fact $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $p^2\mathcal{O}_L$, and so we may take $r' = 4$.

Next we consider the case when p is ramified. There are three cases. The first is when we have superspecial reduction and the Rapoport condition holds. In that case, $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $p\mathcal{O}_L$, and we may take $r' = 2$. The second case is when we have superspecial reduction and the Rapoport condition does not hold (but the Deligne–Pappas condition holds). In this case, $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $\mathfrak{p}$, where $\mathfrak{p}$ is the prime of $\mathcal{O}_L$ above p, and we can take $r' = 1$. The last possibility is, ostensibly, that we have supersingular reduction, which is not superspecial. This in fact never happens in the presence of CM by the full ring of integers. It is interesting to note, though, that for supersingular and not superspecial reduction, the abelian variety A has a unique copy of the group scheme α_p contained in it, which is therefore preserved under all endomorphisms. Thus, $\mathrm{End}(A) \hookrightarrow \mathrm{End}(A/\alpha_p)$, and A/α_p is superspecial but doesn't satisfy the Rapoport condition [Andreatta and Goren 2003]. And so, were this case to occur, we could have taken $r' = 1$. □

Remark 11.5. Suppose that $r = 0$. Then g is even, and a maximal order $R \subset B_{p,L}$ has discriminant 1 since $B_{p,L}$ can only be ramified at primes dividing p, and if $F/\mathbb{Q}_p$ is a field extension and $[F : \mathbb{Q}_p] = \alpha$, then $B_{p,\infty} \otimes_{\mathbb{Q}_p} F$ is split if and only if α is even. Taking $F = L_{\mathfrak{q}}$, we have that $\alpha = e(\mathfrak{q}/p)f(\mathfrak{q}/p)$. For every prime p (and for any decomposition behavior of p), there certainly exist supersingular abelian varieties A with RM such that $\mathrm{End}_{\mathcal{O}_L}(A) = R$. This is easily achieved by choosing an R-stable lattice of the Dieudonné module of A. Experience shows, however, that such abelian varieties tend to be badly behaved; for example, the Deligne–Pappas condition tends to fail when p is unramified (it fails in the cases we have checked, and we did not find an example where it holds), or in other cases, such as when p is totally ramified, the Deligne–Pappas condition holds, but the endomorphism ring is not the maximal order. Thus, one would expect that under the Deligne–Pappas condition the discriminant of $\mathrm{End}_{\mathcal{O}_L}(A)$ is never 1 and, if so, one obtains a version of Corollary 11.4(1) in all cases.

In fact, one can be more optimistic and guess that the largest order $\mathcal{O}$ arising for a supersingular characteristic p abelian variety with RM A satisfying the Deligne–Rapoport condition also arises for some superspecial such abelian variety. Superspecial abelian varieties with RM were studied by Nicole [2005; 2008]. When p is unramified in L and A is superspecial, $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $p\mathcal{O}_L$. When p is ramified in L, larger orders arise [Nicole 2005, Theorem 2.8.5], but at least when p is totally ramified, $p\mathcal{O}_L = \mathfrak{p}^{[L:\mathbb{Q}]}$, still the largest order arising (for a superspecial abelian variety) has discriminant $\mathfrak{p}$.

12. Computations: $g = 2$

Consider the two primitive Galois quartic CM fields $K' = \mathbb{Q}(\sqrt{-85+34\sqrt{5}})$ and $K = \mathbb{Q}(\zeta_5)$. The common real quadratic subfield $L = K^+ = K'^+ = \mathbb{Q}(\sqrt{5})$ has strict class number 1 as it has class number 1 and a unit $(1+\sqrt{5})/2$ of negative norm. The field K has class number 1, and the triple of absolute Igusa invariants of the principally polarized abelian surface with CM by K is $i_1 = i_2 = i_3 = 0$. The field K' has class number 2, and the triple of absolute Igusa invariants for one of the CM points associated to K' is

$$i_1 = \frac{2^{33}\cdot 3^{10}\cdot 5^5\cdot 19^5\cdot 521^5}{71^{12}}, \qquad i_2 = \frac{2^{23}\cdot 3^{10}\cdot 5^5\cdot 19^5\cdot 521^3}{71^8},$$
$$i_3 = \frac{2^{16}\cdot 3^7\cdot 5^4\cdot 19^3\cdot 521^2\cdot 755777339}{71^8}.$$

Genus-2 curves over $\mathbb{Q}$ with these invariants are given by the affine models

$$y^2 = x^5 - 1,$$
$$y^2 = -584x^6 - 4020x^5 + 28860x^4 + 130240x^3 - 514920x^2 - 190244x - 289455$$

for $\mathbb{Q}(\zeta_5)$ and K', respectively. In this case, the triple of absolute invariants is insufficient to determine whether the two curves are isomorphic modulo a prime p since the first invariant is zero. To understand for which primes the curves are isomorphic, it is necessary to compute all ten Igusa invariants for the CM point associated to K' to determine which primes divide all ten invariants (see [Goren and Lauter 2012, Section 2.2] for an explanation, especially Consequence 3 at the end of the subsection). In particular, primes that divide the differences of all ten Igusa invariants associated to two CM points of K and K' are primes for which the *coincidence number* of K and K' defined in Section 9 is nonzero.

The prime 19 appears in all three invariants, and checking all ten invariants, we find that they too are all zero modulo 19. There is also a positive contribution at the prime $p = 19$ in our formula in (8-3), which implies a nonzero coincidence number. Since K has class number 1, there is only one superspecial order $R(\mathbb{O}, \lambda)$. We find an element $x \in \mathbb{O}_L$ satisfying conditions **C** and count the elements in $S_2(\mathbb{O}, x)$. Let d and d' be as in Section 6. We find that for $x = 3\sqrt{5} - 3$, the ideal in $\mathbb{O}_L$ generated by $(x^2 - dd')/4$ factors as

$$\mathfrak{p}_2^2\mathfrak{p}_{19,1}\mathfrak{p}_{19,2}.$$

We see that there is a positive contribution for $p = 19$ in our formula because this factorization has both split factors for 19, and 2 is totally inert in K/L but appears to the power 2, so $(x^2 - dd')/(4\cdot 19)$ is a norm of an ideal from K/L, and the set $S_2(\mathbb{O}, x)$ is nonempty.

Consider the other primes that are common to all three numerators in this example. The prime 5 is ramified in L, so our results do not cover it; neither do our formulas pertain to the prime 2, which also appears in all three numerators. The prime 3 divides all ten invariants but is supersingular, not superspecial, and it certainly satisfies the crude bound Theorem 11.3 from Section 11. The prime 521 does not divide all ten invariants.

References

[Andreatta and Goren 2003] F. Andreatta and E. Z. Goren, "Geometry of Hilbert modular varieties over totally ramified primes", *Int. Math. Res. Not.* **2003**:33 (2003), 1786–1835. MR 2005a:14060 Zbl 1045.14012

[Bachmat and Goren 1999] E. Bachmat and E. Z. Goren, "On the non-ordinary locus in Hilbert–Blumenthal surfaces", *Math. Ann.* **313**:3 (1999), 475–506. MR 2000b:14058 Zbl 0919.14014

[Chai 1995] C.-L. Chai, "Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli", *Invent. Math.* **121**:3 (1995), 439–479. MR 96f:11082 Zbl 0990.11039

[Charles et al. 2009a] D. X. Charles, E. Z. Goren, and K. E. Lauter, "Families of Ramanujan graphs and quaternion algebras", pp. 53–80 in *Groups and symmetries* (Montréal, 2007), edited by J. Harnad and P. Winternitz, CRM Proc. Lecture Notes **47**, Amer. Math. Soc., Providence, RI, 2009. MR 2010m:14056 Zbl 1250.05057

[Charles et al. 2009b] D. X. Charles, K. E. Lauter, and E. Z. Goren, "Cryptographic hash functions from expander graphs", *J. Cryptology* **22**:1 (2009), 93–113. MR 2010d:94074 Zbl 1166.94006

[Conrad 2004] B. Conrad, "Gross–Zagier revisited", pp. 67–163 in *Heegner points and Rankin L-series*, edited by H. Darmon and S.-W. Zhang, Math. Sci. Res. Inst. Publ. **49**, Cambridge Univ. Press, 2004. MR 2005h:11121 Zbl 1072.11040

[Dorman 1988] D. R. Dorman, "Special values of the elliptic modular function and factorization formulae", *J. Reine Angew. Math.* **383** (1988), 207–220. MR 89k:11026 Zbl 0626.10022

[Dorman 1989a] D. R. Dorman, "Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves", pp. 108–116 in *Théorie des nombres* (Québec, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR 90j:11043 Zbl 0697.12011

[Dorman 1989b] D. R. Dorman, "Singular moduli, modular polynomials, and the index of the closure of $\mathbf{Z}[j(\tau)]$ in $\mathbf{Q}(j(\tau))$", *Math. Ann.* **283**:2 (1989), 177–191. MR 90k:11149 Zbl 0642.12014

[Goren 2002] E. Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series **14**, Amer. Math. Soc., Providence, RI, 2002. MR 2003c:11038 Zbl 0986.11037

[Goren and Lauter 2006] E. Z. Goren and K. E. Lauter, "Evil primes and superspecial moduli", *Int. Math. Res. Not.* **2006** (2006), Art. ID 53864, 19. MR 2007f:11061 Zbl 1124.14042

[Goren and Lauter 2007] E. Z. Goren and K. E. Lauter, "Class invariants for quartic CM fields", *Ann. Inst. Fourier* (*Grenoble*) **57**:2 (2007), 457–480. MR 2008i:11075 Zbl 1172.11018

[Goren and Lauter 2009] E. Z. Goren and K. E. Lauter, "The distance between superspecial abelian varieties with real multiplication", *J. Number Theory* **129**:6 (2009), 1562–1578. MR 2010k:14085 Zbl 1203.14047

[Goren and Lauter 2012] E. Z. Goren and K. E. Lauter, "Genus 2 curves with complex multiplication", *Int. Math. Res. Not.* **2012**:5 (2012), 1068–1142. MR 2899960 Zbl 1236.14033

[Gross 1986] B. H. Gross, "On canonical and quasicanonical liftings", *Invent. Math.* **84**:2 (1986), 321–326. MR 87g:14051 Zbl 0597.14044

[Gross and Zagier 1985] B. H. Gross and D. B. Zagier, "On singular moduli", *J. Reine Angew. Math.* **355** (1985), 191–220. MR 86j:11041 Zbl 0545.10015

[Lang 1986] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, New York, 1986. MR 95f:11085 Zbl 0601.12001

[Nicole 2005] M.-H. Nicole, *Superspecial abelian varieties, theta series and the Jacquet–Langlands correspondence*, Ph.D. thesis, McGill University, 2005, Available at http://search.proquest.com/docview/305374771?accountid=14496. MR 2709763

[Nicole 2008] M.-H. Nicole, "Superspecial abelian varieties and the Eichler basis problem for Hilbert modular forms", *J. Number Theory* **128**:11 (2008), 2874–2889. MR 2009m:11084 Zbl 1214.11076

[Vignéras 1980] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics **800**, Springer, Berlin, 1980. In French. MR 82i:12016 Zbl 0422.12008

[van Wamelen 1999] P. van Wamelen, "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68**:225 (1999), 307–320. MR 99c:11079 Zbl 0906.14025

[Waterhouse and Milne 1971] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields", pp. 53–64 in *1969 Number Theory Institute* (Stony Brook, NY, 1969), Proc. Sympos. Pure Math. **20**, Amer. Math. Soc., Providence, R.I., 1971. MR 47 #3397 Zbl 0216.33102

[Yu 2004] C.-F. Yu, "The isomorphism classes of abelian varieties of CM-type", *J. Pure Appl. Algebra* **187**:1-3 (2004), 305–319. MR 2004k:14077 Zbl 1087.14030

Communicated by Brian Conrad
Received 2012-02-23 Revised 2012-10-05 Accepted 2012-11-03

goren@math.mcgill.ca *Department of Mathematics and Statistics, McGill University, 805 Sherbrooke Street West, Montreal QC H3A 2K6, Canada*

klauter@microsoft.com *Cryptography Research Group, Microsoft Research, 1 Microsoft Way, Redmond, WA 98052, United States*

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1451

Counting rational points over number fields on a singular cubic surface

Christopher Frei

A conjecture of Manin predicts the distribution of K-rational points on certain algebraic varieties defined over a number field K. In recent years, a method using universal torsors has been successfully applied to several hard special cases of Manin's conjecture over the field $\mathbb{Q}$. Combining this method with techniques developed by Schanuel, we give a proof of Manin's conjecture over arbitrary number fields for the singular cubic surface S given by the equation $x_0^3 = x_1x_2x_3$.

1. Introduction

We consider the cubic surface $S \subseteq \mathbb{P}^3$ defined over any number field K by the equation

$$x_0^3 = x_1x_2x_3.$$

It is toric, has three singular points $(0:1:0:0)$, $(0:0:1:0)$, $(0:0:0:1)$, and contains three lines $L_i := \{x_0 = x_i = 0\}$, for $i \in \{1, 2, 3\}$. The set $S(K)$ of K-rational points on S is infinite.

The Weil height of $\boldsymbol{x} = (x_0 : x_1 : x_2 : x_3) \in \mathbb{P}^3(K)$ is defined by

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} \max\{|x_0|_v, |x_1|_v, |x_2|_v, |x_3|_v\}^{d_v}.$$

Here, $M(K)$ is the set of places of K, the absolute values $|\cdot|_v$ are normalized such that they extend the usual absolute values on $\mathbb{Q}$, and d_v is the local degree $[K_v : \mathbb{Q}_p]$, if v extends the place p of $\mathbb{Q}$.

MSC2010: primary 11D45; secondary 14G05.
Keywords: Manin's conjecture, number fields, rational points, singular cubic surface.

It is well known that there are only finitely many points of bounded height in $\mathbb{P}^3(K)$, so it makes sense to study the number of K-rational points on S of height bounded by B, as B tends to infinity. A generalization of a conjecture by Manin [Franke et al. 1989; Batyrev and Tschinkel 1998b], applied to our case, links the asymptotic behavior of this quantity to geometric features of S, provided that we exclude the points lying on the lines L_i. Indeed, the number of K-rational points of bounded height on these lines dominates the number of K-rational points on the rest of S, whereas much of the geometric information about S would be lost when considering just the lines.

Therefore, we denote by U the complement of the three lines in S and define the counting function

$$N(B) := |\{\boldsymbol{x} \in U(K) \mid H(\boldsymbol{x}) \leq B\}|.$$

Here, $U(K)$ is the set of K-rational points on U. The above-mentioned generalization of Manin's conjecture [Franke et al. 1989; Batyrev and Tschinkel 1998b] to Fano varieties with at worst canonical singularities predicts in this case that

$$N(B) \sim cB(\log B)^6,$$

with a positive leading constant $c = c_{S,K,H}$. A conjectural interpretation of the leading constant in Manin's conjecture was given by Peyre [1995] and extended to Fano varieties with at worst canonical singularities by Batyrev and Tschinkel [1998b]. When writing "Manin's conjecture", we implicitly include the conjecture about the leading constant.

Manin's conjecture has been proved for smooth toric varieties over arbitrary number fields by Batyrev and Tschinkel [1998a], studying the height zeta function with the help of Fourier analysis. In [Batyrev and Tschinkel 1998b] they explain how this result can be applied to prove Manin's conjecture for our singular surface S. Similar methods work for other varieties that are equivariant compactifications of certain algebraic groups; for example, see [Chambert-Loir and Tschinkel 2002].

Salberger [1998] gave a new proof of Manin's conjecture for split toric varieties over the field $\mathbb{Q}$ of rational numbers by a fundamentally different approach using universal torsors. These were first introduced by Colliot-Thélène and Sansuc [1980; 1987] to study the Hasse principle. In the context of Manin's conjecture, the basic idea is to find a parametrization of the rational points on the variety under consideration that makes it feasible to count them by analytic number theory.

Based on Salberger's ideas, proofs were found for several hard special cases of Manin's conjecture over $\mathbb{Q}$, to which the methods of Batyrev and Tschinkel cannot be applied; see for instance [Baier and Browning 2013; de la Bretèche 2002; de la Bretèche and Browning 2011; de la Bretèche et al. 2007; de la Bretèche and Fouvry 2004; de la Bretèche et al. 2012; Browning and Derenthal 2009; Le Boudec 2012].

For our surface S, independent proofs of Manin's conjecture over $\mathbb{Q}$ were given by de la Bretèche [1998], Fouvry [1998], Salberger [1998], Heath-Brown and Moroz [1999], and de la Bretèche and Swinnerton-Dyer [2007], with the help of such parametrizations. The best error terms have been obtained in [de la Bretèche 1998; de la Bretèche and Swinnerton-Dyer 2007].

In a first attempt to generalize universal torsor techniques to number fields other than $\mathbb{Q}$, Derenthal and Janda [2013] modified the approach by Heath-Brown and Moroz [1999] and successfully applied it to the case of imaginary quadratic number fields of class number 1.

In this article, we combine the method of Derenthal and Janda with ideas developed by Schanuel [1979] and apply it to arbitrary number fields. To the author's best knowledge, this is the first example of universal torsor techniques applied to a special case of Manin's conjecture over general number fields, aside from Schanuel's result for $\mathbb{P}^n$. Hopefully, similar approaches will lead to results for nontoric varieties.

Before we state the theorem, let us fix some notation: by Δ_K, h_K, R_K, and ω_K, we denote the discriminant, class number, regulator, and number of roots of unity of K. Moreover, r and s denote the number of real and complex places of K, and $q := r + s - 1$. We write $\mathbb{O}_K$ for the ring of integers of K and $\mathfrak{N}\mathfrak{a}$ for the absolute norm of the nonzero fractional ideal $\mathfrak{a}$ of K.

Theorem 1. *For every number field K, we have*

$$N(B) = c_K B(\log B)^6 + O(B(\log B)^5),$$

for $B \geq e$. Here, the implicit O-constant depends on K, and

$$c_K := \frac{9^q}{4 \cdot 6!} \left(\frac{2^r (2\pi)^s}{\sqrt{|\Delta_K|}} \right)^9 \left(\frac{h_K R_K}{\omega_K} \right)^7 \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathfrak{N}\mathfrak{p}} \right)^7 \left(1 + \frac{7}{\mathfrak{N}\mathfrak{p}} + \frac{1}{\mathfrak{N}\mathfrak{p}^2} \right),$$

where the product runs over all nonzero prime ideals $\mathfrak{p}$ of $\mathbb{O}_K$.

The leading constant. Let us check the leading constant c_K in Theorem 1 against the expected one. According to [Batyrev and Tschinkel 1998b, Section 3.4, Step 4], it should have the form

$$\frac{\gamma_{\mathfrak{K}^{-1}}(U) \delta_{\mathfrak{K}^{-1}}(U) \tau_{\mathfrak{K}^{-1}}(U)}{6!},$$

where $\gamma_{\mathfrak{K}^{-1}}(U)$ is the volume of a certain polytope depending only on U, $\delta_{\mathfrak{K}^{-1}}(U)$ is a cohomological invariant, and $\tau_{\mathfrak{K}^{-1}}(U)$ is a generalized version of the Tamagawa number introduced by Peyre [1995] for smooth Fano varieties.

Derenthal and Janda [2013, Section 3] computed these constants for our U over arbitrary number fields K, using a minimal desingularization $\tilde{S}$ of S constructed

by blow-ups of $\mathbb{P}^2$ in six rational points: We have $\delta_{\mathcal{H}^{-1}}(U) = 1$, and, as already given in [Batyrev and Tschinkel 1998b, Section 5.3], $\gamma_{\mathcal{H}^{-1}}(U) = \frac{1}{36}$. The Tamagawa number $\tau_{\mathcal{H}^{-1}}(U)$ is an adelic invariant given as a product of local densities with certain convergence factors

$$\tau_{\mathcal{H}^{-1}}(U) = \left(\frac{2^r(2\pi)^s h_K R_K}{\omega_K \sqrt{|\Delta_K|}}\right)^7 |\Delta_K|^{-1} \prod_{\nu|\infty} \omega_{\mathcal{H}^{-1},\nu}(\tilde{S}(K_\nu)) \prod_{\nu\nmid\infty} \lambda_\nu^{-1} \omega_{\mathcal{H}^{-1},\nu}(\tilde{S}(K_\nu)).$$

For the Archimedean densities, we have

$$\omega_{\mathcal{H}^{-1},\nu}(\tilde{S}(K_\nu)) = \begin{cases} 36 & \text{if } K_\nu = \mathbb{R}, \\ 36\pi^2 & \text{if } K_\nu = \mathbb{C}. \end{cases}$$

The non-Archimedean density at the place ν corresponding to the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is given by

$$\lambda_\nu^{-1} \omega_{\mathcal{H}^{-1},\nu}(\tilde{S}(K_\nu)) = \left(1 - \frac{1}{\mathfrak{N}\mathfrak{p}}\right)^7 \left(1 + \frac{7}{\mathfrak{N}\mathfrak{p}} + \frac{1}{\mathfrak{N}\mathfrak{p}^2}\right).$$

Putting this together, we see that the constant c_K in Theorem 1 is as expected.

More notation. The ideal class of a nonzero fractional ideal $\mathfrak{a}$ of K is denoted by $[\mathfrak{a}]$. We write P_K for the group of nonzero principal fractional ideals of K. We denote the real embeddings by $\sigma_1, \dots, \sigma_r : K \to \mathbb{R}$ and the complex embeddings by $\sigma_{r+1}, \overline{\sigma}_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma}_{r+s} : K \to \mathbb{C}$. The componentwise continuation of σ_i to K^n is also denoted by σ_i. If ν is the place corresponding to σ_i then we put $d_i := d_\nu$. When convenient, we write $\alpha^{(i)} := \sigma_i(\alpha)$ for $\alpha \in K$. If $\mathfrak{a}$, $\mathfrak{b}$ are fractional ideals of K, we put $(\mathfrak{a}, \mathfrak{b}) := \mathfrak{a} + \mathfrak{b}$. For any point $\boldsymbol{x} = (x_0, \dots, x_n) \in K^{n+1}$, let $\mathfrak{J}(\boldsymbol{x}) := (x_0\mathcal{O}_K, \dots, x_n\mathcal{O}_K)$. Then, for $\boldsymbol{x} \in K^4$,

$$H(\boldsymbol{x}) = \mathfrak{N}\mathfrak{J}(\boldsymbol{x})^{-1} \prod_{i=1}^{r+s} \max\left\{|x_0^{(i)}|, |x_1^{(i)}|, |x_2^{(i)}|, |x_3^{(i)}|\right\}^{d_i}.$$

We fix, once and for all, a system of fundamental units of $\mathcal{O}_K$, and denote by $\mathcal{F}$ the multiplicative subgroup of $K^\times$ generated by this system. Then $\mathcal{F}$ is a free Abelian group of rank q, and the unit group $\mathcal{O}_K^\times$ is the direct product $\mathcal{O}_K^\times = \mu_K \mathcal{F}$, where μ_K is the group of roots of unity in K.

Moreover, we fix, once and for all, a system $\mathcal{C}$ of integral representatives for the ideal classes of $\mathcal{O}_K$, that is, a set of h_K nonzero ideals of $\mathcal{O}_K$, one from every ideal class.

2. Passing to a universal torsor

In this section, we find a parametrization of the rational points of bounded height on U by (almost) integral points on an open subset of $\mathbb{A}^9_K$, subject to some height- and

coprimality conditions, and up to a certain action of $(\mathcal{O}_K^\times)^7$. This parametrization has the merit that, due to the coprimality conditions, the non-Archimedean parts of the height conditions are trivial.

Over $\mathbb{Q}$ and imaginary quadratic number fields, the action of $(\mathcal{O}_K^\times)^7$ makes no problems, since then $\mathcal{O}_K^\times$ is finite. In general, that is not the case; this is one of the main difficulties which we have to overcome.

While we will use purely number-theoretic arguments, we mention that the open subset of $\mathbb{A}^9$ is a universal torsor over S, and that our construction is motivated by geometric considerations; see [Derenthal and Janda 2013]. The choice of indices might seem slightly counterintuitive at the beginning. It is, however, closely related to those geometric considerations and will lead to a rather symmetric result.

Parametrization. Let $\Psi_0 : K^3 \to K^4$ be given by

$$\Psi_0(x_{23}, x_{31}, x_{12}) = (x_{12}x_{23}x_{31}, x_{12}x_{31}^2, x_{23}x_{12}^2, x_{31}x_{23}^2).$$

We will also consider Ψ_0 as a rational map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^3$. Let $W \subseteq \mathbb{P}^2$ be the open subset

$$W = \{(x_{23} : x_{31} : x_{12}) \in \mathbb{P}^2 \mid x_{12}x_{23}x_{31} \neq 0\}.$$

Then Ψ_0 induces a bijection between $W(K) \subseteq \mathbb{P}_2(K)$ and $U(K) \subseteq \mathbb{P}_3(K)$ with inverse $(x_0 : x_1 : x_2 : x_3) \mapsto (x_0^2 : x_0x_1 : x_1x_2)$. Therefore,

$$N(B) = |\{\boldsymbol{x} \in W(K) \mid H(\Psi_0(\boldsymbol{x})) \leq B\}|. \tag{2-1}$$

Whenever indices j, k, l appear in an expression, this expression is understood to hold for all $(j, k, l) \in \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\} =: A$.

Lemma 2.1. *Let $\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3$ be nonzero ideals of $\mathcal{O}_K$, and let $\mathfrak{c} := (\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3)$. Then there exist unique nonzero ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_{12}, \mathfrak{a}_{21}, \mathfrak{a}_{23}, \mathfrak{a}_{32}, \mathfrak{a}_{31}, \mathfrak{a}_{13}$ of $\mathcal{O}_K$ such that*

$$\mathfrak{b}_j = \mathfrak{c} \cdot \mathfrak{a}_{jk} \cdot \mathfrak{a}_k^2 \cdot \mathfrak{a}_{lk} \cdot \mathfrak{a}_j \cdot \mathfrak{a}_{kj}, \tag{2-2}$$

and such that the following coprimality conditions hold:

$$(\mathfrak{a}_k, \mathfrak{a}_j) = \mathcal{O}_K, \quad (2\text{-}3) \qquad (\mathfrak{a}_k, \mathfrak{a}_{lj}) = \mathcal{O}_K, \quad (2\text{-}6) \qquad (\mathfrak{a}_{lk}, \mathfrak{a}_{lj}) = \mathcal{O}_K, \quad (2\text{-}9)$$

$$(\mathfrak{a}_k, \mathfrak{a}_{kj}) = \mathcal{O}_K, \quad (2\text{-}4) \qquad (\mathfrak{a}_k, \mathfrak{a}_{kl}) = \mathcal{O}_K, \quad (2\text{-}7) \qquad (\mathfrak{a}_{lk}, \mathfrak{a}_{jl}) = \mathcal{O}_K, \quad (2\text{-}10)$$

$$(\mathfrak{a}_k, \mathfrak{a}_{jl}) = \mathcal{O}_K, \quad (2\text{-}5) \qquad (\mathfrak{a}_{lk}, \mathfrak{a}_{jk}) = \mathcal{O}_K, \quad (2\text{-}8) \qquad (\mathfrak{a}_{jk}, \mathfrak{a}_{kl}) = \mathcal{O}_K. \quad (2\text{-}11)$$

Conversely, given ideals $\mathfrak{a}_k, \mathfrak{a}_{jk}, \mathfrak{a}_{lk}$ as in (2-3)–(2-11), the ideals $\mathfrak{b}_j$ defined by (2-2) satisfy $(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \mathfrak{c}$.

Proof. It is enough to prove the lemma if $\mathfrak{c} = \mathbb{O}_K$, since we can always replace $\mathfrak{b}_j$ by $\mathfrak{c}^{-1}\mathfrak{b}_j$. In this case, we have $(\mathfrak{b}_j, \mathfrak{b}_k^2)(\mathfrak{b}_l, \mathfrak{b}_j) \mid \mathfrak{b}_j$. Let

$$\mathfrak{a}_{jk} := \frac{\mathfrak{b}_j}{(\mathfrak{b}_j, \mathfrak{b}_k^2)(\mathfrak{b}_l, \mathfrak{b}_j)}, \quad \mathfrak{a}_k := \left(\frac{\mathfrak{b}_j}{(\mathfrak{b}_j, \mathfrak{b}_k)}, \mathfrak{b}_k\right), \quad \text{and} \quad \mathfrak{a}_{lk} := \frac{(\mathfrak{b}_j, \mathfrak{b}_k)}{\mathfrak{a}_k}. \tag{2-12}$$

Then the $\mathfrak{a}_{jk}$, $\mathfrak{a}_k$, $\mathfrak{a}_{lk}$ are nonzero ideals of $\mathbb{O}_K$ and (2-2) holds, since

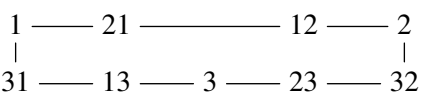
$$(\mathfrak{b}_j, \mathfrak{b}_k^2) = (\mathfrak{b}_j, \mathfrak{b}_k)\mathfrak{a}_k = \mathfrak{a}_k^2\mathfrak{a}_{lk} \quad \text{and} \quad (\mathfrak{b}_l, \mathfrak{b}_j) = \mathfrak{a}_j\mathfrak{a}_{kj}.$$

One readily verifies that the left-hand sides in conditions (2-3)–(2-6), (2-9), and (2-10) divide $(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \mathbb{O}_K$. Similarly, the left-hand sides in (2-7), (2-11) divide $(\mathfrak{b}_j/(\mathfrak{b}_j, \mathfrak{b}_k), \mathfrak{b}_k/(\mathfrak{b}_j, \mathfrak{b}_k)) = \mathbb{O}_K$, and the left-hand side in (2-8) divides $(\mathfrak{b}_k/\mathfrak{a}_k, \mathfrak{b}_j/((\mathfrak{b}_j, \mathfrak{b}_k)\mathfrak{a}_k)) = \mathbb{O}_K$.

Now assume that (2-2) holds, with given nonzero ideals $\mathfrak{a}_k$, $\mathfrak{a}_{jk}$, $\mathfrak{a}_{lk}$ satisfying the coprimality conditions (2-3)–(2-11). These conditions imply that $(\mathfrak{b}_j, \mathfrak{b}_k) = \mathfrak{a}_k\mathfrak{a}_{lk}$, and furthermore $(\mathfrak{b}_j/(\mathfrak{a}_k\mathfrak{a}_{lk}), \mathfrak{b}_k) = \mathfrak{a}_k$. Thus, the $\mathfrak{a}_k$,$\mathfrak{a}_{lk}$ are as in (2-12). Clearly, this holds as well for the $\mathfrak{a}_{jk}$, and uniqueness is proved.

The last assertion is again a direct consequence of (2-3)–(2-11). □

The coprimality conditions (2-3)–(2-11) can be expressed in a more convenient way: Let $G = (V, E)$ be the graph with vertex set $V := \{1, 2, 3, 12, 21, 23, 32, 31, 13\}$ and edge set $E := \{\{k, jk\}, \{k, lk\}, \{kl, lk\} \mid (j, k, l) \in A\}$. We can draw it as follows:



Then (2-3)–(2-11) hold if and only if $(\mathfrak{a}_v, \mathfrak{a}_w) = \mathbb{O}_K$ for all pairs (v, w) of nonadjacent vertices of V. If we denote the edge set of the complement graph by E', this means that

$$\text{for any } \{v, w\} \in E', \text{ we have } (\mathfrak{a}_v, \mathfrak{a}_w) = \mathbb{O}_K. \tag{2-13}$$

For every point $(x_{23} : x_{31} : x_{12}) \in W(K)$, the ideal class $[\mathfrak{J}(x_{23}, x_{31}, x_{12})]$ is well-defined, and $[\mathfrak{J}(x_{23}, x_{31}, x_{12})] = [C]$, for some $C \in \mathscr{C}$. By multiplying with a suitable element of $K^\times$, we can choose a representative $\boldsymbol{x} = (x_{23}, x_{31}, x_{12}) \in (\mathbb{O}_K \setminus \{0\})^3$ with $\mathfrak{J}(\boldsymbol{x}) = C$. This representative is unique up to scalar multiplication by units in $\mathbb{O}_K^\times$.

We apply Lemma 2.1 to the principal ideals $\mathfrak{b}_j := x_{jk}\mathbb{O}_K$ and obtain

$$x_{jk}\mathbb{O}_K = C \cdot \mathfrak{a}_{jk} \cdot \mathfrak{a}_k^2 \cdot \mathfrak{a}_{lk} \cdot \mathfrak{a}_j \cdot \mathfrak{a}_{kj},$$

with unique ideals $\mathfrak{a}_v$ of $\mathbb{O}_K$ satisfying (2-13). For all $v \in V \setminus \{12, 23, 31\}$, there is a unique $C_v \in \mathscr{C}$ with $[\mathfrak{a}_v] = [C_v^{-1}]$. Choose $y_v \in K^\times$ with $y_v\mathbb{O}_K = \mathfrak{a}_v C_v$, and

define $y_{12}, y_{23}, y_{31} \in K^\times$ by the equations

$$x_{jk} = y_{jk} \cdot y_k^2 \cdot y_{lk} \cdot y_j \cdot y_{kj}. \tag{2-14}$$

Then

$$y_{jk}\mathbb{O}_K = \mathfrak{a}_{jk} C_{jk} \quad \text{with } C_{jk} := C C_k^{-2} C_{lk}^{-1} C_j^{-1} C_{kj}^{-1}.$$

For $\boldsymbol{C} = (C, C_1, C_2, C_3, C_{21}, C_{32}, C_{13}) \in \mathscr{C}^7$, we define $M_{\boldsymbol{C}}$ as the set of all $\boldsymbol{y} = (y_v)_{v\in V} \in (K^\times)^9$ such that

$$y_v \in C_v \text{ for all } v \in V, \text{ and the ideals } \mathfrak{a}_v := y_v C_v^{-1} \text{ satisfy (2-13).} \tag{2-15}$$

By what we have shown above, relations (2-14) define a surjective mapping

$$\phi : \bigcup_{\boldsymbol{C}\in\mathscr{C}^7} M_{\boldsymbol{C}} \to W(K).$$

If $\boldsymbol{y} \in M_{\boldsymbol{C}}$ and $\phi(\boldsymbol{y}) = (x_{23} : x_{31} : x_{12})$ with x_{jk} as in (2-14) then

$$x_{jk}\mathbb{O}_K = C \cdot \mathfrak{a}_{jk} \cdot \mathfrak{a}_k^2 \cdot \mathfrak{a}_{lk} \cdot \mathfrak{a}_j \cdot \mathfrak{a}_{kj}.$$

By Lemma 2.1, we have $\mathfrak{J}(x_{23}, x_{31}, x_{12}) = C$, and the $\mathfrak{a}_v$ (and thus as well the C_v) are uniquely determined by the $x_{jk}\mathbb{O}_K$. In particular, the sets $M_{\boldsymbol{C}}$, $\boldsymbol{C} \in \mathscr{C}^7$, are pairwise disjoint. Moreover, (x_{23}, x_{31}, x_{12}) and the y_v, $v \in V$, are determined by $\phi(\boldsymbol{y})$ up to multiplication by units. Therefore, $\phi(\boldsymbol{y}) = \phi(\boldsymbol{z})$ if and only if there are units $\zeta, \zeta_v \in \mathbb{O}_K^\times$ with

$$z_v = \zeta_v y_v \text{ for all } v \in V \quad \text{and} \quad \zeta_{jk}\zeta_k^2\zeta_{lk}\zeta_j\zeta_{kj} = \zeta \text{ for all } (j,k,l) \in A.$$

By eliminating the ζ_{jk}, we see that $\phi(\boldsymbol{y}) = \phi(\boldsymbol{z})$ if and only if $\boldsymbol{y}$ and $\boldsymbol{z}$ are in the same orbit of the action $\odot$ of $(\mathbb{O}_K^\times)^7$ on $(K^\times)^9$ given by

$$(\zeta, \zeta_1, \zeta_2, \zeta_3, \zeta_{21}, \zeta_{32}, \zeta_{13}) \odot (y_v)_v := (z_v)_v, \tag{2-16}$$

where $z_v := \zeta_v y_v$ for all $v \in V \setminus \{12, 23, 31\}$ and $z_{jk} := \zeta\zeta_k^{-2}\zeta_{lk}^{-1}\zeta_j^{-1}\zeta_{kj}^{-1} y_{jk}$.

In what follows, it will be more convenient to work with the free Abelian subgroup $\mathscr{F}$ of $\mathbb{O}_K^\times$ generated by our fixed system of fundamental units. Clearly, $(\mathbb{O}_K^\times)^7$ is the direct product $(\mathbb{O}_K^\times)^7 = \mu_K^7 \cdot \mathscr{F}^7$. Since the action of $(\mathbb{O}_K^\times)^7$ on $(K^\times)^9$ is free, every orbit of $(K^\times)^9$ under the action of $(\mathbb{O}_K^\times)^7$ is the union of $|\mu_K^7| = \omega_K^7$ orbits under the action of $\mathscr{F}^7$.

Let $\mathscr{R}$ be a system of representatives for the orbits of $(K^\times)^9$ under the action of $\mathscr{F}^7$. Then ϕ induces an ω_K^7-to-1 map

$$\phi : \bigcup_{\boldsymbol{C}\in\mathscr{C}^7} (M_{\boldsymbol{C}} \cap \mathscr{R}) \to W(K).$$

The benefits of our construction become apparent in the height condition. With $\boldsymbol{x} = (x_{23}, x_{31}, x_{12})$ as in (2-14), we have $\psi_0(\boldsymbol{x}) = y_1^2 y_2^2 y_3^2 y_{21} y_{32} y_{13} \cdot \psi(\boldsymbol{y})$, where

$$\psi(\boldsymbol{y}) = (\psi(\boldsymbol{y})_0, \psi(\boldsymbol{y})_1, \psi(\boldsymbol{y})_2, \psi(\boldsymbol{y})_3),$$

with

$$\psi(\boldsymbol{y})_0 := \prod_{v \in V} y_v \quad \text{and} \quad \psi(\boldsymbol{y})_j := y_j^3 y_{jk} y_{jl} y_{kj}^2 y_{lj}^2 \quad \text{for } 1 \le j \le 3.$$

Therefore,

$$H(\psi_0(\boldsymbol{x})) = H(\psi(\boldsymbol{y})) = \mathfrak{N}\mathfrak{J}(\psi(\boldsymbol{y}))^{-1} \prod_{i=1}^{r+s} \max_{0 \le j \le 3} \{|\psi(\boldsymbol{y})_j^{(i)}|\}^{d_i}.$$

A straightforward computation using $y_v = \mathfrak{a}_v C_v$ and (2-13) shows that

$$\mathfrak{J}(\psi(\boldsymbol{y})) = C^3 C_1^{-2} C_2^{-2} C_3^{-2} C_{21}^{-1} C_{32}^{-1} C_{13}^{-1}.$$

By our construction, $\psi(\boldsymbol{y})$ satisfies the equation $\psi(\boldsymbol{y})_0^3 = \psi(\boldsymbol{y})_1 \psi(\boldsymbol{y})_2 \psi(\boldsymbol{y})_3$. Since this holds as well for all conjugates, the maximum is always one of $|\psi(\boldsymbol{y})_1^{(i)}|$, $|\psi(\boldsymbol{y})_2^{(i)}|$, $|\psi(\boldsymbol{y})_3^{(i)}|$. We define

$$\mathcal{R}(B) := \left\{ \boldsymbol{y} \in \mathcal{R} \;\middle|\; \prod_{i=1}^{r+s} \max_{1 \le j \le 3} \{|\sigma_i(y_j^3 y_{jk} y_{jl} y_{kj}^2 y_{lj}^2)|\}^{d_i} \le B \right\}. \tag{2-17}$$

The results of this section can be summarized as follows.

Proposition 2.2. *Let $M_{\boldsymbol{C}}$ be as in (2-15), let $\mathcal{R}$ be any system of representatives for the orbits of $(K^\times)^9$ under the action $\odot$ of $\mathcal{F}^7$ given by (2-16), and let $\mathcal{R}(B)$ be as in (2-17). Then $M_{\boldsymbol{C}} \cap \mathcal{R}(B)$ is finite for all $B > 0$, $\boldsymbol{C} \in \mathcal{C}^7$, and*

$$N(B) = \frac{1}{\omega_K^7} \sum_{\boldsymbol{C} \in \mathcal{C}^7} |M_{\boldsymbol{C}} \cap \mathcal{R}(u_{\boldsymbol{C}} B)|,$$

where $u_{\boldsymbol{C}} := \mathfrak{N}(C^3 C_1^{-2} C_2^{-2} C_3^{-2} C_{21}^{-1} C_{32}^{-1} C_{13}^{-1})$.

A system of representatives for the orbits. We construct a system $\mathcal{R}$ of representatives for the orbits of $(K^\times)^9$ under the action $\odot$ of $\mathcal{F}^7$ given by (2-16).

Lemma 2.3. *Let $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{F}$ and consider the system of equations*

$$\zeta \zeta_k^{-2} \zeta_j^{-1} = \alpha_j, \text{ for } (j,k) \in \{(1,2),(2,3),(3,1)\}, \tag{2-18}$$

with variables $\zeta, \zeta_j \in \mathcal{F}$.

(i) *If $\alpha_1\alpha_2\alpha_3$ is not a cube in $\mathcal{F}$ then this system has no solutions.*

(ii) *If $\alpha_1\alpha_2\alpha_3 = \xi^3$ with $\xi \in \mathcal{F}$ then the solutions are given by*

$$\zeta_1 = \delta, \qquad \zeta_2 = \delta\xi^{-1}\alpha_3, \qquad \zeta_3 = \delta\xi\alpha_2^{-1}, \qquad \zeta = \delta^3\xi\alpha_2^{-1}\alpha_3,$$

for all $\delta \in \mathcal{F}$.

Proof. Equations (2-18) imply that

$$\zeta^3\zeta_j^{-9} = \alpha_j\alpha_k^{-2}\alpha_l^4 = \alpha_1\alpha_2\alpha_3\alpha_k^{-3}\alpha_l^3, \tag{2-19}$$

which proves (i).

Now assume that $\alpha_1\alpha_2\alpha_3 = \xi^3$ for some $\xi \in \mathcal{F}$. Then ξ is unique since $\mathcal{F}$ is free Abelian. Direct computations verify that the values given in (ii) are solutions.

Given any solution $(\zeta, \zeta_1, \zeta_2, \zeta_3)$ of (2-18), let $\delta := \zeta_1$. Then (2-19) with $j = 1$ shows that ζ has the desired form. Similar computations using (2-19) with $j = 2$ and $j = 3$ prove that ζ_2 and ζ_3 are as desired. □

Let H be the subgroup of $(K^\times)^6$ of all $\underline{\alpha} = (\alpha_{12}, \alpha_{21}, \alpha_{23}, \alpha_{32}, \alpha_{31}, \alpha_{13}) \in \mathcal{F}^6$ for which $\alpha_{12}\alpha_{21}^2\alpha_{23}\alpha_{32}^2\alpha_{31}\alpha_{13}^2$ is a cube in $\mathcal{F}$.

Lemma 2.4. *Let $\mathcal{R}_1 \subseteq (K^\times)^3$ be a system of representatives for the orbits of $(K^\times)^3$ under the action of $\mathcal{F}$ by scalar multiplication, and let $\mathcal{R}_2 \subseteq (K^\times)^6$ be a system of representatives for $(K^\times)^6/H$. Then $\mathcal{R} := \mathcal{R}_1 \times \mathcal{R}_2$ is a system of representatives for the orbits of $(K^\times)^9$ under the action $\odot$ of $\mathcal{F}^7$.*

Proof. Let $\boldsymbol{y} = (y_v)_{v\in V} \in (K^\times)^9$. Then there is a unique $\underline{\alpha} \in H$ such that

$$(\alpha_{12}y_{12}, \alpha_{21}y_{21}, \alpha_{23}y_{23}, \alpha_{32}y_{32}, \alpha_{31}y_{31}, \alpha_{13}y_{13}) \in \mathcal{R}_2.$$

The elements $\underline{\zeta} = (\zeta, \zeta_1, \zeta_2, \zeta_3, \zeta_{21}, \zeta_{32}, \zeta_{13}) \in \mathcal{F}^7$ with $\underline{\zeta} \odot \boldsymbol{y} \in (K^\times)^3 \times \mathcal{R}_2$ are those satisfying

$$\zeta_{kj} = \alpha_{kj} \text{ and } \zeta\zeta_k^{-2}\zeta_{lk}^{-1}\zeta_j^{-1}\zeta_{kj}^{-1} = \alpha_{jk}. \tag{2-20}$$

With $\alpha_j := \alpha_{jk}\alpha_{kj}\alpha_{lk}$, this simplifies to (2-18). Now

$$\alpha_1\alpha_2\alpha_3 = \alpha_{12}\alpha_{21}^2\alpha_{23}\alpha_{32}^2\alpha_{31}\alpha_{13}^2$$

is a cube in $\mathcal{F}$, so ζ, ζ_1, ζ_2, ζ_3 are of the form given in Lemma 2.3(ii), for $\delta \in \mathcal{F}$. There is exactly one $\delta \in \mathcal{F}$ such that the corresponding ζ_1, ζ_2, ζ_3 satisfy $(\zeta_1 y_1, \zeta_2 y_2, \zeta_3 y_3) \in \mathcal{R}_1$. Hence, there is exactly one $\underline{\zeta} \in \mathcal{F}^7$ with $\underline{\zeta} \odot \boldsymbol{y} \in \mathcal{R}$. □

Lemma 2.5. *Let $R \subseteq K^\times$ be a system of representatives for $K^\times/\mathcal{F}$, and let $R_{\mathcal{F}} \subseteq \mathcal{F}$ be a system of representatives for $\mathcal{F}/\{\xi^3 \mid \xi \in \mathcal{F}\}$. Then*

$$\mathcal{R}_2 := \bigcup_{\rho\in R_{\mathcal{F}}} (\rho R \times R \times R \times R \times R \times R)$$

is a system of representatives for $(K^\times)^6/H$.

Proof. Clearly, $\bigcup_{\rho\in\mathcal{R}_{\mathcal{F}}} \rho R$ is a system of representatives for $K^\times/\{\xi^3 \mid \xi \in \mathcal{F}\}$. Let $\boldsymbol{y} \in (K^\times)^6$. For all $v \in \{21, 23, 32, 31, 13\}$, there is exactly one $\alpha_v \in \mathcal{F}$ with $\alpha_v y_v \in R$. Moreover, there is exactly one $\xi \in \mathcal{F}$ such that

$$y_{12}(\alpha_{21}^2\alpha_{23}\alpha_{32}^2\alpha_{31}\alpha_{13}^2)^{-1}\xi^3 \in \bigcup_{\rho\in\mathcal{R}_{\mathcal{F}}} \rho R.$$

Hence, there is exactly one $\alpha_{12} := (\alpha_{21}^2\alpha_{23}\alpha_{32}^2\alpha_{31}\alpha_{13}^2)^{-1}\xi^3 \in \mathcal{F}$ such that

$$\underline{\alpha} = (\alpha_{12}, \alpha_{21}, \alpha_{23}, \alpha_{32}, \alpha_{31}, \alpha_{13}) \in H \quad \text{and} \quad \underline{\alpha}\,\boldsymbol{y} \in \mathcal{R}_2. \qquad \square$$

We choose the system $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2$ as in Lemma 2.4, where $\mathcal{R}_1$ is any system of representatives for the diagonal action of $\mathcal{F}$ on $(K^\times)^3$, and $\mathcal{R}_2$ is as in Lemma 2.5.

3. Proof of Theorem 1

This section is a generalization of [Derenthal and Janda 2013, Section 5]. We reduce Theorem 1 to a central lemma (Lemma 3.1), whose proof will take up the rest of the article. We assume that K is of degree $d \geq 2$. Over $\mathbb{Q}$, one would need to replace Lemma 5.2 by a slightly more intricate argument to make the sum over the error terms converge, for which we refer to [Heath-Brown and Moroz 1999].

Möbius inversions. Let $\boldsymbol{C} = (C, C_1, C_2, C_3, C_{21}, C_{32}, C_{13}) \in \mathcal{C}^7$ be fixed. We investigate the quantity $|M_{\boldsymbol{C}} \cap \mathcal{R}(u_{\boldsymbol{C}}B)|$ from Proposition 2.2. We can write

$$|M_{\boldsymbol{C}} \cap \mathcal{R}(u_{\boldsymbol{C}}B)| = \sum_{\substack{\boldsymbol{y} \in \mathcal{R}(u_{\boldsymbol{C}}B) \\ \text{(2-15) holds}}} 1.$$

Möbius inversion for all the coprimality conditions in (2-13) yields

$$|M_{\boldsymbol{C}} \cap \mathcal{R}(u_{\boldsymbol{C}}B)| = \sum_{\substack{(\mathfrak{d}_e)_{e\in E'} \\ \{0\} \neq \mathfrak{d}_e \trianglelefteq \mathcal{O}_K}} \Bigg(\prod_{e\in E'} \mu(\mathfrak{d}_e)\Bigg) \sum_{\substack{\boldsymbol{y} \in \mathcal{R}(u_{\boldsymbol{C}}B) \\ \forall e=\{v,w\}\in E' : y_v \in \mathfrak{d}_e C_v,\, y_w \in \mathfrak{d}_e C_w}} 1, \tag{3-1}$$

where each $\mathfrak{d}_e$ runs over all nonzero ideals of $\mathcal{O}_K$ and μ is the Möbius function for nonzero ideals of $\mathcal{O}_K$. Lemma 3.1 will imply that the last sum is always finite and nonzero for at most finitely many $(\mathfrak{d}_e)_{e\in E'}$. With $\mathfrak{a}_v := \bigcap_{v\in e\in E'} \mathfrak{d}_e C_v$, we obtain

$$\sum_{\substack{\boldsymbol{y} \in \mathcal{R}(u_{\boldsymbol{C}}B) \\ \forall e=\{v,w\}\in E' : y_v \in \mathfrak{d}_e C_v,\, y_w \in \mathfrak{d}_e C_w}} 1 = \sum_{\substack{\boldsymbol{y} \in \mathcal{R}(u_{\boldsymbol{C}}B) \\ \forall v : y_v \in \mathfrak{a}_v}} 1. \tag{3-2}$$

We estimate this sum by the following lemma. Its proof is central to this article and will be given in Section 5.

Lemma 3.1. *For every $v \in V$, let $\mathfrak{a}_v$ be a fractional ideal of K with $\mathfrak{N}\mathfrak{a}_v \geq c$, for some constant $c > 0$ depending only on K. With $\mathcal{R}(B)$ as in (2-17), we have*

$$\sum_{\substack{\boldsymbol{y} \in \mathcal{R}(B) \\ \forall v : y_v \in \mathfrak{a}_v}} 1 = \frac{9^q}{4\cdot 6!}\left(\frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\right)^9 \frac{R_K^7}{\prod_{v\in V}\mathfrak{N}\mathfrak{a}_v} B(\log B)^6 + O\left(\frac{\max_j\{\mathfrak{N}\mathfrak{a}_j\}^{1/d}}{\prod_j \mathfrak{N}\mathfrak{a}_j \prod_{i\neq j}\mathfrak{N}\mathfrak{a}_{ij}^{1-2/(3d)}} B(\log B)^5\right),$$

for $B \geq e$. The implicit O-constant depends on K.

For any $(\mathfrak{d}_e)_{e\in E'}$ and $v \in V$, we define $r_v := \mathfrak{N}(\cap_{v\in e\in E'}\mathfrak{d}_e)$,

$$R_1 := \prod_{v\in V} r_v, \quad \text{and} \quad R_2 := \max_j\{r_j\}^{-1/d}\prod_j r_j \prod_{i\neq j} r_{ij}^{1-2/(3d)}. \tag{3-3}$$

We notice that $\mathfrak{N}\mathfrak{a}_v = \mathfrak{N}(\cap_{v\in e\in E'}\mathfrak{d}_e C_v) = \mathfrak{N}(C_v)r_v$. Recall that we defined $C_{jk} := CC_k^{-2}C_{lk}^{-1}C_j^{-1}C_{kj}^{-1}$ for $jk \in \{12, 23, 31\}$, so

$$\prod_{v\in V} \mathfrak{N}C_v = \mathfrak{N}(C^3C_1^{-2}C_2^{-2}C_3^{-2}C_{21}^{-1}C_{32}^{-1}C_{13}^{-1}) = u_{\boldsymbol{C}}.$$

Since the C, C_j, C_{kj} are members of the fixed finite set $\mathscr{C}$, their absolute norms are bounded from below and above by positive constants depending only on K. With this and Lemma 3.1, we obtain

$$\sum_{\substack{\boldsymbol{y}\in\mathcal{R}(u_{\boldsymbol{C}}B)\\ y_v\in\mathfrak{a}_v}} 1 = \frac{9^q}{4\cdot 6!}\left(\frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\right)^9 R_K^7\frac{B}{R_1}(\log B)^6 + O\Big(\frac{B}{R_2}(\log B)^5\Big),$$

whenever $B \geq e/u_{\boldsymbol{C}}$. Otherwise, the error term dominates the main term. Let

$$\omega := \sum_{\substack{(\mathfrak{d}_e)_{e\in E'}\\ \{0\}\neq\mathfrak{d}_e\trianglelefteq\mathbb{O}_K}} \prod_{e\in E'} \mu(\mathfrak{d}_e)R_1^{-1}, \qquad \rho := \sum_{\substack{(\mathfrak{d}_e)_{e\in E'}\\ \{0\}\neq\mathfrak{d}_e\trianglelefteq\mathbb{O}_K}} \prod_{e\in E'} |\mu(\mathfrak{d}_e)|R_2^{-1}. \tag{3-4}$$

We will see in Lemma 3.2 that these sums converge under our assumption that $d \geq 2$. Since the sum defining ρ converges, (3-1) and (3-2) yield

$$|M_{\boldsymbol{C}} \cap \mathcal{R}(u_{\boldsymbol{C}}B)| = \frac{9^q}{4\cdot 6!}\left(\frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\right)^9 R_K^7\omega B(\log B)^6 + O(B(\log B)^5).$$

Computation of the constant. We notice that the above expression for

$$|M_{\boldsymbol{C}} \cap \mathcal{R}(u_{\boldsymbol{C}}B)|$$

does not depend on $\boldsymbol{C} \in \mathscr{C}^7$. Therefore, Proposition 2.2 implies

$$N(B) = \frac{9^q}{4\cdot 6!}\left(\frac{2^r(2\pi)^s}{\sqrt{|\Delta_K|}}\right)^9 \left(\frac{h_K R_K}{\omega_K}\right)^7 \omega B(\log B)^6 + O(B(\log B)^5).$$

Theorem 1 is an immediate consequence of the following lemma.

Lemma 3.2. *Let ω, ρ be as in (3-4), with R_1, R_2 as in (3-3). If $d \geq 2$ then both sums converge, and*

$$\omega = \prod_{\mathfrak{p}}\Big(1 - \frac{1}{\mathfrak{N}\mathfrak{p}}\Big)^7\Big(1 + \frac{7}{\mathfrak{N}\mathfrak{p}} + \frac{1}{\mathfrak{N}\mathfrak{p}^2}\Big), \tag{3-5}$$

where the product runs over all nonzero prime ideals $\mathfrak{p}$ of $\mathbb{O}_K$.

Proof. The proof is a straightforward generalization of the one in [Derenthal and Janda 2013, Section 5]. An obvious modification of the argument given there shows that the Euler factor of ρ corresponding to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is $1 + O(\mathfrak{N}\mathfrak{p}^{-(6d-5)/(3d)})$, so the sum defining ρ is convergent whenever $d \geq 2$. Since $\omega \leq \rho$, the sum defining ω converges as well.

Let $A(x)$ be the polynomial defined [ibid., Section 5], and $A_{\mathfrak{p}}$ the Euler factor of ω corresponding to $\mathfrak{p}$. Then we have $A_{\mathfrak{p}} = A(\mathfrak{N}\mathfrak{p}^{-1})$, and (3-5) follows from the investigation of $A(x)$ [ibid., Section 5]. □

This completes our proof of Theorem 1, up to proving Lemma 3.1.

4. Auxiliary results

Let n, M be positive integers and $L > 0$. By $\mathrm{Lip}(n, M, L)$ we denote the set of all subsets $\mathcal{B}$ of $\mathbb{R}^n$ for which there exist M maps $\Phi : [0, 1]^{n-1} \to \mathbb{R}^n$ satisfying a Lipschitz condition

$$|\Phi(v) - \Phi(w)| \leq L|v - w|$$

such that $\mathcal{B}$ is covered by the union of the images of the maps Φ. Here, $|\cdot|$ is the usual Euclidean norm. (The subsets in $\mathrm{Lip}(1, M, L)$ are just those with at most M elements.) We will use the following lemma to bound the error terms when estimating a sum by an integral. Part (i) generalizes an argument used in [Lang 1994, Chapter VI, Theorem 2].

Lemma 4.1. *Let $D, \mathcal{B} \subseteq \mathbb{R}^n$ be bounded subsets with $\mathcal{B} \in \mathrm{Lip}(n, M, L)$.*

(i) *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Then*

$$|\{\lambda \in \Lambda \mid (\lambda + D) \cap \mathcal{B} \neq \varnothing\}| \ll_{\Lambda, D} M(L+1)^{n-1}.$$

(ii) *If $D, \mathcal{B}$ are compact then $\{\boldsymbol{x} \in \mathbb{R}^n \mid (x + D) \cap \mathcal{B} \neq \varnothing\}$ is measurable and*

$$\mathrm{Vol}\{\boldsymbol{x} \in \mathbb{R}^n \mid (x + D) \cap \mathcal{B} \neq \varnothing\} \ll_D M(L+1)^{n-1}.$$

Proof. For $x \in \mathbb{R}^n$, we have $(x + D) \cap \mathcal{B} \neq \varnothing$ if and only if $x \in \mathcal{B} - D$. If $\mathcal{B}$ and D are compact, the set $\mathcal{B} - D$ is compact as well. This proves measurability of the set in (ii).

Let $\Phi : [0, 1]^{n-1} \to \mathbb{R}^n$ be one of the M maps with Lipschitz constant L whose images cover $\mathcal{B}$. We split up $[0, 1]^{n-1}$ into L_1^{n-1} subcubes of side length $1/L_1$, where $L_1 := \lfloor L \rfloor + 1$. Let C be one of those subcubes. Then $\Phi(C)$ has diameter at most $\sqrt{n-1}L/L_1 \leq \sqrt{n-1}$, so it is contained in a closed ball $B_z(2\sqrt{n-1})$ of radius $2\sqrt{n-1}$ centered at some point $z \in \mathbb{R}^n$.

Since D is bounded, it is contained in a closed zero-centered ball $B_{\mathbf{0}}(R_D)$ of some radius R_D. Every point $\boldsymbol{x} \in \mathbb{R}^n$ with $(\boldsymbol{x} + D) \cap \Phi(C) \neq \varnothing$ satisfies $\boldsymbol{x} \in B_z(2\sqrt{n-1}) - B_{\mathbf{0}}(R_D) = B_z(2\sqrt{n-1} + R_D)$.

The number of lattice points in such a ball is finite and can be bounded independently from z. Therefore,

$$|\{\lambda \in \Lambda \mid (\lambda + D) \cap \Phi(C) \neq \varnothing\}| \ll_{\Lambda, D} 1. \tag{4-1}$$

Moreover,

$$\mathrm{Vol}\{\boldsymbol{x} \in \mathbb{R}^n \mid (x + D) \cap \Phi(C) \neq \varnothing\} \leq \mathrm{Vol}\, B_z(2\sqrt{n-1} + R_D) \ll_D 1. \tag{4-2}$$

Summing (4-1) and (4-2) over all C and Φ yields (i) and (ii). □

Counting lattice points. We will need to count lattice points in certain bounded subsets of $\mathbb{R}^n$ for lattices $\Lambda \subseteq \mathbb{R}^n$ of the form $\Lambda = \Lambda_1 \times \cdots \times \Lambda_r$, where each Λ_i is a lattice in $\mathbb{R}^{n_i}$ and $n_1 + \cdots + n_r = n$. Then we have $\det(\Lambda) = \det(\Lambda_1) \cdots \det(\Lambda_r)$, and the successive minima (with respect to the unit ball) of Λ are just the successive minima of $\Lambda_1, \ldots, \Lambda_r$. Several authors (for instance [Christensen and Gubler 2008; Masser and Vaaler 2007]) provide counting results where the first successive minimum is reflected in the error term by making an argument from [Lang 1994, Chapter VI, Theorem 2] explicit. For our application, we need the error term to reflect information about all the lattices Λ_i, which is accomplished with the help of a theorem by Widmer.

Theorem 4.2 [Widmer 2010, Theorem 5.4]. *Let Λ be a lattice in $\mathbb{R}^n$ with successive minima (with respect to the unit ball) $\lambda_1, \ldots, \lambda_n$. Let $\mathcal{B}$ be a bounded set in $\mathbb{R}^n$ with boundary $\partial\mathcal{B} \in \mathrm{Lip}(n, M, L)$. Then $\mathcal{B}$ is measurable, and moreover*

$$\left| |\mathcal{B} \cap \Lambda| - \frac{\mathrm{Vol}\,\mathcal{B}}{\det \Lambda} \right| \leq c_0(n) M \max_{0 \leq k < n} \frac{L^k}{\lambda_1 \cdots \lambda_k}.$$

For $k = 0$, the expression in the maximum is to be understood as 1. Furthermore, one can choose $c_0(n) = n^{3n^2/2}$.

Let $\lambda_{i1} \leq \cdots \leq \lambda_{in_i}$ be the successive minima of Λ_i, and assume that the Λ_i are ordered in such a way that $\lambda_{11} \leq \lambda_{21} \leq \cdots \leq \lambda_{r1}$ holds.

Corollary 4.3. *Let Λ and Λ_i be as above, and let $\mathcal{B} \subseteq \mathbb{R}^n$ be a bounded set with boundary $\partial\mathcal{B} \in \mathrm{Lip}(n, M, L)$. Then $\mathcal{B}$ is measurable and*

$$\left| |\mathcal{B} \cap \Lambda| - \frac{\mathrm{Vol}\,\mathcal{B}}{\det \Lambda} \right| \leq c_0(n) M \prod_{i=1}^{r-1} \left(\frac{L}{\lambda_{i1}} + 1 \right)^{n_i} \left(\frac{L}{\lambda_{r1}} + 1 \right)^{n_r - 1}.$$

Proof. We use Theorem 4.2. Let $\lambda_1 \leq \cdots \leq \lambda_n$ be the successive minima of Λ, that is, the λ_{ij} in correct order. Clearly,

$$\max_{0 \leq k < n} \frac{L^k}{\lambda_1 \cdots \lambda_k} \leq \prod_{j=1}^{n-1} \left(\frac{L}{\lambda_j} + 1 \right) \leq \prod_{i=1}^{r} \left(\frac{L}{\lambda_{i1}} + 1 \right)^{n_i} \Big/ \left(\frac{L}{\lambda_{i_0 1}} + 1 \right),$$

where i_0 is chosen such that $\lambda_{i_0 n_{i_0}} = \lambda_n$. The last expression is at most

$$\prod_{i=1}^{r-1}\left(\frac{L}{\lambda_{i1}}+1\right)^{n_i}\left(\frac{L}{\lambda_{r1}}+1\right)^{n_r-1}. \qquad \square$$

Lemma 4.4. *Let Λ and Λ_i be as above, and let $\mathcal{B} \subseteq \mathbb{R}^n$ be contained in a zero-centered ball of radius R. Assume, moreover, that $\partial\mathcal{B} \in \mathrm{Lip}(n, M, L)$, and that the following property holds for all $\boldsymbol{x} \in \mathcal{B}$:*

$$\text{If we write } \boldsymbol{x} = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_r) \text{ with } \boldsymbol{x}_i \in \mathbb{R}^{n_i} \text{ then } \boldsymbol{x}_i \neq \boldsymbol{0} \text{ for all } i. \tag{4-3}$$

Then $\mathcal{B}$ is measurable and, for all $T \geq 0$, we have

$$\left|\,|T\mathcal{B}\cap\Lambda| - \frac{T^n \operatorname{Vol}\mathcal{B}}{\det\Lambda}\right| \ll_{n,M,R,L} \prod_{i=1}^{r-1}\left(\frac{T}{\lambda_{i1}}\right)^{n_i}\left(\frac{T}{\lambda_{r1}}\right)^{n_r-1}.$$

Proof. By Theorem 4.2, $\mathcal{B}$ is measurable. We start with the case where $TR < \lambda_{r1}$. Suppose that $\boldsymbol{a} = (\boldsymbol{a}_1, \dots, \boldsymbol{a}_r) \in T\mathcal{B} \cap \Lambda$. Then $\boldsymbol{a}_r \neq \boldsymbol{0}$ by (4-3). Therefore, $|\boldsymbol{a}| \geq |\boldsymbol{a}_r| \geq \lambda_{r1} > TR$, so $\boldsymbol{a} \notin T\mathcal{B}$, a contradiction. Hence, $|T\mathcal{B}\cap\Lambda| = 0$. Denote by V_1 the volume of a ball of radius 1 in $\mathbb{R}^n$. Then $\operatorname{Vol}\mathcal{B} \leq R^n V_1$. We denote the successive minima of Λ again by $\lambda_1, \dots, \lambda_n$. By Minkowski's second theorem we have

$$\frac{T^n \operatorname{Vol}\mathcal{B}}{\det\Lambda} \leq \frac{V_1 2^n (RT)^n}{\lambda_1 \cdots \lambda_n V_1} \leq 2^n R^{n-1} \prod_{i=1}^{r-1}\left(\frac{T}{\lambda_{i1}}\right)^{n_i}\left(\frac{T}{\lambda_{r1}}\right)^{n_r-1}.$$

Now assume $TR \geq \lambda_{r1}$. Clearly, $\operatorname{Vol}(T\mathcal{B}) = T^n \operatorname{Vol}\mathcal{B}$ and $\partial(T\mathcal{B}) \in \mathrm{Lip}(n, M, TL)$. To finish the proof, we use Corollary 4.3 and observe that

$$\begin{aligned}\prod_{i=1}^{r-1}\left(\frac{TL}{\lambda_{i1}}+1\right)^{n_i}\left(\frac{TL}{\lambda_{r1}}+1\right)^{n_r-1} &\leq \prod_{i=1}^{r-1}\left(\frac{T(L+R)}{\lambda_{i1}}\right)^{n_i}\left(\frac{T(L+R)}{\lambda_{r1}}\right)^{n_r-1}\\ &= (L+R)^{n-1}\prod_{i=1}^{r-1}\left(\frac{T}{\lambda_{i1}}\right)^{n_i}\left(\frac{T}{\lambda_{r1}}\right)^{n_r-1}. \qquad \square\end{aligned}$$

The basic sets. Here, we describe the sets $\mathcal{B}$ to which Lemma 4.4 will be applied. These sets were introduced in [Schanuel 1979] and, in a more general context, in [Masser and Vaaler 2007]. Our notation is similar to that of the latter. When talking about lattices, volumes, etc., we identify $\mathbb{C}$ with $\mathbb{R}^2$.

Let Σ be the hyperplane in $\mathbb{R}^{r+s}$ where $x_1 + \cdots + x_{r+s} = 0$. It is well known that the map $l : K^\times \to \mathbb{R}^{r+s}$ defined by $l(\alpha) = (d_1 \log|\alpha^{(1)}|, \dots, d_{r+s}\log|\alpha^{(r+s)}|)$ induces a group homomorphism of $\mathcal{O}_K^\times$ onto a lattice in Σ, with kernel μ_K. In particular, l induces a group isomorphism from $\mathcal{F}$ to $l(\mathcal{O}_K^\times)$. Let F be a fundamental

parallelotope for this lattice, and let $\delta := (d_1, \dots, d_{r+s}) \in \mathbb{R}^{r+s}$. We define the vector sums

$$F(\infty) := F + \mathbb{R}\delta \quad \text{and} \quad F(T) := F + (-\infty, \log T]\,\delta \quad \text{for } T > 0.$$

Then $F(\infty)$ is a system of representatives for the orbits of the additive action of $l(\mathfrak{F}) = l(\mathbb{O}_K^\times)$ on $\mathbb{R}^{r+s}$. Let $S_F^n(T)$ be the set of all

$$(z_{1,1}, \dots, z_{1,n}, \dots, z_{r+s,1}, \dots, z_{r+s,n}) \in (\mathbb{R}^n \setminus \{\mathbf{0}\})^r \times (\mathbb{C}^n \setminus \{\mathbf{0}\})^s$$

such that

$$\big(d_i \log \max_{1\le j\le n} \{|z_{i,j}|\}\big)_{i=1}^{r+s} \in F(T).$$

Since $F \subseteq \Sigma$ and $d_1 + \cdots + d_{r+s} = d$, this is equivalent to

$$(d_i \log \max_{1\le j\le n} \{|z_{i,j}|\})_{i=1}^{r+s} \in F(\infty) \quad \text{and} \quad \prod_{i=1}^{r+s} \max_{1\le j\le n} \{|z_{i,j}|\}^{d_i} \le T^d.$$

The set $S_F^n(\infty)$ is defined similarly. Here are some basic properties of $S_F^n(T)$:

(i) $S_F^n(T) = T\,S_F^n(1)$ is homogeneously expanding.

(ii) $S_F^n(1)$ is bounded.

(iii) $\partial S_F^n(1) \in \mathrm{Lip}(nd, M_n, L_n)$ for some M_n, L_n.

(iv) $S_F^n(1)$ is measurable and $\mathrm{Vol}\, S_F^n(1) = n^q 2^{nr} \pi^{ns} R_K$.

Properties (i), (ii) follow directly from the definition, and (iii), (iv) are immediate consequences of Lemmas 3 and 4 of [Masser and Vaaler 2007]. Strictly speaking, the case $n = 1$ is not covered in that paper, but the proofs remain correct without change. We need a slightly modified version: Define

$$S_F^{n*}(T) := S_F^n(T) \cap ((\mathbb{R}^\times)^{nr} \times (\mathbb{C}^\times)^{ns}). \tag{4-4}$$

Then (i)–(iv) hold as well for $S_F^{n*}(T)$. This is clear for (i), (ii), (iv). For (iii), let $X := (\mathbb{R}^{nr} \times \mathbb{C}^{ns}) \setminus ((\mathbb{R}^\times)^{nr} \times (\mathbb{C}^\times)^{ns})$. Then $\partial S_F^{n*}(1) \subseteq \partial S_F^n(1) \cup (\overline{S_F^n(1)} \cap X)$. Since $\overline{S_F^n(1)}$ is bounded and X is a union of finitely many proper subspaces, we have $(\overline{S_F^n(1)} \cap X) \in \mathrm{Lip}(nd, M_n', L_n')$, for suitably chosen M_n', L_n', so

$$\partial S_F^{n*}(1) \in \mathrm{Lip}(nd, M_n + M_n', \max\{L_n, L_n'\}).$$

5. Proof of Lemma 3.1

Whenever we use Vinogradov's $\ll$ notation, the implicit constant may depend on K. Let us start by summing over y_1, y_2, y_3, for fixed y_{jk}, y_{kj}. Write

$$V' := V \setminus \{1, 2, 3\} = \{12, 21, 23, 32, 31, 13\}.$$

For any choice of y_v, $v \in V'$, we define $\xi_j := y_{jk} y_{jl} y_{kj}^2 y_{lj}^2$. The height condition in (2-17) implies that

$$|N(y_j)^3 N(\xi_j)| = \prod_{i=1}^{r+s} |\sigma_i(y_j^3 \xi_j)|^{d_i} \le B.$$

For $y_j \in \mathfrak{a}_j$, we obtain $|N(\xi_j)| \le B|N(y_j)|^{-3} \le B\mathfrak{N}\mathfrak{a}_j^{-3}$. By our choice of $\mathcal{R}$ in Lemma 2.4, we can write the sum in Lemma 3.1 as

$$\sum_{\substack{\boldsymbol{y} \in \mathcal{R}(B) \\ y_v \in \mathfrak{a}_v}} 1 = \sum_{\substack{(y_v)_{v \in V'} \in \mathcal{R}_2 \\ y_v \in \mathfrak{a}_v \\ \forall j : |N(\xi_j)| \le B\mathfrak{N}\mathfrak{a}_j^{-3}}} \sum_{\substack{(y_1, y_2, y_3) \in \mathcal{R}_1 \\ y_j \in \mathfrak{a}_j \\ \prod_{i=1}^{r+s} \max_j \{|\sigma_i(y_j^3 \xi_j)|\}^{d_i} \le B}} 1. \tag{5-1}$$

The first summation. Here, we handle the inner sum in (5-1). The necessary tool is provided in Lemma 5.2.

Lemma 5.1. *Let $\mathfrak{a}$ be a fractional ideal of K, and let τ be the linear automorphism of $\mathbb{R}^r \times \mathbb{C}^s$ (regarded as $\mathbb{R}^d$) given by $\tau(z_1, \dots, z_{r+s}) = (t_1 z_1, \dots, t_{r+s} z_{r+s})$, with $t_1, \dots, t_{r+s} > 0$. Let $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ be the standard embedding. Then $\tau \circ \sigma(\mathfrak{a})$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$ of determinant*

$$\det(\tau \circ \sigma(\mathfrak{a})) = t_1^{d_1} \cdots t_{r+s}^{d_{r+s}} \cdot 2^{-s} \cdot \mathfrak{N}(\mathfrak{a}_j) \cdot \sqrt{|\Delta_K|}$$

and first successive minimum $\lambda \ge (t_1^{d_1} \cdots t_{r+s}^{d_{r+s}} \cdot \mathfrak{N}\mathfrak{a})^{1/d}$.

Proof. For $d = 1$, the lemma is trivial, so we assume $d \ge 2$. Classically, $\sigma(\mathfrak{a})$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$ of determinant $2^{-s}\mathfrak{N}(\mathfrak{a}_j)\sqrt{|\Delta_K|}$. Since τ is a linear automorphism of determinant $t_1^{d_1} \cdots t_{r+s}^{d_{r+s}}$, it follows immediately that $\tau \circ \sigma(\mathfrak{a})$ is a lattice with the correct determinant.

For λ, we slightly generalize the argument in [Masser and Vaaler 2007, Lemma 5] (see also [Widmer 2010, Lemma 9.7]). There is an $\alpha \in \mathfrak{a}$ with $\lambda = |\tau \circ \sigma(\alpha)|$. By the inequality of weighted arithmetic and geometric means, we have

$$\lambda^2 = \sum_{i=1}^{r+s} |t_i \alpha^{(i)}|^2 \ge \tfrac{1}{2} \sum_{i=1}^{r+s} d_i |t_i \alpha^{(i)}|^2 \ge \frac{d}{2} \left(\prod_{i=1}^{r+s} |t_i \alpha^{(i)}|^{d_i} \right)^{\frac{2}{d}} \ge \left(t_1^{d_1} \cdots t_{r+s}^{d_{r+s}} |N(\alpha)| \right)^{\frac{2}{d}}.$$

The lemma follows upon noticing that $|N(\alpha)| \ge \mathfrak{N}\mathfrak{a}$. □

Lemma 5.2. *Given constants $C_{ij} > 0$, for $i \in \{1, \dots, r+s\}$ and $j \in \{1, 2, 3\}$, let*

$$C_j := C_{1j}^{d_1} \cdots C_{r+s,j}^{d_{r+s}}.$$

Let $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \ne \{0\}$ be fractional ideals of K, and $\mathcal{R}_1$ a system of representatives

for the orbits of $(K^\times)^3$ *under the action of* $\mathcal{F}$ *by scalar multiplication. Define*

$$M_1(T) := (\mathfrak{a}_1 \times \mathfrak{a}_2 \times \mathfrak{a}_3) \cap \left\{ (y_1, y_2, y_3) \in \mathcal{R}_1 \;\middle|\; \prod_{i=1}^{r+s} \max_{1\le j\le 3} \{C_{ij}|y_j^{(i)}|\}^{d_i} \le T^d \right\}.$$

Then $M_1(T)$ *is finite and*

$$|M_1(T)| = \frac{3^q 2^{3r} (2\pi)^{3s} R_K}{(\sqrt{|\Delta_k|})^3 C_1C_2C_3 \mathfrak{N}\mathfrak{a}_1 \mathfrak{N}\mathfrak{a}_2 \mathfrak{N}\mathfrak{a}_3} T^{3d} + O\left(\frac{T^{3d-1} \max_j\{C_j \mathfrak{N}\mathfrak{a}_j\}^{1/d}}{C_1C_2C_3 \mathfrak{N}\mathfrak{a}_1 \mathfrak{N}\mathfrak{a}_2 \mathfrak{N}\mathfrak{a}_3} \right)$$

for all $T > 0$. *The implicit* O*-constant depends only on* K.

Proof. We notice that $|M_1(T)|$ does not depend on the choice of $\mathcal{R}_1$, since both $\mathfrak{a}_1 \times \mathfrak{a}_2 \times \mathfrak{a}_3$ and the height condition are invariant under scalar multiplication of (y_1, y_2, y_3) by units. Hence, it is enough to prove the lemma with a specific choice of $\mathcal{R}_1$, which we construct below.

Let $\sigma : K^3 \to \mathbb{R}^{3r} \times \mathbb{C}^{3s}$ be the embedding given by $\sigma(\boldsymbol{y}) = (\sigma_i(\boldsymbol{y}))_{i=1}^{r+s}$. For $i \in \{1, \dots, r+s\}$, let ϕ_i be the linear automorphism of $\mathbb{R}^3$ (if $i \le r$) or $\mathbb{C}^3$ (if $i > r$) given by $\phi_i(z_1, z_2, z_3) = (C_{i1}z_1, C_{i2}z_2, C_{i3}z_3)$, and let $\phi : \mathbb{R}^{3r} \times \mathbb{C}^{3s} \to \mathbb{R}^{3r} \times \mathbb{C}^{3s}$ be the automorphism obtained by applying the ϕ_i componentwise.

With $S_F^{3*}(T)$ as in (4-4), we define $\mathcal{R}_1$ as the set of all $\boldsymbol{y} \in (K^\times)^3$ such that $\phi \circ \sigma(\boldsymbol{y}) \in S_F^{3*}(\infty)$. Then $\mathcal{R}_1$ is a system of representatives for the orbits of $(K^\times)^3$ under the action of $\mathcal{F}$ by scalar multiplication. Indeed, for any $\boldsymbol{y} \in (K^\times)^3$ and $\zeta \in \mathcal{F}$, we have

$$(d_i \log \max_{1\le j\le 3} \{|C_{ij}\sigma_i(\zeta y_j)|\})_{i=1}^{r+s} = (d_i \log \max_{1\le j\le 3} \{|C_{ij}\sigma_i(y_j)|\})_{i=1}^{r+s} + l(\zeta),$$

and $F(\infty)$ is a system of representatives for the orbits of the additive action of $l(\mathcal{F})$ on $\mathbb{R}^{r+s}$.

Let $\Lambda := \phi \circ \sigma(\mathfrak{a}_1 \times \mathfrak{a}_2 \times \mathfrak{a}_3)$. Then Λ is a lattice in $\mathbb{R}^{3r} \times \mathbb{C}^{3s}$, and $\phi \circ \sigma$ induces a one-to-one correspondence between $M_1(T)$ and $\Lambda \cap S_F^{3*}(T)$. Therefore,

$$|M_1(T)| = |\Lambda \cap S_F^{3*}(T)|. \tag{5-2}$$

Since $S_F^{3*}(T)$ is bounded, $M_1(T)$ is finite. To simplify the notation, we change the order of coordinates by

$$(z_{11}, z_{12}, z_{13}, \dots, z_{r+s,1}, z_{r+s,2}, z_{r+s,3}) \mapsto (z_{11}, \dots, z_{r+s,1}, \dots, z_{13}, \dots, z_{r+s,3}).$$

This way, $\mathbb{R}^{3r} \times \mathbb{C}^{3s}$ becomes $(\mathbb{R}^r \times \mathbb{C}^s)^3$, and Λ becomes

$$\Lambda = \tau_1 \circ \sigma(\mathfrak{a}_1) \times \tau_2 \circ \sigma(\mathfrak{a}_2) \times \tau_3 \circ \sigma(\mathfrak{a}_3),$$

where $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ is the standard embedding given by $\sigma(y) = (\sigma_i(y))_{i=1}^r$ and

$$\tau_j(z_1, \dots, z_{r+s}) := (C_{1j}z_1, \dots, C_{r+s,j}z_{r+s}).$$

Each $\Lambda_j := \tau_j \circ \sigma(\mathfrak{a}_j)$ is a lattice in $\mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$. Let λ_j be the first successive minimum of Λ_j. By Lemma 5.1, we have

$$\det \Lambda = \det \Lambda_1 \cdot \det \Lambda_2 \cdot \det \Lambda_3 = 2^{-3s}(\sqrt{|\Delta_K|})^3 C_1 C_2 C_3 \mathfrak{N}\mathfrak{a}_1 \mathfrak{N}\mathfrak{a}_2 \mathfrak{N}\mathfrak{a}_3$$

and $\lambda_j \geq (C_j \mathfrak{N}\mathfrak{a}_j)^{1/d}$. The lemma now follows from (5-2), Lemma 4.4 and the properties of the basic sets discussed on pages 1464–1465. □

The inner sum in (5-1) is exactly $|M_1(T)|$ in Lemma 5.2, with

$$C_{ij} := |\sigma_i(\xi_j)|^{1/3}, \quad C_j := |N(\xi_j)|^{1/3} \quad \text{and} \quad T := B^{1/(3d)}.$$

Observe that $C_1 C_2 C_3 = |N(\xi_1 \xi_2 \xi_3)|^{1/3} = \prod_{v \in V'} |N(y_v)|$. We define

$$\mathcal{M}(B, (\mathfrak{a}_v)_v) := \sum_{\substack{(y_v)_{v \in V'} \in \mathcal{R}_2 \\ y_v \in \mathfrak{a}_v \\ \forall j : |N(\xi_j)| \leq B \mathfrak{N}\mathfrak{a}_j^{-3}}} \frac{1}{\prod_{v \in V'} |N(y_v)|}, \tag{5-3}$$

$$\mathcal{R}(B, (\mathfrak{a}_v)_v) := \sum_{\substack{(y_v)_{v \in V'} \in \mathcal{R}_2 \\ y_v \in \mathfrak{a}_v \\ \forall j : |N(\xi_j)| \leq B \mathfrak{N}\mathfrak{a}_j^{-3}}} \frac{\max_j \{|N(\xi_j)|\}^{1/(3d)}}{\prod_{v \in V'} |N(y_v)|}. \tag{5-4}$$

Then (5-1) and Lemma 5.2 imply

$$\sum_{\substack{\boldsymbol{y} \in \mathcal{R}(B) \\ y_v \in \mathfrak{a}_v}} 1 = \frac{3^q 2^{3r} (2\pi)^{3s} R_K B}{(\sqrt{|\Delta_K|})^3 \mathfrak{N}\mathfrak{a}_1 \mathfrak{N}\mathfrak{a}_2 \mathfrak{N}\mathfrak{a}_3} \mathcal{M}(B, (\mathfrak{a}_v)_v) + O\left(\frac{\max_j \{\mathfrak{N}\mathfrak{a}_j\}^{1/d}}{\mathfrak{N}\mathfrak{a}_1 \mathfrak{N}\mathfrak{a}_2 \mathfrak{N}\mathfrak{a}_3} B^{1-1/(3d)} \mathcal{R}(B, (\mathfrak{a}_v)_v) \right). \tag{5-5}$$

Recall that the $\mathfrak{N}\mathfrak{a}_v$ are bounded from below by a positive constant c depending only on K. This implies, for example,

$$\mathfrak{N}(\mathfrak{a}_{jk} \mathfrak{a}_{jl} \mathfrak{a}_{kj}^2 \mathfrak{a}_{lj}^2)^{1/(3d)} \ll \prod_{v \in V'} \mathfrak{N}\mathfrak{a}_v^{2/(3d)}, \tag{5-6}$$

$$\mathfrak{N}(\mathfrak{a}_j^3 \mathfrak{a}_{jk} \mathfrak{a}_{jl} \mathfrak{a}_{kj}^2 \mathfrak{a}_{lj}^2)^{-1} \leq c_2, \tag{5-7}$$

for some constant $c_2 \geq 1$ depending only on K.

The error term. With $\mathcal{R}_2$ as in Lemma 2.5, the term $\mathcal{R}(B, (\mathfrak{a}_v)_v)$ has the form

$$\mathcal{R}(B, (\mathfrak{a}_v)_v) = \sum_{\rho \in R_{\mathcal{F}}} \sum_{\substack{\forall v \neq 12 : y_v \in R \cap \mathfrak{a}_v \\ y_{12} \in \rho R \cap \mathfrak{a}_{12} \\ \forall j : |N(\xi_j)| \leq B \mathfrak{N}\mathfrak{a}_j^{-3}}} \frac{\max_j \{|N(\xi_j)|\}^{1/(3d)}}{\prod_{v \in V'} |N(y_v)|}.$$

Both R and ρR are systems of representatives for $K^\times/\mathcal{F}$, so they contain exactly ω_K generators for every nonzero principal fractional ideal of K. Let H_v be the principal fractional ideal $H_v = y_v\mathbb{O}_K$. The norm condition and the summand in the inner sum depend only on $(H_v)_{v\in V'}$. Therefore, the sum does not depend on ρ. Since $|\mathcal{R}_\mathcal{F}| = 3^q \ll 1$, we obtain

$$\mathcal{R}(B,(\mathfrak{a}_v)_v) \ll \sum_{\substack{\{0\}\neq H_v\in P_K,\ v\in V'\\ H_v\subseteq\mathfrak{a}_v\\ \forall j:\mathfrak{N}(H_{jk}H_{jl}H_{kj}^2H_{lj}^2)\le B\mathfrak{N}\mathfrak{a}_j^{-3}}} \frac{\max_j\{\mathfrak{N}(H_{jk}H_{jl}H_{kj}^2H_{lj}^2)\}^{1/(3d)}}{\prod_{v\in V'}\mathfrak{N}(H_v)}.$$

We replace H_v by $H_v\mathfrak{a}_v^{-1}\trianglelefteq\mathbb{O}_K$ and use (5-6), (5-7) to bound this sum by

$$\ll \frac{1}{\prod_{v\in V'}\mathfrak{N}(\mathfrak{a}_v)^{1-2/(3d)}} \sum_{\substack{\{0\}\neq H_v\trianglelefteq\mathbb{O}_K,\ v\in V'\\ H_v\in[\mathfrak{a}_v]^{-1}\\ \forall j:\mathfrak{N}(H_{jk}H_{jl}H_{kj}^2H_{lj}^2)\le c_2B}} \frac{\max_j\{\mathfrak{N}(H_{jk}H_{jl}H_{kj}^2H_{lj}^2)\}^{1/(3d)}}{\prod_{v\in V'}\mathfrak{N}(H_v)}.$$

Let us denote the above sum by $\mathcal{R}_1(B,(\mathfrak{a}_v)_v)$. What follows is a rather straightforward generalization of arguments used by Heath-Brown and Moroz [1999] and Derenthal and Janda [2013]. By symmetry, we may assume that the maximum in the summand is taken for $j=1$. This allows us to bound $\mathcal{R}_1(B,(\mathfrak{a}_v)_v)$ by

$$\ll \sum_{\substack{\{0\}\neq H_v\trianglelefteq\mathbb{O}_K,\ v\in V'\\ \forall j:\mathfrak{N}(H_{jk}H_{jl}H_{kj}^2H_{lj}^2)\le c_2B}} \frac{1}{\mathfrak{N}(H_{12}H_{13})^{1-1/(3d)}\mathfrak{N}(H_{21}H_{31})^{1-2/(3d)}\mathfrak{N}(H_{23}H_{32})}$$

$$\ll \sum_{\substack{\{0\}\neq H_{ij}\trianglelefteq\mathbb{O}_K,\ i\neq1\\ \mathfrak{N}H_{ij}\le c_2B}} \frac{1}{\mathfrak{N}(H_{21}H_{31})^{1-2/(3d)}\mathfrak{N}(H_{23}H_{32})} \sum_{\substack{\{0\}\neq U\trianglelefteq\mathbb{O}_K\\ \mathfrak{N}U\le u}} \frac{d(U)}{\mathfrak{N}U^{1-1/(3d)}},$$

where $u := c_2B\mathfrak{N}(H_{21}H_{31})^{-2}$ and d is the divisor function for nonzero ideals.

Lemma 5.3. *For $T\ge1$, we have*

$$\sum_{\substack{\{0\}\neq\mathfrak{a}\trianglelefteq\mathbb{O}_K\\ \mathfrak{N}\mathfrak{a}\le T}} \mathfrak{N}\mathfrak{a}^\alpha \ll \begin{cases} T^{\alpha+1} & \text{if } -1<\alpha\le0,\\ \max\{1,\log T\} & \text{if } \alpha=-1.\end{cases}$$

Proof. This is a straightforward generalization of [Derenthal and Janda 2013, Lemma 4]. The proof uses Abel's summation formula and the well known fact that

$$|\{\{0\}\neq\mathfrak{a}\trianglelefteq\mathbb{O}_K \mid \mathfrak{N}\mathfrak{a}\le T\}| \ll T. \qquad \square$$

In the following computation, the sums run over nonzero ideals of $\mathcal{O}_K$. Using Lemma 5.3, we obtain

$$\begin{aligned}\sum_{\mathfrak{N}U\le u}\frac{d(U)}{\mathfrak{N}U^{1-1/(3d)}} &= \sum_{\mathfrak{N}U\le u}\sum_{V\mid U}\mathfrak{N}U^{-1+1/(3d)}\\ &= \sum_{\mathfrak{N}V\le u}\mathfrak{N}V^{-1+1/(3d)}\sum_{\mathfrak{N}U\le u/\mathfrak{N}V}\mathfrak{N}U^{-1+1/(3d)}\\ &\ll \sum_{\mathfrak{N}V\le c_2B}\mathfrak{N}V^{-1+1/(3d)}(u/\mathfrak{N}V)^{1/(3d)} \ll u^{1/(3d)}\log B.\end{aligned}$$

Therefore,

$$\begin{aligned}\mathcal{R}_1(B,(\mathfrak{a}_v)_v) &\ll B^{1/(3d)}\log B\sum_{\substack{\{0\}\neq H_{ij}\trianglelefteq\mathcal{O}_K,\,i\neq 1\\ \mathfrak{N}H_{ij}\le c_2B}}\frac{1}{\mathfrak{N}(H_{21}H_{31}H_{23}H_{32})}\\ &\ll B^{1/(3d)}(\log B)^5.\end{aligned}$$

Having estimated $\mathcal{R}_1(B,(\mathfrak{a}_v)_v)$ and thus $\mathcal{R}(B,(\mathfrak{a}_v)_v)$, we obtain from (5-5):

$$\begin{aligned}\sum_{\substack{\boldsymbol{y}\in\mathcal{R}(B)\\ y_v\in\mathfrak{a}_v}}1 &= \frac{3^q2^{3r}(2\pi)^{3s}R_KB}{(\sqrt{|\Delta_K|})^3\mathfrak{N}\mathfrak{a}_1\mathfrak{N}\mathfrak{a}_2\mathfrak{N}\mathfrak{a}_3}\mathcal{M}(B,(\mathfrak{a}_v)_v)\\ &\quad+O\biggl(\frac{\max_j\{\mathfrak{N}\mathfrak{a}_j\}^{1/d}}{\prod_j\mathfrak{N}\mathfrak{a}_j\prod_{i\neq j}\mathfrak{N}\mathfrak{a}_{ij}^{1-2/(3d)}}B(\log B)^5\biggr).\end{aligned}\tag{5-8}$$

The main term. Just as before, we have

$$\mathcal{M}(B,(\mathfrak{a}_v)_v)=\sum_{\rho\in R_{\mathcal{F}}}\sum_{\substack{\forall v\neq 12:\,y_v\in R\cap\mathfrak{a}_v\\ y_{12}\in\rho R\cap\mathfrak{a}_{12}\\ \forall j:|N(\xi_j)|\le B\mathfrak{N}\mathfrak{a}_j^{-3}}}\frac{1}{\prod_{v\in V'}|N(y_v)|}.$$

For all $v\in V'$, let $\mathfrak{b}_v\in\mathscr{C}$ with $[\mathfrak{b}_v]=[\mathfrak{a}_v]$, and $t_v\in K^\times$ with $t_v\mathfrak{a}_v=\mathfrak{b}_v$. Moreover, we define $b_j:=\mathfrak{N}(\mathfrak{a}_j^3\mathfrak{a}_{jk}\mathfrak{a}_{jl}\mathfrak{a}_{kj}^2\mathfrak{a}_{lj}^2)^{-1}\mathfrak{N}(\mathfrak{b}_{jk}\mathfrak{b}_{jl}\mathfrak{b}_{kj}^2\mathfrak{b}_{lj}^2)$. Then (5-7) implies that

$$b_j\le c_3\quad\text{for all }\ j\in\{1,2,3\},\tag{5-9}$$

with a constant $c_3\ge 1$ depending only on K. We replace y_v by t_vy_v and obtain

$$\mathcal{M}(B,(\mathfrak{a}_v)_v)=\biggl(\prod_{v\in V'}\frac{\mathfrak{N}\mathfrak{b}_v}{\mathfrak{N}\mathfrak{a}_v}\biggr)\sum_{\rho\in\mathcal{R}_{\mathcal{F}}}\sum_{\substack{\forall v\neq 12:\,y_v\in t_vR\cap\mathfrak{b}_v\\ y_{12}\in t_v\rho R\cap\mathfrak{b}_{12}\\ \forall j:|N(\xi_j)|\le b_jB}}\frac{1}{\prod_{v\in V'}|N(y_v)|}.$$

Again, the inner sum does not depend on the sets of representatives $t_v R$, $t_v \rho R$ for $K^\times/\mathcal{F}$. Thus,

$$\mathcal{M}(B,(\mathfrak{a}_v)_v) = 3^q \Big(\prod_{v\in V'} \frac{\mathfrak{N}\mathfrak{b}_v}{\mathfrak{N}\mathfrak{a}_v}\Big) \sum_{\substack{y_v\in R\cap\mathfrak{b}_v, v\in V' \\ \forall j:|N(\xi_j)|\le b_j B}} \frac{1}{\prod_{v\in V'}|N(y_v)|}, \tag{5-10}$$

where R is any system of representatives for $K^\times/\mathcal{F}$. Let $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ be the standard embedding, and let $S_F^1(T)$ be defined as on page 1465. We choose R to be the set of all $y \in K^\times$ with $\sigma(y) \in S_F^1(\infty)$. This is indeed a set of representatives for $K^\times/\mathcal{F}$: For any $y \in K^\times$, $\zeta \in \mathcal{F}$, we have

$$(d_i \log|\sigma_i(\zeta y)|)_{i=1}^{r+s} = (d_i \log|\sigma_i(y)|)_{i=1}^{r+s} + l(\zeta),$$

and $F(\infty)$ is a system of representatives for the orbits of the additive action of $l(\mathcal{F})$ on $\mathbb{R}^{r+s}$. We will first consider the sum

$$\mathcal{M}_1(B,(\mathfrak{b}_v)_v) := \sum_{\substack{y_v\in R\cap\mathfrak{b}_v, v\in V' \\ \forall j:|N(\xi_j)|\le B}} \frac{1}{\prod_{v\in V'}|N(y_v)|}.$$

For any $z \in \mathbb{R}^r \times \mathbb{C}^s$, let $N(z) := |z_1|^{d_1} \cdots |z_{r+s}|^{d_{r+s}}$. We define $M(B)$ as the set of all $(z_v)_{v\in V'} \in (\mathbb{R}^r \times \mathbb{C}^s)^6$ such that

$$\begin{aligned} &\text{for all } v \in V', \text{ we have } z_v \in S_F^1(\infty) \text{ and } N(z_v) \ge 1, \text{ and} \\ &\text{for all } j, \text{ we have } N(z_{jk})N(z_{jl})N(z_{kj})^2 N(z_{lj})^2 \le B. \end{aligned}$$

Then $M(B)$ is bounded for all B. Let Λ be the lattice in $(\mathbb{R}^r \times \mathbb{C}^s)^6$ defined by

$$\Lambda := \prod_{v\in V'} \sigma(\mathfrak{b}_v).$$

By the componentwise extension of σ to K^6, we obtain

$$\mathcal{M}_1(B,(\mathfrak{b}_v)_v) = \sum_{(z_v)_v\in\Lambda\cap M(B)} \frac{1}{\prod_{v\in V'} N(z_v)}. \tag{5-11}$$

We identify $\mathbb{C}$ with $\mathbb{R}^2$ and estimate this sum by an integral. Let

$$I(B) := \Big(\frac{2^s}{\sqrt{|\Delta_K|}}\Big)^6 \frac{1}{\prod_{v\in V'}\mathfrak{N}\mathfrak{b}_v} \int_{M(B)} \prod_{v\in V'} \frac{dz_v}{N(z_v)}.$$

Lemma 5.4. *We have*

$$\sum_{(z_v)_v\in\Lambda\cap M(B)} \frac{1}{\prod_{v\in V'} N(z_v)} = I(B) + O((\log B)^5)$$

for $B \ge e$. The implicit O-constant depends on K.

Proof. This is a generalization of [Derenthal and Janda 2013, Lemma 5]. Let us fix some notation. For $v \in V'$, let F_v be a fundamental parallelotope for the lattice $\sigma(\mathfrak{b}_v) \subseteq \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d$, and let R_v be the minimal d-dimensional interval containing F_v. We denote the side lengths of R_v by $l_{v,1}, \dots, l_{v,d}$. For any $\boldsymbol{z} = (z_1, \dots, z_d) \in \mathbb{R}^d$ satisfying

$$|z_i| \geq 1 + l_{v,i} \text{ for all } i \in \{1, \dots, d\}, \tag{5-12}$$

let $R_v(\boldsymbol{z})$ be the (unique) translate of R_v such that $\boldsymbol{z}$ is the corner of $R_v(\boldsymbol{z})$ at utmost distance from the origin, and let $F_v(\boldsymbol{z})$ be the (unique) translate of F_v contained in $R_v(\boldsymbol{z})$. Similarly, for any $\boldsymbol{z}$ with

$$|z_i| \geq 1 \text{ for all } i \in \{1, \dots, d\}, \tag{5-13}$$

let $R'_v(\boldsymbol{z})$ be the (unique) translate of R_v such that $\boldsymbol{z}$ is the corner of $R'_v(\boldsymbol{z})$ closest to the origin, and let $F'_v(\boldsymbol{z})$ be the (unique) translate of F_v contained in $R'_v(\boldsymbol{z})$. Consistently with the above definition of $N(\boldsymbol{z})$ for $\boldsymbol{z} \in \mathbb{R}^r \times \mathbb{C}^s$, we let

$$N(\boldsymbol{z}) := |z_1 \cdots z_r (z_{r+1}^2 + z_{r+2}^2) \cdots (z_{d-1}^2 + z_d^2)|.$$

Since $N(\boldsymbol{z}) \geq N(\boldsymbol{y})$ for all $\boldsymbol{y} \in F_v(\boldsymbol{z})$, we have

$$\frac{1}{N(\boldsymbol{z})} \leq \frac{1}{\operatorname{Vol} F_v(\boldsymbol{z})} \int_{F_v(\boldsymbol{z})} \frac{d\boldsymbol{y}}{N(\boldsymbol{y})} = \frac{2^s}{\sqrt{|\Delta_K|}\mathfrak{N}\mathfrak{b}_v} \int_{F_v(\boldsymbol{z})} \frac{d\boldsymbol{y}}{N(\boldsymbol{y})}. \tag{5-14}$$

Similarly,

$$\frac{1}{N(\boldsymbol{z})} \geq \frac{1}{\operatorname{Vol} F'_v(\boldsymbol{z})} \int_{F'_v(\boldsymbol{z})} \frac{d\boldsymbol{y}}{N(\boldsymbol{y})} = \frac{2^s}{\sqrt{|\Delta_K|}\mathfrak{N}\mathfrak{b}_v} \int_{F'_v(\boldsymbol{z})} \frac{d\boldsymbol{y}}{N(\boldsymbol{y})}. \tag{5-15}$$

Clearly, if $\boldsymbol{z} \neq \boldsymbol{z}' \in \sigma(\mathfrak{b}_v)$ with (5-12) then $F_v(\boldsymbol{z}) \cap F_v(\boldsymbol{z}') = \varnothing$. Let us first prove that

$$\sum_{(\boldsymbol{z}_v)_v \in \Lambda \cap M(B)} \frac{1}{\prod_{v \in V'} N(\boldsymbol{z}_v)} \leq I(B) + O((\log B)^5). \tag{5-16}$$

To this end, we define

$$E(B) := \{(\boldsymbol{z}_v)_v \in M(B) \mid \text{ all } \boldsymbol{z}_v \text{ satisfy (5-12) and } F_v(\boldsymbol{z}_v) \subseteq S_F^1(\infty)\},$$

and $G(B) := M(B) \setminus E(B)$. Keep in mind that $E(B)$ and $G(B)$ depend on $(\mathfrak{b}_v)_{v \in V'}$. For any $(\boldsymbol{z}_v)_v \in \Lambda \cap E(B)$, we have $\prod_v F_v(\boldsymbol{z}_v) \subseteq M(B)$. Therefore,

$$\begin{aligned}\sum_{(\boldsymbol{z}_v)_v \in \Lambda \cap E(B)} \frac{1}{\prod_{v \in V'} N(\boldsymbol{z}_v)} &\leq \sum_{(\boldsymbol{z}_v)_v \in \Lambda \cap E(B)} \prod_{v \in V'} \frac{2^s}{\sqrt{|\Delta_K|}\mathfrak{N}\mathfrak{b}_v} \int_{F_v(\boldsymbol{z}_v)} \frac{d\boldsymbol{y}}{N(\boldsymbol{y})} \\ &\leq \left(\frac{2^s}{\sqrt{|\Delta_K|}}\right)^6 \frac{1}{\prod_{v \in V'} \mathfrak{N}\mathfrak{b}_v} \sum_{(\boldsymbol{z}_v)_v \in \Lambda \cap E(B)} \prod_{v \in V'} \int_{F_v(\boldsymbol{z}_v)} \frac{d\boldsymbol{z}_v}{N(\boldsymbol{z}_v)} \leq I(B).\end{aligned}$$

We need to prove that

$$\sum_{(z_v)_v \in \Lambda \cap G(B)} \frac{1}{\prod_{v \in V'} N(z_v)} = O((\log B)^5). \tag{5-17}$$

For every $(z_v)_v \in \Lambda \cap G(B)$, there is at least one $w \in V'$ such that either

$$z_w \text{ does not satisfy (5-12)} \tag{5-18}$$

or

$$z_w \text{ satisfies (5-12) and } F_w(z_w) \not\subseteq S_F^1(\infty). \tag{5-19}$$

Therefore, we have

$$\begin{aligned}
&\sum_{(z_v)_v \in \Lambda \cap G(B)} \frac{1}{\prod_{v \in V'} N(z_v)} \\
&\qquad \le \sum_{w \in V'} \sum_{\substack{(z_v)_v \in \Lambda \cap S_F^1(\infty)^6 \\ N(z_v) \le B \\ \text{(5-18) or (5-19)}}} \frac{1}{\prod_{v \in V'} N(z_v)} \\
&\qquad = \sum_{w \in V'} \Bigg(\prod_{v \ne w} \sum_{\substack{z \in \sigma(\mathfrak{b}_v) \cap S_F^1(\infty) \\ N(z) \le B}} \frac{1}{N(z)} \Bigg) \sum_{\substack{z \in \sigma(\mathfrak{b}_w) \cap S_F^1(\infty) \\ N(z) \le B \\ \text{(5-18) or (5-19) for } z}} \frac{1}{N(z)}.
\end{aligned} \tag{5-20}$$

Now

$$\sum_{\substack{z \in \sigma(\mathfrak{b}_v) \cap S_F^1(\infty) \\ N(z) \le B}} \frac{1}{N(z)} = \omega_K \sum_{\substack{\{0\} \ne H \in P_K \\ H \subseteq \mathfrak{b}_v \\ \mathfrak{N}H \le B}} \frac{1}{\mathfrak{N}H} \le \sum_{\substack{\{0\} \ne H \trianglelefteq \mathbb{O}_K \\ \mathfrak{N}H \le B}} \frac{1}{\mathfrak{N}H} \ll \log B, \tag{5-21}$$

by Lemma 5.3. Moreover, we write

$$\sum_{\substack{z \in \sigma(\mathfrak{b}_w) \cap S_F^1(\infty) \\ N(z) \le B \\ \text{(5-18) or (5-19) for } z}} \frac{1}{N(z)} = \sum_{n=1}^{B} a_n \cdot \frac{1}{n}, \tag{5-22}$$

with $a_n := \big|\{z \in \sigma(\mathfrak{b}_w) \cap S_F^1(\infty) \mid N(z) = n, \text{ (5-18) or (5-19) holds for } z\}\big|$. We will apply the Abel sum formula, so we need to understand

$$A(T) := \sum_{n \le T} a_n = \big|\{z \in \sigma(\mathfrak{b}_w) \cap S_F^1(T^{1/d}) \mid \text{(5-18) or (5-19) holds for } z\}\big|.$$

Let

$$H := \{z \in \mathbb{R}^d \mid z_1 \cdots z_d = 0\}, \tag{5-23}$$

and let D_w be the d-dimensional interval

$$D_w := [-(l_{w,1}+1), l_{w,1}+1] \times \cdots \times [-(l_{w,d}+1), l_{w,d}+1] \subseteq \mathbb{R}^d. \tag{5-24}$$

Then any z counted by $A(T)$ satisfies $(z + D_w) \cap H \neq \varnothing$ (if (5-18) holds) or $z + D_w \not\subseteq S_F^1(T^{1/d})$ (if (5-19) holds). Therefore, any such z is contained in $A_1(T) \cup A_2(T)$, where

$$\begin{aligned} A_1(T) &:= \{z \in \sigma(\mathfrak{b}_w) \mid (z + D_w) \cap \partial S_F^1(T^{1/d}) \neq \varnothing\} \\ &\supseteq \{z \in \sigma(\mathfrak{b}_w) \cap S_F^1(T^{1/d}) \mid (z + D_w) \not\subseteq S_F^1(T^{1/d})\}, \\ A_2(T) &:= \{z \in \sigma(\mathfrak{b}_w) \mid (z + D_w) \cap (S_F^1(T^{1/d}) \cap H) \neq \varnothing\} \\ &\supseteq \{z \in \sigma(\mathfrak{b}_w) \cap S_F^1(T^{1/d}) \mid (z + D_w) \subseteq S_F^1(T^{1/d}), (z_w + D_w) \cap H \neq \varnothing\}. \end{aligned}$$

Now $\partial S_F^1(T^{1/d}) = T^{1/d} \partial S_F^1(1) \in \mathrm{Lip}(d, M_1, T^{1/d} L_1)$. We recall that $\mathfrak{b}_v \in \mathscr{C}$, so Lemma 4.1(i) implies that

$$|A_1(T)| \ll M_1 (L_1 T^{1/d} + 1)^{d-1} \ll T^{(d-1)/d} \quad \text{for all } T \geq 1.$$

Moreover, $S_F^1(T^{1/d}) \cap H = T^{1/d}(S_F^1(1) \cap H)$, and clearly $S_F^1(1) \cap H \in \mathrm{Lip}(d, \tilde{M}_1, \tilde{L}_1)$ for some $\tilde{M}_1$ and $\tilde{L}_1$. By Lemma 4.1(i),

$$|A_2(T)| \ll \tilde{M}_1 (\tilde{L}_1 T^{1/d} + 1)^{d-1} \ll T^{(d-1)/d} \quad \text{for all } T \geq 1.$$

Therefore, $A(T) \ll T^{(d-1)/d}$ for $T \geq 1$. The Abel sum formula yields

$$\sum_{n=1}^{B} a_n \cdot \frac{1}{n} = A(B)/B + \int_{t=1}^{B} A(t)/t^2 \, dt \ll B^{-1/d} + \int_{t=1}^{B} t^{-(1+1/d)} dt \ll 1.$$

With (5-20), (5-21), (5-22), we see that (5-17) holds, which finishes the proof of (5-16). Let us prove the other inequality, that is

$$I(B) \leq \sum_{(z_v)_v \in \Lambda \cap M(B)} \frac{1}{\prod_{v \in V'} N(z_v)} + O((\log B)^5). \tag{5-25}$$

For every $v \in V'$ and every $z \in \mathbb{R}^d$ satisfying (5-12), there is a unique $\lambda_v(z) \in \sigma(\mathfrak{b}_v)$ with (5-13) such that $z \in F_v'(\lambda_v(z))$. In a similar way as above, we define

$$E'(B) := \{(z_v)_v \in M(B) \mid \text{ all } z_v \text{ satisfy (5-12) and } \lambda_v(z_v) \in S_F^1(\infty)\},$$

and $G'(B) := M(B) \setminus E'(B)$. Both $E'(B)$ and $G'(B)$ are clearly measurable. For any $(z_v)_v$ in $E'(B)$, the point $(\lambda_v(z_v))_v$ is the unique element of $\Lambda \cap M(B)$ with

$z_v \in F_v'(\lambda_v(z_v))$ for all $v \in V'$. With this and (5-15), we obtain

$$\frac{2^{6s}}{(\sqrt{|\Delta_K|})^6 \prod_{v\in V'} \mathfrak{Nb}_v} \int_{E'(B)} \prod_{v\in V'} \frac{dz_v}{N(z_v)} \le \sum_{\substack{(\lambda_v)_v \in \\ \Lambda\cap M(B)}} \prod_{v\in V'} \frac{2^s}{\sqrt{|\Delta_K|}\mathfrak{Nb}_v} \int_{F_v'(\lambda_v)} \frac{dz}{N(z)}$$
$$\le \sum_{(\lambda_v)_v\in\Lambda\cap M(B)} \frac{1}{\prod_{v\in V'} N(\lambda_v)}. \tag{5-26}$$

We need to prove that

$$\left(\frac{2^s}{\sqrt{|\Delta_K|}}\right)^6 \frac{1}{\prod_{v\in V'} \mathfrak{Nb}_v} \int_{G'(B)} \prod_{v\in V'} \frac{dz_v}{N(z_v)} = O((\log B)^5). \tag{5-27}$$

For every $(z_v)_v \in G'(B)$, there is some $w \in V'$ such that either

$$z_w \text{ does not satisfy (5-12)} \tag{5-28}$$

or

$$z_w \text{ satisfies (5-12) and } \lambda_w(z_w) \notin S_F^1(\infty). \tag{5-29}$$

Similarly to (5-20), we obtain

$$\int_{G'(B)} \prod_{v\in V'} \frac{dz_v}{N(z_v)} \le \sum_{w\in V'} \left(\prod_{v\ne w} \int_{\substack{z\in S_F^1(\infty)\\ 1\le N(z)\le B}} \frac{dz}{N(z)}\right) \int_{\substack{z\in S_F^1(\infty)\\ 1\le N(z)\le B\\ \text{(5-28) or (5-29) for } z}} \frac{dz}{N(z)}. \tag{5-30}$$

We denote the Lebesgue measure on $\mathbb{R}$, $\mathbb{R}^d$ by m_1, m_d. The restriction of N to $S_F^1(\infty)$ defines a measurable function $N_1 : S_F^1(\infty) \to \mathbb{R}$. Since

$$(m_d \circ N_1^{-1})((a,b]) = \operatorname{Vol} S_F^1(b^{1/d}) - \operatorname{Vol} S_F^1(a^{1/d}) = (b-a)\operatorname{Vol} S_F^1(1)$$

for all $0 < a \le b \in \mathbb{R}$, we obtain $m_d \circ N_1^{-1} = \operatorname{Vol} S_F^1(1) m_1$ on $\mathbb{R}^{>0}$. Therefore,

$$\int_{\substack{z\in S_F^1(\infty)\\ 1\le N(z)\le B}} \frac{dz}{N(z)} = \int_{N_1^{-1}([1,B])} \frac{dm_d}{N_1(z)} = \int_{[1,B]} \frac{1}{t}\, d(m_d \circ N_1^{-1}) = \operatorname{Vol} S_F^1(1) \log B. \tag{5-31}$$

Let $A(T) := \{z \in S_F^1(\infty) \mid 1 \le N(z) \le T$, (5-28) or (5-29) holds for $z\}$. Then $A(T)$ is measurable for all T and the restriction of N to $A(B)$ defines a measurable function $N_2 : A(B) \to [1, B]$. For any $E \subseteq [1, B]$ with $m_1(E) = 0$, we have $N_2^{-1}(E) \subseteq N_1^{-1}(E)$ and $(m_d \circ N_1^{-1})(E) = 0$. Thus, $m_d \circ N_2^{-1}$ is absolutely continuous. With the distribution function $F(T) := (m_d \circ N_2^{-1})([1, T])$, we obtain

$$\int_{A(B)} \frac{dz}{N(z)} = \int_{N_2^{-1}([1,B])} \frac{dm_d}{N_2(z)} = \int_{[1,B]} \frac{1}{t}\, d(m_d \circ N_2^{-1}) = \int_1^B \frac{1}{t}\, dF(t). \tag{5-32}$$

Integration by parts for the Stieltjes integral on the right-hand side suggests that we need to find a suitable bound for $F(T)$. Clearly,

$$F(T) = \mathrm{Vol}(N_2^{-1}([1,T])) = \mathrm{Vol}\, A(T).$$

With H, D_w as in (5-23), (5-24), let

$$A_1(T) := \{z \in \mathbb{R}^d \mid (z + D_w) \cap \partial S_F^1(T^{1/d}) \neq \varnothing\},$$
$$A_2(T) := \{z \in \mathbb{R}^d \mid (z + D_w) \cap (\overline{S_F^1(T^{1/d})} \cap H) \neq \varnothing\}.$$

A similar argument to before shows that $A(T) \subseteq A_1(T) \cup A_2(T)$. We already know that $\partial S_F^1(T^{1/d}) \in \mathrm{Lip}(d, M_1, T^{1/d}L_1)$ and $S_F^1(T^{1/d}) \cap H \in \mathrm{Lip}(n, \tilde{M}_1, T^{1/d}\tilde{L}_1)$. The same holds of course for the closure. By Lemma 4.1(ii) we obtain

$$\mathrm{Vol}\, A_1(T) \ll T^{(d-1)/d}, \quad \mathrm{Vol}\, A_2(T) \ll T^{(d-1)/d} \quad \text{for } T \geq 1,$$

and thus $F(T) \ll T^{(d-1)/d}$ for $T \geq 1$. Integration by parts gives

$$\int_1^B \frac{1}{t}\, dF(t) = F(B)/B - F(1) - \int_1^B F\, d\frac{1}{t} \ll B^{-1/d} + \int_1^B t^{-(1+1/d)}\, dt \ll 1.$$

With (5-30), (5-31) and (5-32), we obtain (5-27). Together with (5-26) this gives (5-25). □

Lemma 5.5. *We have*

$$I(B) = \frac{1}{4\cdot 6!}\left(\frac{2^r(2\pi)^s R_K}{\sqrt{|\Delta_K|}}\right)^6 \frac{1}{\prod_{v\in V'} \mathfrak{N}\mathfrak{b}_v} (\log B)^6.$$

Proof. Let m_n denote the Lebesgue measure on $\mathbb{R}^n$. We define the measurable function $f : (S_F^1(\infty))^6 \to \mathbb{R}^6$ by $f((z_v)_{v\in V'}) = (N(z_v))_{v\in V'}$. For any cell $E := \prod_{v\in V'}(a_v, b_v]$, with $0 < a_v \leq b_v$, we have

$$(m_{6d} \circ f^{-1})(E) = \prod_{v\in V'} (\mathrm{Vol}\, S_F^1(b_v^{1/d}) - \mathrm{Vol}\, S_F^1(a_v^{1/d})) = (\mathrm{Vol}\, S_F^1(1))^6 m_6(E).$$

Thus, $m_{6d} \circ f^{-1} = (\mathrm{Vol}\, S_F^1(1))^6 m_6$ on $(\mathbb{R}^{\geq 0})^6$. Let

$$M_{\mathbb{Q}}(B) := \{(t_v)_{v\in V'} \in \mathbb{R}^6 \mid t_v \geq 1 \text{ for all } v \text{ and } t_{jk}t_{jl}t_{kj}^2 t_{lj}^2 \leq B \text{ for all } j\}.$$

Then

$$\int_{M(B)} \prod_{v\in V'} \frac{dz_v}{N(z_v)} = \int_{f^{-1}(M_{\mathbb{Q}}(B))} \prod_{v\in V'} \frac{1}{f(z)_v}\, dm_{6d} = \int_{M_{\mathbb{Q}}(B)} \prod_{v\in V'} \frac{1}{t_v}\, d(m_{6d} \circ f^{-1})$$
$$= (\mathrm{Vol}\, S_F^1(1))^6 \int_{M_{\mathbb{Q}}(B)} \prod_{v\in V'} \frac{1}{t_v}\, dm_6 = \frac{(\mathrm{Vol}\, S_F^1(1))^6}{4\cdot 6!} (\log B)^6.$$

The last integral is computed at the end of [Heath-Brown and Moroz 1999]. □

We define

$$C_0(K) := \frac{1}{4\cdot 6!}\left(\frac{2^r(2\pi)^s R_K}{\sqrt{|\Delta_K|}}\right)^6 \quad \text{and} \quad C(K) := 3^q C_0(K).$$

Then (5-11) and the previous two lemmata imply that

$$\mathcal{M}_1(B, (\mathfrak{b}_v)_v) = \frac{C_0(K)}{\prod_{v\in V'} \mathfrak{Nb}_v}(\log B)^6 + O(\log B)^5.$$

Keep in mind that $\mathfrak{b}_v \in \mathscr{C}$ for all $v \in V'$. With (5-9), (5-10), we obtain

$$\mathcal{M}(B, (\mathfrak{a}_v)_v) \le \frac{C(K)}{\prod_{v\in V'} \mathfrak{Na}_v}(\log B)^6 + O\left(\frac{1}{\prod_{v\in V'} \mathfrak{Na}_v}(\log B)^5\right).$$

Let $R := \max_j\{\mathfrak{Na}_j\}^{1/d} \prod_{v\in V'} \mathfrak{Na}_v^{2/(3d)}$. Then $R \ge c_4 > 0$ for some constant c_4 depending only on K. This implies in particular that $\log R \ll R$. Moreover, we have $1/(c_5 R^{3d}) \le b_j$ for some constant $c_5 \ge 1$ depending only on K. Therefore,

$$\mathcal{M}(B, (\mathfrak{a}_v)_v) \ge 3^q\left(\prod_{v\in V'} \frac{\mathfrak{Nb}_v}{\mathfrak{Na}_v}\right)\mathcal{M}_1(B/(c_5R^{3d}), (\mathfrak{b}_v)_v).$$

Whenever $B \ge ec_5R^{3d}$, we obtain

$$\begin{aligned}\mathcal{M}(B, (\mathfrak{a}_v)_v) &\ge \frac{C(K)}{\prod_{v\in V'} \mathfrak{Na}_v}\log(B/(c_5R^{3d}))^6 + O\left(\frac{1}{\prod_{v\in V'} \mathfrak{Na}_v}\log(B/(c_5R^{3d}))^5\right)\\ &= \frac{C(K)}{\prod_{v\in V'} \mathfrak{Na}_v}(\log B)^6 + O\left(\frac{R}{\prod_{v\in V'} \mathfrak{Na}_v}(\log B)^5\right).\end{aligned}$$

This result holds as well if $e \le B < ec_5R^{3d}$, since then the error term dominates the main term. Therefore,

$$\mathcal{M}(B, (\mathfrak{a}_v)_v) = \frac{C(K)}{\prod_{v\in V'} \mathfrak{Na}_v}(\log B)^6 + O\left(\frac{R}{\prod_{v\in V'} \mathfrak{Na}_v}(\log B)^5\right),$$

and Lemma 3.1 follows from (5-8).

References

[Baier and Browning 2013] S. Baier and T. D. Browning, "Inhomogeneous cubic congruences and rational points on Del Pezzo surfaces", *J. Reine Angew. Math.* **680** (2013), 69–151.

[Batyrev and Tschinkel 1998a] V. V. Batyrev and Y. Tschinkel, "Manin's conjecture for toric varieties", *J. Algebraic Geom.* **7**:1 (1998), 15–53. MR 2000c:11107 Zbl 0946.14009

[Batyrev and Tschinkel 1998b] V. V. Batyrev and Y. Tschinkel, "Tamagawa numbers of polarized algebraic varieties", pp. 299–340 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000d:11090 Zbl 0926.11045

[de la Bretèche 1998] R. de la Bretèche, "Sur le nombre de points de hauteur bornée d'une certaine surface cubique singulière", pp. 51–77 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000b:11074 Zbl 0969.14014

[de la Bretèche 2002] R. de la Bretèche, "Nombre de points de hauteur bornée sur les surfaces de del Pezzo de degré 5", *Duke Math. J.* **113**:3 (2002), 421–464. MR 2003m:14033 Zbl 1054.14025

[de la Bretèche and Browning 2011] R. de la Bretèche and T. D. Browning, "Manin's conjecture for quartic del Pezzo surfaces with a conic fibration", *Duke Math. J.* **160**:1 (2011), 1–69. MR 2012k:11038 Zbl 1245.11044

[de la Bretèche and Fouvry 2004] R. de la Bretèche and É. Fouvry, "L'éclaté du plan projectif en quatre points dont deux conjugués", *J. Reine Angew. Math.* **576** (2004), 63–122. MR 2005f:11131 Zbl 1065.11080

[de la Bretèche and Swinnerton-Dyer 2007] R. de la Bretèche and P. Swinnerton-Dyer, "Fonction zêta des hauteurs associée à une certaine surface cubique", *Bull. Soc. Math. France* **135**:1 (2007), 65–92. MR 2009f:14041 Zbl 1207.11068

[de la Bretèche et al. 2007] R. de la Bretèche, T. D. Browning, and U. Derenthal, "On Manin's conjecture for a certain singular cubic surface", *Ann. Sci. École Norm. Sup.* (4) **40**:1 (2007), 1–50. MR 2008e:11038 Zbl 1125.14008

[de la Bretèche et al. 2012] R. de la Bretèche, T. Browning, and E. Peyre, "On Manin's conjecture for a family of Châtelet surfaces", *Ann. of Math.* (2) **175**:1 (2012), 297–343. MR 2874644 Zbl 1237.11018

[Browning and Derenthal 2009] T. D. Browning and U. Derenthal, "Manin's conjecture for a cubic surface with D_5 singularity", *Int. Math. Res. Not.* **2009**:14 (2009), 2620–2647. MR 2011a:14041 Zbl 1173.14017

[Chambert-Loir and Tschinkel 2002] A. Chambert-Loir and Y. Tschinkel, "On the distribution of points of bounded height on equivariant compactifications of vector groups", *Invent. Math.* **148**:2 (2002), 421–452. MR 2003d:11094 Zbl 1067.11036

[Christensen and Gubler 2008] C. Christensen and W. Gubler, "Der relative Satz von Schanuel", *Manuscripta Math.* **126**:4 (2008), 505–525. MR 2009e:11124 Zbl 1155.11034

[Colliot-Thélène and Sansuc 1980] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles", pp. 223–237 in *Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979*, edited by A. Beauville, Sijthoff & Noordhoff, Alphen aan den Rijn, 1980. MR 82d:14016 Zbl 0451.14018

[Colliot-Thélène and Sansuc 1987] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles, II", *Duke Math. J.* **54**:2 (1987), 375–492. MR 89f:11082 Zbl 0659.14028

[Derenthal and Janda 2013] U. Derenthal and F. Janda, "Gaussian rational points on a singular cubic surface", pp. 210–230 in *Torsors, étale homotopy and applications to rational points* (Edinburgh, 2011), London Math. Soc. Lecture Note Series **405**, Cambridge Univ. Press, 2013.

[Fouvry 1998] É. Fouvry, "Sur la hauteur des points d'une certaine surface cubique singulière", pp. 31–49 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000b:11075 Zbl 0930.11044

[Franke et al. 1989] J. Franke, Y. I. Manin, and Y. Tschinkel, "Rational points of bounded height on Fano varieties", *Invent. Math.* **95**:2 (1989), 421–435. MR 89m:11060 Zbl 0674.14012

[Heath-Brown and Moroz 1999] D. R. Heath-Brown and B. Z. Moroz, "The density of rational points on the cubic surface $X_0^3 = X_1X_2X_3$", *Math. Proc. Cambridge Philos. Soc.* **125**:3 (1999), 385–395. MR 2000f:11080 Zbl 0938.11016

[Lang 1994] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, New York, 1994. MR 95f:11085 Zbl 0811.11001

[Le Boudec 2012] P. Le Boudec, "Manin's conjecture for a cubic surface with $2A_2 + A_1$ singularity type", *Math. Proc. Cambridge Philos. Soc.* **153**:3 (2012), 419–455.

[Masser and Vaaler 2007] D. Masser and J. D. Vaaler, "Counting algebraic numbers with large height. II", *Trans. Amer. Math. Soc.* **359**:1 (2007), 427–445. MR 2008m:11208 Zbl 1215.11100

[Peyre 1995] E. Peyre, "Hauteurs et mesures de Tamagawa sur les variétés de Fano", *Duke Math. J.* **79**:1 (1995), 101–218. MR 96h:11062 Zbl 0901.14025

[Salberger 1998] P. Salberger, "Tamagawa measures on universal torsors and points of bounded height on Fano varieties", pp. 91–258 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), Astérisque **251**, Société Mathématique de France, Paris, 1998. MR 2000d:11091 Zbl 0959.14007

[Schanuel 1979] S. H. Schanuel, "Heights in number fields", *Bull. Soc. Math. France* **107**:4 (1979), 433–449. MR 81c:12025 Zbl 0428.12009

[Widmer 2010] M. Widmer, "Counting primitive points of bounded height", *Trans. Amer. Math. Soc.* **362**:9 (2010), 4793–4829. MR 2011i:11099 Zbl 05791771

Communicated by Jean-Louis Colliot-Thélène
Received 2012-04-10 Revised 2012-07-30 Accepted 2012-09-07

frei@math.lmu.de *Mathematisches Institut, LMU München, Theresienstr. 39, D-80333 München, Germany*
http://www.mathematik.uni-muenchen.de/~frei

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1481

On the ample cone of a rational surface with an anticanonical cycle

Robert Friedman

Let Y be a smooth rational surface, and let D be a cycle of rational curves on Y that is an anticanonical divisor, i.e., an element of $|-K_Y|$. Looijenga studied the geometry of such surfaces Y in case D has at most five components and identified a geometrically significant subset R of the divisor classes of square -2 orthogonal to the components of D. Motivated by recent work of Gross, Hacking, and Keel on the global Torelli theorem for pairs (Y, D), we attempt to generalize some of Looijenga's results in case D has more than five components. In particular, given an integral isometry f of $H^2(Y)$ that preserves the classes of the components of D, we investigate the relationship between the condition that f preserves the "generic" ample cone of Y and the condition that f preserves the set R.

Introduction

The ample cone of a del Pezzo surface Y (or rather the associated dual polyhedron) was studied classically by, among others, Gosset, Schoute, Kantor, Coble, Todd, Coxeter, and Du Val. For a brief historical discussion, one can consult the remarks in [Coxeter 1973, §11.x]. From this point of view, the lines on Y are the main object of geometric interest as they are the walls of the ample cone or the vertices of the dual polyhedron. The corresponding root system (in case $K_Y^2 \leq 6$) only manifests itself geometrically by allowing del Pezzo surfaces with rational double points or, equivalently, smooth surfaces Y with $-K_Y$ nef and big but not ample. This is explicitly worked out in [Du Val 1934]. On the other hand, the root system, or rather its Weyl group, appears for a smooth del Pezzo surface as a group of symmetries of the ample cone, a fact which (in a somewhat different guise) was already known to Cartan. Perhaps the culmination of the classical side of the story is [Du Val 1937], where the blowup of $\mathbb{P}^2$ at $n \geq 9$ points is also systematically considered. In modern times, Manin explained the appearance of the Weyl group by noting that the orthogonal complement to K_Y in $H^2(Y; \mathbb{Z})$ is a root lattice Λ. Moreover, given any root of Λ, in other words an element β of square -2, there

MSC2010: 14J26.
Keywords: rational surface, anticanonical cycle, exceptional curve, ample cone.

exists a deformation of Y for which $\beta = \pm[C]$, where C is a smooth rational curve of self-intersection -2. For modern expositions of the theory, see for example the book of Manin [1986] or the account of Demazure [1980a; 1980b; 1980c; 1980d].

In general, it seems hard to study an arbitrary rational surface Y without imposing some extra conditions. One very natural condition is that $-K_Y$ is effective, i.e., that $-K_Y = D$ for an effective divisor D. In case the intersection matrix of D is negative definite, such pairs (Y, D) arise naturally in the study of minimally elliptic singularities: the case where D is a smooth elliptic curve corresponds to the case of simple elliptic singularities, the case where D is a nodal curve or a cycle of smooth rational curves meeting transversally corresponds to the case of cusp singularities, and the case where D is reduced but has one component with a cusp, two components with a tacnode, or three components meeting at a point corresponds to triangle singularities. From this point of view, the case where D is a cycle of rational curves is the most plentiful. The systematic study of such surfaces in case the intersection matrix of D is negative definite dates back to [Looijenga 1981]. However, for various technical reasons, most of the results of that paper are proved under the assumption that the number of components in the cycle is at most 5. Some of the main points of Looijenga's seminal paper are as follows. Let R denote the set of elements in $H^2(Y; \mathbb{Z})$ of square -2 that are orthogonal to the components of D and that are of the form $\pm[C]$, where C is a smooth rational curve disjoint from D, for some deformation of the pair (Y, D). In terms of deformations of singularities, the set R is related to the possible rational double point singularities that can arise as deformations of the dual cusp to the cusp singularity corresponding to D. Looijenga noted that, in general, there exist elements in $H^2(Y; \mathbb{Z})$ of square -2 that are orthogonal to the components of D but that do not lie in R. Moreover, reflections in elements of the set R give symmetries of the "generic" ample cone (which is the same as the ample cone in case there are no smooth rational curves on Y disjoint from D). Finally, still under the assumption of at most five components, any isometry of $H^2(Y; \mathbb{Z})$ that preserves the positive cone, the classes $[D_i]$, and the set R preserves the generic ample cone.

This paper, which is an attempt to see how much of [Looijenga 1981] can be generalized to the case of arbitrarily many components, is motivated by a question raised by the recent work of Gross, Hacking, and Keel [Gross et al. 2013] on, among other matters, the global Torelli theorem for pairs (Y, D) where D is an anticanonical cycle on the rational surface Y. In order to formulate this theorem in a fairly general way, one would like to characterize the isometries f of $H^2(Y, \mathbb{Z})$, preserving the positive cone and fixing the classes $[D_i]$, which preserve the ample cone of Y. It is natural to ask if, at least in the generic case, the condition that $f(R) = R$ is sufficient. In this paper, we give various criteria on R that insure that, if an isometry f of $H^2(Y; \mathbb{Z})$ preserves the positive cone, the classes $[D_i]$,

and the set R, then f preserves the generic ample cone. Typically, one needs a hypothesis that says that R is large. For example, one such hypothesis is that there is a subset of R that spans a negative definite codimension-1 subspace of the orthogonal complement to the components of D. In theory, at least under various extra hypotheses, such a result gives a necessary and sufficient condition for an isometry to preserve the generic ample cone. In practice, however, the determination of the set R in general is a difficult problem, which seems close in its complexity to the problem of describing the generic ample cone of Y. Finally, we show that some assumptions on (Y, D) are necessary by giving examples where $R = \varnothing$, so that the condition that an isometry f preserves R is automatic, and of isometries f such that f preserves the positive cone, the classes $[D_i]$, and (vacuously) the set R but f does not preserve the generic ample cone. We do not yet have a good understanding of the relationship between preserving the ample cone and preserving the set R.

An outline of this paper is as follows. The preliminary Section 1 reviews standard methods for constructing nef classes on algebraic surfaces and applies this to the study of when the normal surface obtained by contracting a negative definite anticanonical cycle on a rational surface is projective. In Section 2, we analyze the ample cone and generic ample cone of a pair (Y, D) and show that the set R defined by Looijenga is exactly the set of elements β in $H^2(Y; \mathbb{Z})$ of square -2 that are orthogonal to the components of D such that reflection about β preserves the generic ample cone. Much of the material of Section 2 overlaps with results in [Gross et al. 2013], proved there by somewhat different methods. Section 3 is devoted to giving various sufficient conditions for an isometry f of $H^2(Y; \mathbb{Z})$ to preserve the generic ample cone, including the one described above. Section 4 gives examples of pairs (Y, D) satisfying the sufficient conditions of Section 3 where the number of components of D and the multiplicity $-D^2$ are arbitrarily large as well as examples showing that some hypotheses on (Y, D) are necessary.

Notation and conventions. We work over $\mathbb{C}$. If X is a smooth projective surface with $h^1(\mathcal{O}_X) = h^2(\mathcal{O}_X) = 0$ and $\alpha \in H^2(X; \mathbb{Z})$, we let L_α denote the corresponding holomorphic line bundle, i.e., $c_1(L_\alpha) = \alpha$. Given a curve C or divisor class G on X, we let $[C]$ or $[G]$ denote the corresponding element of $H^2(X; \mathbb{Z})$. Intersection pairing on curves or divisors, or on elements in the second cohomology of a smooth surface (viewed as a canonically oriented 4-manifold), is denoted by multiplication.

1. Preliminaries

In this paper, Y denotes a smooth rational surface with $-K_Y = D = \sum_{i=1}^{r} D_i$ a (reduced) cycle of rational curves; i.e., each D_i is a smooth rational curve and D_i meets $D_{i\pm1}$ transversally, where i is taken mod r except for $r = 1$, in which case $D_1 = D$ is an irreducible nodal curve. We note, however, that many of the results

in this paper can be generalized to the case where $D \in |-K_Y|$ is not assumed to be a cycle. The integer $r = r(D)$ is called the *length* of D. An *orientation* of D is an orientation of the dual graph (with appropriate modifications in case $r = 1$). We shall abbreviate the data of the surface Y and the oriented cycle D by (Y, D) and refer to it as an *anticanonical pair*. If the intersection matrix $(D_i \cdot D_j)$ is negative definite, we say that (Y, D) is a *negative definite anticanonical pair*.

Definition 1.1. An irreducible curve E on Y is an *exceptional curve* if $E \cong \mathbb{P}^1$, $E^2 = -1$, and $E \neq D_i$ for any i. An irreducible curve C on Y is a -2-*curve* if $C \cong \mathbb{P}^1$, $C^2 = -2$, and $C \neq D_i$ for any i. Let Δ_Y be the set of all -2-curves on Y, and let $\mathrm{W}(\Delta_Y)$ be the group of integral isometries of $H^2(Y; \mathbb{R})$ generated by the reflections in the classes in the set Δ_Y.

Definition 1.2. Let $\Lambda = \Lambda(Y, D) \subseteq H^2(Y; \mathbb{Z})$ be the orthogonal complement of the lattice spanned by the classes $[D_i]$. Fixing the identification $\mathrm{Pic}^0 D \cong \mathbb{G}_m$ defined by the orientation of the cycle D, we define the *period homomorphism* $\varphi_Y : \Lambda \to \mathbb{G}_m$ as follows: if $\alpha \in \Lambda$ and L_α is the corresponding line bundle, then $\varphi_Y(\alpha) \in \mathbb{G}_m$ is the image of the line bundle of multidegree 0 on D defined by $L_\alpha | D$. Clearly φ_Y is a homomorphism. The *period map* is the function that associates to the pair (Y, D) the homomorphism $\varphi_Y : \Lambda \to \mathbb{G}_m$.

By [Looijenga 1981; Friedman and Scattone 1986; Friedman 1984], we have:

Theorem 1.3. *The period map is surjective. More precisely, given Y as above and given an arbitrary homomorphism $\varphi : \Lambda \to \mathbb{G}_m$, there exists a deformation of the pair (Y, D) over a smooth connected base, which we can take to be $(\mathbb{G}_m)^n$ for some n, such that the monodromy of the family is trivial and there exists a fiber of the deformation, say (Y', D'), such that $\varphi_{Y'} = \varphi$ under the induced identification of $\Lambda(Y', D')$ with Λ.* □

For future reference, we recall some standard facts about negative definite curves on a surface.

Lemma 1.4. *Let X be a smooth projective surface, and let $G_1, \ldots, G_n$ be irreducible curves on X such that the intersection matrix $(G_i \cdot G_j)$ is negative definite. Let F be an effective divisor on X not necessarily reduced or irreducible and such that, for all i, G_i is not a component of F.*

(i) *Given $r_i \in \mathbb{R}$, if $(F + \sum_i r_i G_i) \cdot G_j = 0$ for all j, then $r_i \geq 0$ for all i, and, for every subset I of $\{1, \ldots, n\}$, if $\bigcup_{i \in I} G_i$ is a connected curve such that $F \cdot G_j \neq 0$ for some $j \in I$, then $r_i > 0$ for $i \in I$.*

(ii) *Given $s_i, t_i \in \mathbb{R}$, if $[F] + \sum_i s_i [G_i] = \sum_i t_i [G_i]$, then $F = 0$ and $s_i = t_i$ for all i.*

The following general result is also well known:

Proposition 1.5. *Let X be a smooth projective surface, and let $G_1, \dots, G_n$ be irreducible curves on X such that the intersection matrix $(G_i \cdot G_j)$ is negative definite. (We do not, however, assume that $\bigcup_i G_i$ is connected.) Then there exists a nef and big divisor H on X such that $H \cdot G_j = 0$ for all j and, if C is an irreducible curve such that $C \neq G_j$ for any j, then $H \cdot C > 0$. In fact, the set of nef and big $\mathbb{R}$-divisors that are orthogonal to $\{G_1, \dots, G_n\}$ is a nonempty open subset of $\{G_1, \dots, G_n\}^\perp \otimes \mathbb{R}$.*

Proof. Fix an ample divisor H_0 on X. Since $(G_i \cdot G_j)$ is negative definite, there exist $r_i \in \mathbb{Q}$ such that $\left(\sum_i r_i G_i\right) \cdot G_j = -(H_0 \cdot G_j)$ for every j. Hence, $(H_0 + \sum_i r_i G_i) \cdot G_j = 0$. By Lemma 1.4, $r_i > 0$ for every i. There exists an $N > 0$ such that $N r_i \in \mathbb{Z}$ for all i. Then $H = N(H_0 + \sum_i r_i G_i)$ is an effective divisor satisfying $H \cdot G_j = 0$ for all j. If C is an irreducible curve such that $C \neq G_j$ for any j, then $H_0 \cdot C > 0$ and $G_i \cdot C \geq 0$ for all i. Hence, $H \cdot C > 0$. In particular, H is nef. Finally, H is big since $H^2 = NH \cdot (H_0 + \sum_i r_i G_i) = N(H \cdot H_0) > 0$ as H_0 is ample.

To see the final statement, we apply the above argument to an ample $\mathbb{R}$-divisor x (i.e., an element in the interior of the ample cone) to see that $x + \sum_i r_i G_i$ is a nef and big $\mathbb{R}$-divisor orthogonal to $\{G_1, \dots, G_n\}$. As $x + \sum_i r_i G_i$ is simply the orthogonal projection p of x onto $\{G_1, \dots, G_n\}^\perp \otimes \mathbb{R}$ and $p : H^2(X; \mathbb{R}) \to \{G_1, \dots, G_n\}^\perp \otimes \mathbb{R}$ is an open map, the image of the interior of the ample cone of X is then a nonempty open subset of $\{G_1, \dots, G_n\}^\perp \otimes \mathbb{R}$ consisting of nef and big $\mathbb{R}$-divisors orthogonal to $\{G_1, \dots, G_n\}$. □

Applying the above construction to $X = Y$ and $D_1, \dots, D_r$, we can find a nef and big divisor H such that $H \cdot D_j = 0$ for all j and such that, if C is an irreducible curve such that $C \neq D_j$ for any j, then $H \cdot C > 0$.

Proposition 1.6. *Let (Y, D) be a negative definite anticanonical pair, and let H be a nef and big divisor such that $H \cdot D_j = 0$ for all j and such that, if C is an irreducible curve such that $C \neq D_j$ for any j, then $H \cdot C > 0$. Suppose in addition that $\mathcal{O}_Y(H)|D = \mathcal{O}_D$, i.e., that $\varphi_Y([H]) = 1$. Then the D_i are not fixed components of $|H|$. Hence, if $\overline{Y}$ denotes the normal complex surface obtained by contracting the D_i, then H induces an ample divisor $\overline{H}$ on $\overline{Y}$ and $|3\overline{H}|$ defines an embedding of $\overline{Y}$ in $\mathbb{P}^N$ for some N.*

Proof. Consider the exact sequence

$$0 \to \mathcal{O}_Y(H - D) \to \mathcal{O}_Y(H) \to \mathcal{O}_D \to 0.$$

Looking at the long exact cohomology sequence, as

$$H^1(Y; \mathcal{O}_Y(H - D)) = H^1(Y; \mathcal{O}_Y(H) \otimes K_Y)$$

is Serre dual to $H^1(Y; \mathcal{O}_Y(-H)) = 0$, by Ramanujam's vanishing theorem, there exists a section of $\mathcal{O}_Y(H)$ that is nowhere vanishing on D, proving the first statement.

The second follows from the Nakai–Moishezon criterion and the third from general results on linear series on anticanonical pairs [Friedman 1983]. □

Remark 1.7. By the surjectivity of the period map (Theorem 1.3), for any (Y, D) a negative definite anticanonical pair and H a nef and big divisor on Y such that $H \cdot D_j = 0$ for all j and $H \cdot C > 0$ for all curves $C \neq D_i$, there exists a deformation of the pair (Y, D) such that the divisor corresponding to H has trivial restriction to D. More generally, one can consider deformations such that $\varphi_Y([H])$ is a torsion point of $\mathbb{G}_m$. In this case, if $\overline{Y}$ is the normal surface obtained by contracting D, then $\overline{Y}$ is projective. Note that this implies that the set of pairs (Y, D) such that $\overline{Y}$ is projective is Zariski dense in the moduli space. However, as the set of torsion points is not dense in $\mathbb{G}_m$ in the classical topology, the set of projective surfaces $\overline{Y}$ will not be dense in the classical topology.

2. Roots and nodal classes

Definition 2.1. Let $\mathscr{C} = \mathscr{C}(Y)$ be the positive cone of Y, i.e.,

$$\mathscr{C} = \{x \in H^2(Y; \mathbb{R}) : x^2 > 0\}.$$

Then $\mathscr{C}$ has two components, and exactly one of them, say $\mathscr{C}^+ = \mathscr{C}^+(Y)$, contains the classes of ample divisors. We also define

$$\mathscr{C}_D^+ = \mathscr{C}_D^+(Y) = \{x \in \mathscr{C}^+ : x \cdot [D_i] \geq 0 \text{ for all } i\}.$$

Let $\overline{\mathscr{A}}(Y) \subseteq \mathscr{C}^+ \subseteq H^2(Y; \mathbb{R})$ be (the closure of) the ample (nef, Kähler) cone of Y in $\mathscr{C}^+$. By definition, $\overline{\mathscr{A}}(Y)$ is closed in $\mathscr{C}^+$ but not in general in $H^2(Y; \mathbb{R})$.

Definition 2.2. Let $\alpha \in H^2(Y; \mathbb{Z})$, $\alpha \neq 0$. The *oriented wall* W^α *associated to* α is the set $\{x \in \mathscr{C}^+ : x \cdot \alpha = 0\}$, i.e., the intersection of $\mathscr{C}^+$ with the orthogonal space to α together with the preferred half space defined by $x \cdot \alpha \geq 0$. If C is a curve on Y, we write W^C for $W^{[C]}$. A standard result (see, for example, [Friedman and Morgan 1988, II (1.8)]) shows that, if I is a subset of $H^2(Y; \mathbb{Z})$ and there exists an $N \in \mathbb{Z}^+$ such that $-N \leq \alpha^2 < 0$ for all $\alpha \in I$, then the collection of walls $\{W^\alpha : \alpha \in I\}$ is locally finite on $\mathscr{C}^+$. Finally, we say that W^α is a *face* of $\overline{\mathscr{A}}(Y)$ if $\partial\overline{\mathscr{A}}(Y) \cap W^\alpha$ contains a nonempty open subset of W^α and $x \cdot \alpha \geq 0$ for all $x \in \overline{\mathscr{A}}(Y)$.

Lemma 2.3. *$\overline{\mathscr{A}}(Y)$ is the set of all $x \in \mathscr{C}^+$ such that $x \cdot [D_i] \geq 0$, $x \cdot [E] \geq 0$ for all exceptional curves E, and $x \cdot [C] \geq 0$ for all -2-curves C. Moreover, if α is the class associated to an exceptional or -2-curve, or $\alpha = [D_i]$ for some i such that $D_i^2 < 0$, then W^α is a face of $\overline{\mathscr{A}}(Y)$. If α and β are two such classes, $W^\alpha = W^\beta \iff \alpha = \beta$.*

Proof. For the first claim, it is enough to show that, if G is an irreducible curve on Y with $G^2 < 0$, then G is either D_i for some i, an exceptional curve, or a -2-curve. This follows immediately from adjunction since, if $G \neq D_i$ for any i, then $G \cdot D \geq 0$

and $-2 \le 2p_a(G) - 2 = G^2 - G \cdot D < 0$; hence, $p_a(G) = 0$ and either $G^2 = -2$, $G \cdot D = 0$, or $G^2 = G \cdot D = -1$. The last two statements follow from the openness statement in Proposition 1.5 and the fact that no two distinct classes of the types listed above are multiples of each other. □

As an alternate characterization of the classes in the previous lemma, we have the following:

Lemma 2.4. *Let H be a nef divisor such that $H \cdot D > 0$.*

(i) *If $\alpha \in H^2(Y;\mathbb{Z})$ with $\alpha^2 = \alpha \cdot [K_Y] = -1$, then $\alpha \cdot [H] \ge 0$ if and only if α is the class of an effective curve. In particular, the wall W^α does not pass through the interior of $\overline{\mathcal{A}}(Y)$.* (See [Friedman and Morgan 1988, p. 332] for a more general statement.)

(ii) *If $\beta \in H^2(Y;\mathbb{Z})$ with $\beta^2 = -2$, $\beta \cdot [D_i] = 0$ for all i, $\beta \cdot [H] \ge 0$, and $\varphi_Y(\beta) = 1$, then $\pm\beta$ is the class of an effective curve, and β is effective if $\beta \cdot [H] > 0$.*

Hence, the ample cone $\overline{\mathcal{A}}(Y)$ is the set of all $x \in \mathcal{C}^+$ such that $x \cdot [D_i] \ge 0$ and $x \cdot \alpha \ge 0$ for all classes α and β as described in (i) and (ii) above, where in case (ii) we assume in addition that β is effective or equivalently that $\beta \cdot [H] > 0$ for some nef divisor H.

Proof. (i) Clearly, if α is the class of an effective curve, then $\alpha \cdot [H] \ge 0$ since H is nef. Conversely, assume that $\alpha^2 = \alpha \cdot [K_Y] = -1$ and that $\alpha \cdot [H] \ge 0$. By the Riemann–Roch theorem, $\chi(L_\alpha) = 1$. Hence, either $h^0(L_\alpha) > 0$ or $h^2(L_\alpha) > 0$. But $h^2(L_\alpha) = h^0(L_\alpha^{-1} \otimes K_Y)$ and $[H] \cdot (-\alpha - [D]) < 0$ by assumption. Thus, $h^0(L_\alpha) > 0$ and hence α is the class of an effective curve.

(ii) As in (i), $H \cdot (-\beta - [D]) < 0$, and hence, $h^0(L_\beta^{-1} \otimes K_Y) = 0$. Thus, $h^2(L_\beta) = 0$. Suppose that $h^0(L_\beta) = 0$. Then, by the Riemann–Roch theorem, $\chi(L_\beta) = 0$ and hence $h^1(L_\beta) = 0$. Hence, $h^1(L_\beta^{-1} \otimes K_Y) = 0$. Since $\varphi_Y(\beta) = 1$, $L_\beta^{\pm 1} | D = \mathcal{O}_D$. Thus, there is an exact sequence

$$0 \to L_\beta^{-1} \otimes \mathcal{O}_Y(-D) \to L_\beta^{-1} \to \mathcal{O}_D \to 0.$$

Since $H^1(L_\beta^{-1} \otimes K_Y) = H^1(L_\beta^{-1} \otimes \mathcal{O}_Y(-D)) = 0$, the map $H^0(L_\beta^{-1}) \to H^0(\mathcal{O}_D)$ is surjective and hence $-\beta$ is the class of an effective curve. □

Definition 2.5. Let $\alpha \in H^2(Y;\mathbb{Z})$. Then α is a *numerical exceptional curve* if $\alpha^2 = \alpha \cdot [K_Y] = -1$. The numerical exceptional curve α is *effective* if $h^0(L_\alpha) > 0$, i.e., if $\alpha = [G]$, where G is an effective curve.

A minor variation of the proof of Lemma 2.4 shows the following:

Lemma 2.6. *Let H be a nef and big divisor such that $H \cdot G > 0$ for all irreducible curves G not equal to D_i for some i, and let α be a numerical exceptional curve.*

(i) *Suppose that* $[H] \cdot \alpha \geq 0$. *Then either* $[H] \cdot \alpha > 0$ *and* α *is effective or* $H \cdot D = [H] \cdot \alpha = 0$ *and* α *is an integral linear combination of the* $[D_i]$.

(ii) *If* (Y, D) *is negative definite and* α *is an integral linear combination of the* $[D_i]$, *then either some component* D_i *is a smooth rational curve of self-intersection* -1 *or* $K_Y^2 = -1$, $\alpha = K_Y$, *and hence* α *is not effective.*

(iii) *If no component* D_i *is a smooth rational curve of self-intersection* -1, *then* α *is effective if and only if* $[H] \cdot \alpha > 0$.

Proof. (i) As in the proof of Lemma 2.4, either α or $-\alpha - [D]$ is the class of an effective divisor. If $-\alpha - [D]$ is the class of an effective divisor, then $0 \leq [H] \cdot (-\alpha - [D]) \leq 0$, so $[H] \cdot \alpha = H \cdot D = 0$. In particular, (Y, D) is negative definite. Moreover, if G is an effective divisor with $[G] = -\alpha - [D]$, then every component of G is equal to some D_i. Hence, $[G]$ and therefore $\alpha = -[G] - [D]$ are integral linear combinations of the $[D_i]$.

(ii) Suppose that α is an integral linear combination of the $[D_i]$ but that no D_i is a smooth rational curve of self-intersection -1. We shall show that $K_Y^2 = -1$ and $\alpha = K_Y$. First suppose that $K_Y^2 = -1$. Then $\bigoplus_i \mathbb{Z} \cdot [D_i] = \mathbb{Z} \cdot [K_Y] \oplus L$, where L, the orthogonal complement of $[K_Y]$ in $\bigoplus_i \mathbb{Z} \cdot [D_i]$, is even and negative definite. Thus, $\alpha = a[K_Y] + \beta$, with either $\beta = 0$ or $\beta^2 \leq -2$, and $\alpha^2 = -a^2 + \beta^2$. Hence, if $\alpha^2 = \alpha \cdot [K_Y] = -1$, the only possibility is $\beta = 0$ and $a = 1$. In case $K_Y^2 < -1$, D is reducible, and no D_i is a smooth rational curve of self-intersection -1, then $D_i^2 \leq -2$ for all i and either $D_i^2 \leq -4$ for some i or there exist $i \neq j$ such that $D_i^2 = D_j^2 = -3$. In this case, it is easy to check that, for all integers a_i such that $a_i \neq 0$ for some i, $\left(\sum_i a_i D_i\right)^2 < -1$. This contradicts $\alpha^2 = -1$.

(iii) If $[H] \cdot \alpha > 0$, then α is effective by (i). If $[H] \cdot \alpha < 0$, then clearly α is not effective. Suppose that $[H] \cdot \alpha = 0$; we must show that, again, α is not effective. Suppose that $\alpha = [G]$ is effective. By the hypothesis on H, every component of G is a D_i for some i so that $\alpha = \sum_i a_i [D_i]$ for some $a_i \in \mathbb{Z}$, $a_i \geq 0$. Let $I \subseteq \{1, \ldots, r\}$ be the set of i such that $a_i > 0$. Then $H \cdot D_i = 0$ for all $i \in I$. If $I = \{1, \ldots, r\}$, then (Y, D) is negative definite and we are done by (ii). Otherwise, $\bigcup_{i \in I} D_i$ is a union of chains of curves whose components D_i satisfy $D_i^2 \leq -2$. It is then easy to check that $\alpha^2 < -1$ in this case, a contradiction. Hence, α is not effective. □

Definition 2.7. Let Y_t be a generic small deformation of Y, and identify $H^2(Y_t; \mathbb{R})$ with $H^2(Y; \mathbb{R})$. Define $\overline{\mathscr{A}}_{\text{gen}} = \overline{\mathscr{A}}_{\text{gen}}(Y)$ to be the ample cone $\overline{\mathscr{A}}(Y_t)$ of Y_t, viewed as a subset of $H^2(Y; \mathbb{R})$.

Lemma 2.8. *With notation as above, the following are true*:

(i) *If there do not exist any* -2*-curves on* Y, *then* $\overline{\mathscr{A}}(Y) = \overline{\mathscr{A}}_{\text{gen}}$. *More generally,* $\overline{\mathscr{A}}_{\text{gen}}$ *is the set of all* $x \in \mathscr{C}^+$ *such that* $x \cdot [D_i] \geq 0$ *and* $x \cdot \alpha \geq 0$ *for all effective numerical exceptional curves. In particular,* $\overline{\mathscr{A}}(Y) \subseteq \overline{\mathscr{A}}_{\text{gen}}$.

(ii) *We have* $\overline{\mathscr{A}}(Y) = \{x \in \overline{\mathscr{A}}_{\mathrm{gen}} : x \cdot [C] \geq 0 \text{ for all } -2\text{-curves } C\}$.

Proof. Let Y be a surface with no -2-curves (such surfaces exist and are generic by the surjectivity of the period map (Theorem 1.3)). Fix a nef divisor H on Y with $H \cdot D > 0$. Then $\overline{\mathscr{A}}(Y)$ is the set of all $x \in \mathscr{C}^+$ such that $x \cdot [D_i] \geq 0$ and $x \cdot [E] \geq 0$ for all exceptional curves E, and this last condition is equivalent to $x \cdot \alpha \geq 0$ for all $\alpha \in H^2(Y; \mathbb{Z})$ such that $\alpha^2 = \alpha \cdot [K_Y] = -1$ and $\alpha \cdot [H] \geq 0$ by Lemma 2.4. Since this condition is independent of the choice of Y, because we can choose the divisor H to be ample and to vary in a small deformation, the first part of (i) follows, and the remaining statements are clear. □

In fact, the argument above shows the following:

Lemma 2.9. *The set of effective numerical exceptional curves and the set* $\overline{\mathscr{A}}_{\mathrm{gen}}$ *are locally constant and hence are invariant in a global deformation with trivial monodromy under the induced identifications.* □

Lemma 2.10. *If* C *is a* -2*-curve on* Y*, then the wall* W^C *meets the interior of* $\overline{\mathscr{A}}_{\mathrm{gen}}$*, and in fact,* $r_C(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$*, where* $r_C : H^2(Y; \mathbb{R}) \to H^2(Y; \mathbb{R})$ *is reflection in the class* $[C]$*. Hence,* $\overline{\mathscr{A}}(Y)$ *is a fundamental domain for the action of the group* $\mathsf{W}(\Delta_Y)$ *on* $\overline{\mathscr{A}}_{\mathrm{gen}}$*, where* $\mathsf{W}(\Delta_Y)$ *is the group generated by the reflections in the classes in the set* Δ_Y *of* -2*-curves on* Y*.*

Proof. Clearly, if $r_C(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$, then W^C meets the interior of $\overline{\mathscr{A}}_{\mathrm{gen}}$. To see that $r_C(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$, assume first more generally that $\beta \in \Lambda$ is any class with $\beta^2 = -2$, and let r_β be the corresponding reflection. Then r_β permutes the set of $\alpha \in H^2(Y; \mathbb{Z})$ such that $\alpha^2 = \alpha \cdot [K_Y] = -1$ but does not necessarily preserve the condition that α is effective, i.e., that $\alpha \cdot [H] \geq 0$ for some nef divisor H on Y with $H \cdot D > 0$. However, for $\beta = [C]$, there exists by Proposition 1.5 a nef and big divisor H_0 such that $H_0 \cdot C = 0$ and $H \cdot D > 0$. Hence, $[H_0]$ is invariant under r_C, and so r_C permutes the set of $\alpha \in H^2(Y; \mathbb{Z})$ such that $\alpha^2 = \alpha \cdot [K_Y] = -1$ and $\alpha \cdot [H_0] \geq 0$. Thus, r_C permutes the set of effective numerical exceptional curves and hence the faces of $\overline{\mathscr{A}}_{\mathrm{gen}}$ so that $r_C(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$. Since $\overline{\mathscr{A}}(Y) \subseteq \overline{\mathscr{A}}_{\mathrm{gen}}$ is given by Lemma 2.8(ii), the final statement is then a general result in the theory of reflection groups [Bourbaki 1981, V §3]. □

Remark 2.11. (i) The argument for the first part of Lemma 2.10 essentially boils down to the following. Let $\overline{Y}$ be the normal surface obtained by contracting C. Then the reflection r_C is the monodromy associated to a generic smoothing of the singular surface $\overline{Y}$, and the cone $\overline{\mathscr{A}}_{\mathrm{gen}}$ is invariant under monodromy.

(ii) If E is an exceptional curve, then W^E is a face of $\overline{\mathscr{A}}(Y)$. For a generic Y (i.e., no -2-curves), Lemma 2.10 then says that the set of exceptional curves on Y is invariant under the reflection group generated by all classes of square -2 that become the classes of a -2-curve under some specialization. A somewhat more involved statement holds in the nongeneric case.

Lemma 2.12. *With* $\mathsf{W}(\Delta_Y)$ *as in Definition 1.1, for all* $w \in \mathsf{W}(\Delta_Y)$ *and all* $\beta \in \Lambda$, $\varphi_Y(w(\alpha)) = \varphi_Y(\alpha)$.

Proof. This is clear since $\varphi_Y([C]) = 1$ implies $\varphi_Y(r_C(\alpha)) = \varphi_Y(\alpha)$ for all $\alpha \in \Lambda$. □

Lemma 2.13. *Suppose that* $C = \sum_i a_i C_i$, *where the* C_i *are* -2*-curves,* $a_i \in \mathbb{Z}$, $C^2 = -2$, *the support of* C *is connected, and* $(C_i \cdot C_j)$ *is negative definite. Then there exists an element* w *in the group generated by reflections in the* $[C_i]$ *such that* $w([C]) = [C_i]$ *for some* i.

Proof. This follows from the well known fact that, if R is an irreducible root system such that all roots have the same length, then the Weyl group $\mathsf{W}(R)$ acts transitively on the set of roots. □

Theorem 2.14. *Let* $\beta \in \Lambda$ *with* $\beta^2 = -2$. *Then the following are equivalent*:

(i) *Let* Y_1 *be a deformation of* Y *with trivial monodromy such that* $\varphi_{Y_1}(\beta) = 1$. *Then, with* $\mathsf{W}(\Delta_{Y_1})$ *as in Definition 1.1, there exists* $w \in \mathsf{W}(\Delta_{Y_1})$ *such that* $w(\beta) = [C]$, *where* C *is a* -2*-curve on* Y_1. *In particular, if* Y_1 *is generic subject to the condition that* $\varphi_{Y_1}(\beta) = 1$ (*i.e., if* $\operatorname{Ker} \varphi_{Y_1} = \mathbb{Z} \cdot \beta$), *then* $\pm\beta = [C]$ *for a* -2*-curve* C.

(ii) *The wall* W^β *meets the interior of* $\overline{\mathscr{A}}_{\mathrm{gen}}$.

(iii) *If* r_β *is reflection in the class* β, *then* $r_\beta(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$.

Proof. Lemma 2.10 implies that (i) $\Longrightarrow$ (iii) in case $Y = Y_1$ and $\beta = [C]$ where C is a -2-curve. The case where $w(\beta) = [C]$ follows easily from this since, for all $w \in \mathsf{W}(\Delta_{Y_1})$, $w \circ r_\beta \circ w^{-1} = r_{w(\beta)}$. Lemma 2.9 then handles the case where Y_1 is replaced by a general deformation Y. Also, clearly (iii) $\Longrightarrow$ (ii). So it is enough to show that (ii) $\Longrightarrow$ (i). In fact, by Lemma 2.13, it is enough to show that, if Y is any surface such that $\varphi_Y(\beta) = 1$ and W^β meets the interior of $\overline{\mathscr{A}}_{\mathrm{gen}}$, then there exists a $w \in \mathsf{W}(\Delta_Y)$ such that $w(\beta) = [\sum_i a_i C_i]$ where $a_i \in \mathbb{Z}^+$, the C_i are curves disjoint from D, and $\bigcup_i C_i$ is connected.

By hypothesis, there exists an x in the interior of $\overline{\mathscr{A}}_{\mathrm{gen}}$ such that $x \cdot \beta = 0$. In particular, $x \cdot [D_i] > 0$ for all i. We can assume that $x = [H]$ is the class of a divisor H. After replacing x by $w(x)$ and β by $w(\beta)$ for some $w \in \mathsf{W}(\Delta_Y)$, we can assume that x (and hence H) lies in $\overline{\mathscr{A}}(Y)$ so that H is a nef and big divisor with $H \cdot D_i > 0$ for all i, and we still have $\varphi_Y(\beta) = 1$ by Lemma 2.12. By Lemma 2.4, possibly after replacing β by $-\beta$, $\beta = [\sum_i a_i C_i]$ where the C_i are irreducible curves and $a_i \in \mathbb{Z}^+$. Since $\beta \cdot [H] = \sum_i a_i (C_i \cdot H) = 0$, $C_i \cdot H \geq 0$, and $D_j \cdot H > 0$, $C_i \cdot H = 0$ for all i, and no C_i is equal to D_j for any j. Hence, the C_i are curves meeting each D_j in at most finitely many points and $\sum_i a_i (C_i \cdot D_j) = 0$ so that $C_i \cap D_j = \varnothing$. Finally, each $(C_i)^2 < 0$ by Hodge index, and so each C_i is a -2-curve. Moreover, the C_i span a negative definite lattice, and in particular, their classes are independent. From this, the statement about the connectedness of $\bigcup_i C_i$ is clear. □

Definition 2.15. Let $R = R_Y$ be the set of all $\beta \in \Lambda$ such that $\beta^2 = -2$ and such that there exists some deformation of Y for which β becomes the class of a -2-curve. Following [Gross et al. 2013], we call R the set of *Looijenga roots* (or briefly *roots*) of Y. Note that R only depends on the deformation type of Y.

The definition of R is slightly ill-posed since we have not specified an identification of the cohomologies of the fibers along the deformation. In particular, if $\beta = [C]$ is a -2-curve on Y, then by Remark 2.11(i) if Y' is a nearby deformation of Y, then a general smoothing of the ordinary double point on the contraction of C on Y has monodromy that sends $[C]$ to $-[C]$, and hence, $-\beta \in R$ as well. To avoid this issue, it is simpler to define R to be the set of $\beta \in \Lambda$, $\beta^2 = -2$, which satisfy either of the equivalent conditions Theorem 2.14(ii)–(iii).

Given Y, let Δ_Y be the set of classes of -2-curves on Y and $\mathsf{W}(\Delta_Y)$ the reflection group generated by Δ_Y. Finally set R^{nod}, the set of *nodal classes*, to be $\mathsf{W}(\Delta_Y)\cdot\Delta_Y$. Then $R^{\mathrm{nod}} \subseteq R$.

Corollary 2.16. (i) *If $f : H^2(Y;\mathbb{Z}) \to H^2(Y;\mathbb{Z})$ is an integral isometry preserving the classes $[D_i]$ such that $f(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$, then $f(R) = R$.*

(ii) *If $\mathsf{W}(R)$ is the reflection group generated by reflections in the elements of R, then $\mathsf{W}(R)\cdot R = R$ and $w(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$ for all $w \in \mathsf{W}(R)$.* □

Remark 2.17. A result similar to Theorem 2.14 classifies the elements of $H^2(Y;\mathbb{Z})$ that are represented by the class of a smoothly embedded 2-sphere of self-intersection -2 in terms of the "super P-cell" of [Friedman and Morgan 1988].

For the case where the length $r(D) \le 5$, Looijenga [1981] defines a subset R_L of Λ by starting with a particular configuration B of elements of square -2 (a *root basis* in his terminology) and setting $R_L = \mathsf{W}(B)\cdot B$, where $\mathsf{W}(B)$ is the reflection group generated by B. In fact, the set R_L is just the set R of Looijenga roots.

Proposition 2.18. *In the above notation, $R_L = R$.*

Proof. It is easy to see from the construction of [Looijenga 1981, I §2] that $B \subseteq R$. Hence, $R_L \subseteq R$. Conversely, if $\alpha \in R$, then, by Corollary 2.16(ii), $r_\alpha(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$. It then follows from [Looijenga 1981, Proposition I (4.7)] that $r_\alpha \in \mathsf{W}(B)$. By a general result in the theory of reflection groups [Bourbaki 1981, V §3.2, Theorem 1(iv)], $r_\alpha = r_\beta$ for some $\beta \in R_L$. Thus, $\alpha = \pm\beta$ so that $\alpha \in R_L$. Hence, $R \subseteq R_L$, and therefore, $R_L = R$. □

Example 2.19. Let (Y, D) be the blowup of $\mathbb{P}^2$ at $N \ge 10$ general points on an irreducible nodal cubic curve. We let h be the pullback of the class of a line on $\mathbb{P}^2$ and $e_1, \dots, e_N$ be the classes of the exceptional curves.

(i) Let $\alpha = -3h + \sum_{i=1}^{10} e_i$. Then $\alpha^2 = \alpha\cdot[K_Y] = -1$ so that α is a numerical exceptional curve. But there exists a nef and big divisor H (for example h) such that $\alpha\cdot[H] < 0$ so that α is not effective. Hence, $\alpha\cdot x \le 0$ for all $x \in \overline{\mathscr{A}}(Y) = \overline{\mathscr{A}}_{\mathrm{gen}}$ since W^α

does not pass through the interior of $\overline{\mathscr{A}}_{\text{gen}}$. Note that W^α is never a face of $\overline{\mathscr{A}}_{\text{gen}}$. For $N = 10$, $W^{-\alpha}$ is a face of $\overline{\mathscr{A}}_{\text{gen}}$, but this is no longer the case for $N \geq 11$. Thus, the condition $\alpha \cdot [H] \geq 0$ for some H such that $H \cdot D > 0$ is necessary for α to be effective.

More generally, let $f = 3h - \sum_{i=1}^{9} e_i$ and set $\alpha = kf + e_{10}$ (the case above corresponds to $k = -1$). As above, α is a numerical exceptional curve. For $k \leq -1$, $h \cdot \alpha < 0$. Hence, α is not effective. For $k \geq 1$, α is effective but it is not the class of an exceptional curve: for all $x \in \overline{\mathscr{A}}_{\text{gen}}$, $x \cdot f > 0$, and $x \cdot e_{10} \geq 0$. Hence, $x \cdot \alpha > 0$ for all $x \in \overline{\mathscr{A}}_{\text{gen}}$. Thus, W^α is not a face of $\overline{\mathscr{A}}_{\text{gen}}$ and so α is not the class of an exceptional curve.

(ii) With α any of the classes as above, suppose that $N \geq 11$ and $k \neq 0$ and set $\beta = \alpha - e_{11}$. Then $\beta^2 = -2$ and $\beta \cdot [K_Y] = 0$. However,

$$r_\beta(e_{11}) = e_{11} + (e_{11} \cdot \beta)\beta = \alpha.$$

Since $W^{e_{11}}$ is a face of $\overline{\mathscr{A}}_{\text{gen}}$ and W^α is not a face of $\overline{\mathscr{A}}_{\text{gen}}$, $r_\beta(\overline{\mathscr{A}}_{\text{gen}}) \neq \overline{\mathscr{A}}_{\text{gen}}$. Hence, β does not satisfy any of the equivalent conditions of Theorem 2.14 so that $\beta \notin R$.

Remark 2.20. In the situation of the example above, it is well known that if D is irreducible, $N \leq 9$ (i.e., $D^2 \geq 0$), and there are no -2-curves on Y, then every numerical exceptional curve is the class of an exceptional curve, so (i) above is best possible. A generalization is given in Proposition 3.3 below. We shall show in Proposition 3.5 that the example in (ii) is best possible as well.

The numerical exceptional curves given in Example 2.19(i) were known to Du Val. In fact, he showed that they are essentially the only numerical exceptional curves in case Y is the blowup of $\mathbb{P}^2$ at ten points [Du Val 1937, pp. 46–47].

Proposition 2.21. *Suppose that (Y, D) is the blowup of $\mathbb{P}^2$ at ten points lying on an irreducible cubic, that Y is generic in the sense that there are no -2-curves on Y, and that α is a numerical exceptional curve. Then there exists an exceptional curve E on Y and an integer k such that α is the class of $k(D + E) + E$.*

Proof. Suppose that α is a numerical exceptional curve on Y. Then, since $K_Y^2 = -1$, $\lambda = \alpha + [D] = \alpha - [K_Y]$ satisfies $\lambda^2 = \lambda \cdot \alpha = \lambda \cdot [K_Y] = 0$. In particular, $\lambda \in \Lambda$. Conversely, given an isotropic vector $\lambda \in \Lambda$, if we set $\alpha = \lambda + [K_Y]$, then α is a numerical exceptional curve.

Any isotropic vector $\lambda \in \Lambda$ can be uniquely written as $n\lambda_0$, where $n \in \mathbb{Z}$ and λ_0 is primitive and lies in $\overline{\mathscr{C}^+}$. Note that $H^2(Y; \mathbb{Z}) = \mathbb{Z}[K_Y] \oplus \Lambda$ and that $\Lambda = U \oplus (-E_8)$ (both sums orthogonal). An easy exercise shows that, if $\mathrm{Aut}^+(\Lambda)$ is the group of integral isometries A of Λ such that $A(\mathscr{C}^+ \cap \Lambda) = \mathscr{C}^+ \cap \Lambda$, i.e., A has real spinor norm equal to 1, then every $A \in \mathrm{Aut}^+(\Lambda)$ extends uniquely to an integral isometry of $H^2(Y; \mathbb{Z})$ fixing $[K_Y]$ and hence $[D]$ and moreover that $\mathrm{Aut}^+(\Lambda)$ acts transitively on the set of (nonzero) primitive isotropic vectors in $\overline{\mathscr{C}^+} \cap \Lambda$. Hence, there exists

an $A \in \mathrm{Aut}^+(\Lambda)$ such that $A(\lambda_0) = f$ in the notation of Example 2.19. If we continue to let A denote the extension of A to an isometry of $H^2(Y;\mathbb{Z})$, then $A(\alpha) = nf + [K_Y] = (n-1)f + e_{10}$ since $f = -[K_Y] + e_{10}$. It follows that $\alpha = (n-1)\lambda_0 + A^{-1}(e_{10})$. Using Proposition 3.5 below, A^{-1} preserves the walls of the ample cone of Y, and thus, $A^{-1}(e_{10}) = e$ is the class of an exceptional curve E, and $\lambda_0 = A^{-1}(f) = A^{-1}([D] + e_{10}) = [D] + E$. Hence, setting $k = n-1$, α is the class of $k(D+E) + E$ as claimed. □

The proof above shows the following:

Corollary 2.22. *Let (Y, D) be the blowup of $\mathbb{P}^2$ at ten points lying on an irreducible cubic and such that there are no -2-curves on Y, let α be a numerical exceptional curve on Y, and let $\lambda = \alpha - [K_Y]$. Then*

(i) *α is effective if and only if $\lambda \in (\overline{\mathscr{C}^+} - \{0\}) \cap \Lambda$,*

(ii) *α is not effective if and only if $\lambda \in (-\overline{\mathscr{C}^+}) \cap \Lambda$, and*

(iii) *α is the class of an exceptional curve if and only if λ is a primitive isotropic vector in $\overline{\mathscr{C}^+} \cap \Lambda$. Thus, there is a bijection from the set of exceptional curves on Y to the set of primitive isotropic vectors in $\overline{\mathscr{C}^+} \cap \Lambda$.* □

Remark 2.23. In the above situation, let W be the group generated by the reflections in the classes $e_1 - e_2, \ldots, e_9 - e_{10}, h - e_2 - e_2 - e_3$, which are easily seen to be Looijenga roots. A classical argument (usually called Noether's inequality) shows that, if λ_0 is a primitive integral isotropic vector in Λ lying in $\overline{\mathscr{C}^+}$, then there exists $w \in \mathsf{W}$ such that $w(\lambda_0) = f = 3h - \sum_{i=1}^{9} e_i$ in the notation of Example 2.19. Thus, W acts transitively on the set of such vectors. Using standard results about the affine Weyl group of E_8, it is then easy to see that $\mathsf{W} = \mathrm{Aut}^+(\Lambda)$. This was already noted in [Du Val 1937].

3. Roots and the ample cone

By Corollary 2.16, if $f : H^2(Y;\mathbb{Z}) \to H^2(Y;\mathbb{Z})$ is an integral isometry preserving the classes $[D_i]$ such that $f(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$, then $f(R) = R$. In this section, we find criteria for when the converse holds.

Lemma 3.1. *Let $f : H^2(Y;\mathbb{Z}) \to H^2(Y;\mathbb{Z})$ be an integral isometry preserving $\mathscr{C}^+$ and the classes $[D_i]$. If $f(\overline{\mathscr{A}}_{\mathrm{gen}}) \cap \overline{\mathscr{A}}_{\mathrm{gen}}$ contains an open set, then $f(\overline{\mathscr{A}}_{\mathrm{gen}}) = \overline{\mathscr{A}}_{\mathrm{gen}}$.*

Proof. Choosing $x \in f(\overline{\mathscr{A}}_{\mathrm{gen}}) \cap \overline{\mathscr{A}}_{\mathrm{gen}}$ corresponding to an ample divisor, it is easy to see that $f(\overline{\mathscr{A}}_{\mathrm{gen}})$ and $\overline{\mathscr{A}}_{\mathrm{gen}}$ have the same set of walls and hence are equal. □

Next we deal with the case where one component of D is a smooth rational curve of self-intersection -1.

Lemma 3.2. *Suppose that D is reducible and that $D_r^2 = -1$. Let $(\overline{Y}, \overline{D})$ be the anticanonical pair obtained by contracting D_r. Then any isometry f of $H^2(Y;\mathbb{Z})$ preserving the classes $[D_i]$, $1 \le i \le r$, defines an isometry $\overline{f}$ of $H^2(\overline{Y};\mathbb{Z})$ preserving the classes $[\overline{D}_i]$, $1 \le i \le r-1$, and conversely. Moreover, f preserves $\overline{\mathscr{A}}_{\mathrm{gen}}(Y)$ if and only if $\overline{f}$ preserves $\overline{\mathscr{A}}_{\mathrm{gen}}(\overline{Y})$, and R_Y is naturally identified with the roots $R_{\overline{Y}}$ of $\overline{Y}$.*

Proof. The first statement is clear. Identifying $H^2(\overline{Y},\mathbb{Z})$ with $[D_r]^\perp \subseteq H^2(Y;\mathbb{Z})$, it is clear that $\overline{\mathscr{A}}_{\mathrm{gen}}(Y) \cap [D_r]^\perp = \overline{\mathscr{A}}_{\mathrm{gen}}(\overline{Y})$. Hence, if f preserves $\overline{\mathscr{A}}_{\mathrm{gen}}(Y)$, then $\overline{f}$ preserves $\overline{\mathscr{A}}_{\mathrm{gen}}(\overline{Y})$. Since a divisor $\overline{H}$ on $\overline{Y}$ is ample if and only if $N\overline{H} - D_r$ is ample for all $N \gg 0$, it follows that, if $\overline{f}$ preserves $\overline{\mathscr{A}}_{\mathrm{gen}}(\overline{Y})$, then $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) \cap \overline{\mathscr{A}}_{\mathrm{gen}}(Y)$ contains an open set, and hence, $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y)$ by Lemma 3.1. It follows from this and from Theorem 2.14 that R_Y is naturally identified with $R_{\overline{Y}}$ (or directly from the definition by noting that there is a bijection from the set of deformations of (Y, D) to those of $(\overline{Y}, \overline{D})$). □

Henceforth, then, we shall always assume if need be that no component of D is a smooth rational curve of self-intersection -1.

We turn to the straightforward case where (Y, D) is not negative definite.

Proposition 3.3. *Suppose that (Y, D) and (Y', D') are two anticanonical pairs with $r(D) = r(D')$ and neither pair is negative definite. If $f : H^2(Y;\mathbb{Z}) \to H^2(Y';\mathbb{Z})$ is an integral isometry with $f([D_i]) = [D_i']$ for all i, then $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y')$ and hence $f(R_Y) = R_{Y'}$. Moreover,*

$$R_Y = \{\beta \in \Lambda(Y, D) : \beta^2 = -2\}.$$

Proof. By Lemma 3.2, we may assume that no D_i has self-intersection -1. The statement that the cycle is not negative definite is then equivalent to the statement that either $D_j^2 \ge 0$ for some j or $D_i^2 = -2$ for all i and $r \ge 2$. In the first case, D_j is nef and $D_j \cdot D > 0$. Hence, if α is a numerical exceptional curve such that $\alpha \cdot [D_j] \ge 0$, then α is effective by Lemma 2.4. Thus, $\overline{\mathscr{A}}_{\mathrm{gen}}(Y)$ is the set of all $x \in \mathscr{C}_D^+(Y)$ such that $x \cdot \alpha \ge 0$ for all numerical exceptional curves α such that $\alpha \cdot [D_j] \ge 0$. Since $f(\alpha)^2 = \alpha^2$, $f([D_j]) = [D_j']$, and $f(\alpha) \cdot [K_{Y'}] = \alpha \cdot [K_Y]$, it follows that $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y')$. Applying this to reflection in a class β of square -2 in $\Lambda(Y, D)$ then implies that $\beta \in R_Y$.

The case where $D_i^2 = -2$ for every i is similar, using the nef divisor $D = \sum_i D_i$ with $D^2 = 0$. If α is a numerical exceptional curve, then α is effective since $(-\alpha + [K_Y]) \cdot [D] = \alpha \cdot [K_Y] = -1$. The rest of the argument proceeds as before. □

Remark 3.4. If D is irreducible and not negative definite (i.e., $D^2 \ge 0$) and there are no -2-curves on Y, then, as is well known and noted in Remark 2.20, every numerical exceptional curve is the class of an exceptional curve. However, if D is reducible but not negative definite, then, even if there are no -2-curves on Y, there

may well exist numerical exceptional curves that are not effective and effective numerical exceptional curves that are not the class of an exceptional curve.

From now on, we assume that D is negative definite. The case $K_Y^2 = -1$ can also be handled by straightforward methods as noted in [Looijenga 1981]. (See also [Friedman and Morgan 1988, II (2.7)(c)] in case D is irreducible.)

Proposition 3.5. *Let (Y, D) and (Y', D') be two negative definite anticanonical pairs with $r(D) = r(D')$ and $K_Y^2 = K_{Y'}^2 = -1$. Let $f : H^2(Y; \mathbb{Z}) \to H^2(Y'; \mathbb{Z})$ be an isometry such that $f([D_i]) = [D_i']$ for all i and $f(\mathscr{C}^+(Y)) = \mathscr{C}^+(Y')$. Then $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y')$. Moreover,*

$$R_Y = \{\beta \in \Lambda(Y, D) : \beta^2 = -2\}.$$

Hence, $f(R_Y) = R_{Y'}$.

Proof. Since (Y, D) is negative definite, no component of D is a smooth rational curve of self-intersection -1. Fix a nef and big divisor H such that $H \cdot D_i = 0$ for all i and $H \cdot G > 0$ for every irreducible curve $G \neq D_i$. If α is a numerical exceptional curve, $(\alpha - [K_Y])^2 = (\alpha + [D])^2 = 0$. By Lemma 2.6, α is effective if and only if $[H] \cdot \alpha > 0$ if and only if $[H] \cdot (\alpha + [D]) > 0$. By the light cone lemma [Friedman and Morgan 1988, p. 320], this last condition is equivalent to $\alpha + [D] \in \overline{\mathscr{C}^+} - \{0\}$. Since this condition is clearly preserved by an isometry f as in the statement of the proposition, we see that $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y')$. The final statement then follows as in the proof of Proposition 3.3. □

Remark 3.6. The hypothesis $K_Y^2 = -1$ implies that $r(D) \leq 10$, so there are only finitely many examples of the above type. For $r(D) = 10$, there is essentially just one combinatorial possibility for (Y, D) neglecting the orientation [Friedman and Miranda 1983, (4.7)], where it is easy to check that this is the only possibility. For $r(D) = 9$, however, there are two different possibilities for the combinatorial type of (Y, D) (again ignoring the orientation). Begin with an anticanonical pair $(\overline{Y}, \overline{D})$, where $\overline{Y}$ is a rational elliptic surface and $\overline{D} = \overline{D}_0 + \cdots + \overline{D}_8$ is a fiber of type $\tilde{A}_8$ (or I_9 in Kodaira's notation). There is a unique such rational elliptic surface $\overline{Y}$, and its Mordell–Weil group has order 3 (see, for example, [Miranda and Persson 1986]). In particular, possibly after relabeling the components, there is an exceptional curve meeting $\overline{D}_i$ if and only if $i = 0, 3, 6$. It is easy to see that blowing up a point on a component $\overline{D}_i$ meeting an exceptional curve leads to a different combinatorial possibility for an anticanonical pair (Y, D) with $K_Y^2 = -1$ and $r(D) = 9$ than blowing up a point on a component $\overline{D}_i$ that does not meet an exceptional curve.

We turn now to the case where (Y, D) is negative definite but with no assumption on K_Y^2.

Definition 3.7. A point $x \in \mathscr{C}^+ \cap \Lambda$ is *R-distinguished* if there exists a codimension-1 negative definite subspace V of $\Lambda \otimes \mathbb{R}$ spanned by elements of R such that $x \in V^\perp$. Note that the definition only depends on the deformation type of the pair (Y, D).

Remark 3.8. Clearly, if V is a codimension-1 negative definite subspace of $\Lambda \otimes \mathbb{R}$ spanned by elements of R, then V is defined over $\mathbb{Q}$ and $V^\perp \cap (\Lambda \otimes \mathbb{R})$ is a one-dimensional subspace of $H^2(Y; \mathbb{R})$ defined over $\mathbb{Q}$ and spanned by an $h \in H^2(Y; \mathbb{Z})$ with $h^2 > 0$, $h \cdot [D_i] = 0$, and $h \cdot \beta = 0$ for all $\beta \in R \cap V$. Hence, if $h \in \mathscr{C}^+ \cap \Lambda$, then h is R-distinguished.

Also, if the rank of Λ is one, then $\{0\}$ is a codimension-1 negative definite subspace of $\Lambda \otimes \mathbb{R}$, and hence, every point of $\mathscr{C}^+ \cap \Lambda$ is R-distinguished.

However, as we shall see, there exist deformation types (Y, D) with no R-distinguished points.

The following is also clear:

Lemma 3.9. *Let (Y, D) and (Y', D') be two anticanonical pairs with $r(D) = r(D')$, and let $f : H^2(Y; \mathbb{Z}) \to H^2(Y'; \mathbb{Z})$ be an isometry such that $f([D_i]) = [D_i']$ for all i, $f(\mathscr{C}^+(Y)) = \mathscr{C}^+(Y')$, and $f(R_Y) = R_{Y'}$. Then, if x is an R_Y-distinguished point of $\mathscr{C}^+(Y) \cap \Lambda(Y, D)$, $f(x)$ is an $R_{Y'}$-distinguished point of $\mathscr{C}^+(Y') \cap \Lambda(Y', D')$.*

Our goal now is to prove this:

Theorem 3.10. *Suppose that (Y, D) and (Y', D') are two anticanonical pairs such that $r(D) = r(D')$. Let $f : H^2(Y; \mathbb{Z}) \to H^2(Y'; \mathbb{Z})$ be an isometry such that $f([D_i]) = [D_i']$ for all i, $f(\mathscr{C}^+(Y)) = \mathscr{C}^+(Y')$, and $f(R_Y) = R_{Y'}$. If there exists an R-distinguished point of $\mathscr{C}^+ \cap \Lambda$, then $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y')$.*

We begin by showing:

Proposition 3.11. *Let x be an R-distinguished point of $\mathscr{C}^+ \cap \Lambda$. Then $x \in \overline{\mathscr{A}}_{\mathrm{gen}}$. Moreover, if α is a numerical exceptional curve and α is not in the span of the $[D_j]$, then α is effective if and only if $\alpha \cdot x \geq 0$.*

Proof. It is enough by Lemma 2.9 to check this on some (global) deformation of (Y, D) with trivial monodromy. By Theorem 1.3, we can assume that

$$\operatorname{Ker} \varphi_Y = V \cap \Lambda,$$

where V is as in the definition of R-distinguished. In particular, if $C \in \Delta_Y$, i.e., C is a -2-curve on Y, then $[C] \in V$. It follows from Theorem 2.14(i) that every $\beta \in V \cap R$ is a sum of elements of Δ_Y so that Δ_Y spans V over $\mathbb{Q}$. Thus, there exist -2-curves $C_1, \ldots, C_k$ such that V is spanned by the classes $[C_i]$, and the intersection matrix $(C_i \cdot C_j)$ is negative definite. The classes $[C_1], \ldots, [C_k], [D_1], \ldots, [D_r]$ span a negative definite sublattice of $H^2(Y; \mathbb{Z})$. By Proposition 1.5, there exists a nef and big divisor H such that H is perpendicular to the curves $C_1, \ldots, C_k, D_1, \ldots, D_r$.

Clearly, then $[H] \in \overline{\mathscr{A}}(Y) \subseteq \overline{\mathscr{A}}_{\text{gen}}$ and $[H] = tx$ for some $t \in \mathbb{R}^+$. Hence, $x \in \overline{\mathscr{A}}_{\text{gen}}$ as well. Note that $[H]^\perp$ is spanned over $\mathbb{Q}$ by $[C_1], \ldots, [C_k], [D_1], \ldots, [D_r]$.

Since $x \in \overline{\mathscr{A}}(Y)$, if α is effective, $x \cdot \alpha \geq 0$. Conversely, suppose that α is a numerical exceptional curve with $x \cdot \alpha \geq 0$ and that α is not effective. Then $-\alpha + [K_Y] = [G]$, where G is effective, and $H \cdot (-\alpha + [K_Y]) = -\alpha \cdot [H] \leq 0$. Hence, $(-\alpha + [K_Y]) \cdot [H] = 0$.

Claim 3.12. *We have* $-\alpha + [K_Y] = \sum_i a_i [C_i] + \sum_j b_j [D_j]$, *where* $a_i, b_j \in \mathbb{Z}$.

Proof. In any case, since $-\alpha + [K_Y]$ is perpendicular to $[H]$, there must exist $a_i, b_j \in \mathbb{Q}$ such that $-\alpha + [K_Y] = \sum_i a_i [C_i] + \sum_j b_j [D_j]$. There exist $n_i, m_j \in \mathbb{Z}$ such that $-\alpha + [K_Y] = [G] = \sum_i n_i [C_i] + \sum_j m_j [D_j] + [F]$, where F is an effective curve not containing C_i or D_j in its support for any i, j. By Lemma 1.4(ii), $F = 0$, $a_i = n_i$, and $b_j = m_j$ for all i, j. Hence, $a_i, b_j \in \mathbb{Z}$. □

Because $-\alpha + [K_Y]$ is an integral linear combination of the $[C_i]$ and $[D_j]$, the same holds for α. Then $\alpha = \sum_i c_i [C_i] + \sum_j d_j [D_j]$ with $c_i, d_j \in \mathbb{Z}$. However, $\alpha^2 = -1 = \left(\sum_i c_i C_i\right)^2 + \left(\sum_j d_j D_j\right)^2$. Both terms are nonpositive, and so $\left(\sum_i c_i C_i\right)^2 \geq -1$. But if $\sum_i c_i C_i \neq 0$, then $\left(\sum_i c_i C_i\right)^2 \leq -2$. Thus, $\sum_i c_i C_i = 0$ and α lies in the span of the $[D_j]$. Conversely, if α is not in the span of the $[D_j]$ and $\alpha \cdot x \geq 0$, then α is the class of an effective curve. □

Proof of Theorem 3.10. It follows from Proposition 3.11 that, if $x \in \mathscr{C}^+(Y) \cap \Lambda(Y, D)$ is R_Y-distinguished, then $\overline{\mathscr{A}}_{\text{gen}}(Y)$ is the set of all $y \in \mathscr{C}_D^+(Y)$ such that $\alpha \cdot y \geq 0$ for all α a numerical exceptional curve on Y, not in the span of the $[D_i]$, such that $\alpha \cdot x \geq 0$. Let f be an isometry satisfying the conditions of the theorem. Then $f(x)$ is $R_{Y'}$-distinguished, and $f(\overline{\mathscr{A}}_{\text{gen}}(Y))$ is clearly the set of all $y \in \mathscr{C}_{D'}^+(Y')$ such that $\alpha \cdot y \geq 0$ for all α a numerical exceptional curve on Y', not in the span of the $[D_i']$, such that $\alpha \cdot f(x) \geq 0$. Again by Proposition 3.11, this set is exactly $\overline{\mathscr{A}}_{\text{gen}}(Y')$. □

Theorem 3.10 covers all of the cases in [Looijenga 1981] except for the case of five components: by inspection of the root diagrams on [Looijenga 1981, pp. 275–277], the complement of any trivalent vertex spans a negative definite codimension-1 subspace except in the case of five components. To give a direct argument along the above lines that also handles this case (and all of the other cases in [Looijenga 1981]), we recall the basic setup there: there exists a subset $B = \{\beta_1, \ldots, \beta_n\} \subseteq R$ such that B is a basis for $\Lambda \otimes \mathbb{R}$, and there exist $n_i \in \mathbb{Z}^+$ such that $\left(\sum_i n_i \beta_i\right) \cdot \beta_j > 0$ for all j (compare also [Looijenga 1980, (1.18)]). In particular, note that the intersection matrix $(\beta_i \cdot \beta_j)$ is nonsingular. Finally, by the classification of [Looijenga 1981, Theorem (1.1)], there exists a deformation of (Y, D) for which $\beta_i = [C_i]$ is the class of a -2-curve for all i. (With some care, this explicit argument could be avoided by appealing to the surjectivity of the period map and Theorem 2.14(i).)

Theorem 3.13. *Let (Y, D) and (Y', D') be two anticanonical pairs satisfying the hypotheses of the preceding paragraph, both negative definite, with $r(D) = r(D')$, and let $f : H^2(Y; \mathbb{Z}) \to H^2(Y'; \mathbb{Z})$ be an isometry such that $f([D_i]) = [D_i']$ for all i, $f(\mathscr{C}^+(Y)) = \mathscr{C}^+(Y')$, and $f(R_Y) = R_{Y'}$. Then $f(\overline{\mathscr{A}}_{\mathrm{gen}}(Y)) = \overline{\mathscr{A}}_{\mathrm{gen}}(Y')$.*

Sketch of the proof. With notation as in the paragraph preceding the statement of the theorem, let $h = \sum_i n_i \beta_i$ have the property that $h \cdot \beta_i > 0$. By the arguments used in the proof of Theorem 3.10, it is enough to show that $h \in \overline{\mathscr{A}}_{\mathrm{gen}}$ and that, if α is a numerical exceptional curve and α is not in the span of the $[D_j]$, then α is effective if and only if $\alpha \cdot h \geq 0$. Also, it is enough to prove this for some deformation of (Y, D), so we can assume $\beta_i = [C_i]$ is the class of a -2-curve for all i and hence that h is the class of $H = \sum_i n_i C_i$. By construction, $H \cdot C_j > 0$ for every j. Hence, H is nef and big. By Lemma 2.6, it is enough to show that, if G is an irreducible curve not equal to D_i for any i, then $H \cdot G > 0$. Since H is nef, it suffices to rule out the case $H \cdot G = 0$, in which case $G^2 < 0$. As $G \neq D_j$ for any j, then G is either a -2-curve or an exceptional curve. The case where G is a -2-curve is impossible since then G is orthogonal to the span of the $[C_i]$, but the $[C_i]$ span Λ over $\mathbb{Q}$ and the intersection form is nondegenerate. So $G = E$ is an exceptional curve disjoint from the C_i. If $(\overline{Y}, \overline{D})$ is the anticanonical pair obtained by contracting E, then the $[C_i]$ define classes in $\overline{\Lambda} = \Lambda(\overline{Y}, \overline{D})$. Since the intersection form $(C_i \cdot C_j)$ is nondegenerate, the rank of $\overline{\Lambda}$ is at least that of Λ. It is easy to check that the classes of $\overline{D}_1, \ldots, \overline{D}_r$ are linearly independent: if say E meets D_1, then the intersection matrix of $\overline{D}_2, \ldots, \overline{D}_r$ is still negative definite and then Lemma 1.4(ii) (with $F = \overline{D}_1$ and $G_1, \ldots, G_n = \overline{D}_2, \ldots, \overline{D}_r$) shows that the classes of $\overline{D}_1, \ldots, \overline{D}_r$ are linearly independent. Hence, the rank of $H^2(\overline{Y}; \mathbb{Z})$ is greater than or equal to the rank of $H^2(Y; \mathbb{Z})$, which contradicts the fact that $\overline{Y}$ is obtained from Y by contracting an exceptional curve. □

4. Some examples

Example 4.1. We provide a series of examples that satisfy the hypotheses of Theorem 3.10, where the number of components and the multiplicities are arbitrarily large. Let $(\overline{Y}, \overline{D})$ be the anticanonical pair obtained by making $k+6$ infinitely near blowups starting with the double point of a nodal cubic. Thus, $\overline{D} = \overline{D}_0 + \cdots + \overline{D}_{k+6}$, where $\overline{D}_0^2 = -k$, $\overline{D}_i^2 = -2$, $1 \leq i \leq k+5$, and $\overline{D}_{k+6}^2 = -1$. Now blow up $N \geq 1$ points $p_1, \ldots, p_N$ on $\overline{D}_{k+6}$, and let (Y, D) be the resulting anticanonical pair. Note that (Y, D) is negative definite as long as $k \geq 3$ or $k = 2$ and $N \geq 2$. Clearly $r(D) = k+7$ and $K_Y^2 = 3 - k - N$. It follows that $\Lambda = \Lambda(Y, D)$ has rank N. If $E_1, \ldots, E_N$ are the exceptional curves corresponding to $p_1, \ldots, p_N$, then the classes $[E_i] - [E_{i+1}]$ span a negative definite root lattice of type A_{N-1} in Λ. By making all of the blowups

infinitely near to the first point, we see that all of the classes $[E_i]-[E_{i+1}]$ lie in R. Hence, (Y, D) satisfies the hypotheses of Theorem 3.10.

Next we turn to examples where the rank of Λ is small. The case where the rank of Λ is 1 is covered by Theorem 3.10 as well as the case where the rank of Λ is 2 and $R \neq \varnothing$. Note that, conjecturally at least, the case where $R \neq \varnothing$ should be related to the question of whether the dual cusp singularity deforms to an ordinary double point. It is easy to construct examples where the rank of Λ is 2 and with $R \neq \varnothing$: begin with an anticanonical pair $(\hat{Y}, \hat{D})$ where the rank of $\Lambda(\hat{Y}, \hat{D})$ is 1, locate a component $\hat{D}_i$ such that there exists an exceptional curve E on $\hat{Y}$ with $E \cdot \hat{D}_i = 1$, and blow up a point of $\hat{D}_i$ to obtain a new anticanonical pair (Y, D) together with exceptional curves E and E' (where we continue to let E denote the pullback to Y and E' the new exceptional curve) such that $[E]-[E'] \in R$. So our interest is in finding examples where $R = \varnothing$.

Remark 4.2. In case the rank of Λ is 2 and $R \neq \varnothing$, it is easy to see that either $(\overline{\mathscr{A}}_{\mathrm{gen}} \cap \Lambda)/\mathbb{R}^+$ is a closed (compact) interval or $\overline{\mathscr{A}}_{\mathrm{gen}} \cap \Lambda = \mathscr{C}^+ \cap \Lambda$ (and in fact both cases arise). In either case, there is at most one wall W^β with $\beta \in R$ passing through the interior of $\overline{\mathscr{A}}_{\mathrm{gen}} \cap \Lambda$, and hence, either $R = \varnothing$ or $R = \{\pm\beta\}$.

Example 4.3. We give an example where the rank of Λ is 2 and there are no $\beta \in \Lambda$ such that $\beta^2 = -2$ (in particular, $R = \varnothing$; hence, the condition $f(R) = R$ is automatic for every isometry f) and of an isometry f that preserves $\mathscr{C}^+$ and the classes $[D_i]$ but not the generic ample cone. Let $(\overline{Y}, \overline{D})$ be the anticanonical pair obtained by making nine infinitely near blowups starting with the double point of a nodal cubic. Thus, $\overline{D} = \overline{D}_0 + \cdots + \overline{D}_9$, where $\overline{D}_0 = 3H - 2E_1 - \sum_{i=2}^9 E_i$, $\overline{D}_i = E_i - E_{i+1}$, $1 \leq i \leq 8$, and $\overline{D}_9 = E_9$. Make two more blowups, one at a point p_{10} on $\overline{D}_9$ and one at a point p_{11} on $\overline{D}_4$. This yields an anticanonical pair (Y, D) with $D_0 = 3H - 2E_1 - \sum_{i=2}^9 E_i$, $D_i = E_i - E_{i+1}$, $i > 0$ and $i \neq 4$, and $D_4 = E_4 - E_5 - E_{11}$. Thus,

$$(-d_0, \ldots, -d_9) = (3, 2, 2, 2, 3, 2, 2, 2, 2, 2),$$

i.e., D is of type $\left(\begin{smallmatrix} 3 & 3 \\ 3 & 5 \end{smallmatrix}\right)$, with dual cycle $\left(\begin{smallmatrix} 6 & 8 \\ 0 & 0 \end{smallmatrix}\right)$ in the notation of [Friedman and Miranda 1983]. Set

$$G_1 = 5H - 2\sum_{i=1}^{4} E_i - \sum_{i=5}^{10} E_i - E_{11} \quad \text{and} \quad G_2 = 10H - 5\sum_{i=1}^{4} E_i - \sum_{i=5}^{10} E_i - 4E_{11}.$$

It is straightforward to check that $(G_i \cdot D_j) = 0$ for $i = 1, 2$ and $0 \leq j \leq 9$. Hence, $G_1, G_2 \in \Lambda$. Also,

$$G_1^2 = 2, \quad G_2^2 = -22, \quad G_1 \cdot G_2 = 0.$$

The corresponding quadratic form

$$q(n, m) = (nG_1 + mG_2)^2 = 2n^2 - 22m^2$$

has discriminant $-44 = -2^2 \cdot 11$. Note that this is consistent with the fact that the discriminant of the dual cycle is

$$\det \begin{pmatrix} -6 & 2 \\ 2 & -8 \end{pmatrix} = 44.$$

It is easy to see that G_1 and G_2 are linearly independent mod 2 and hence span a primitive lattice, which must therefore equal Λ.

First, we claim that there is no element of Λ of square -2. This is equivalent to the statement that there is no solution in integers to the equation $n^2 - 11m^2 = -1$, i.e., that the fundamental unit in $\mathbb{Z}[\sqrt{11}]$ has norm 1. But clearly if there were an integral solution to $n^2 - 11m^2 = -1$, then since $-11 \equiv 1 \bmod 4$, we could write -1 as a sum of two squares mod 4, which is impossible. In fact, the fundamental unit in $\mathbb{Z}[\sqrt{11}]$ is $10 + 3\sqrt{11}$. Thus, if R is the set of roots for (Y, D), then $R = \varnothing$. In particular, any isometry f trivially satisfies $f(R) = R$.

Finally, we claim there is an isometry f of $H^2(Y; \mathbb{Z})$ such that $f([D_i]) = [D_i]$ for all i and $f(\mathscr{C}^+) = \mathscr{C}^+$ but such that f does not preserve the generic ample cone. Note the unit group U of $\mathbb{Z}[\sqrt{11}]$ acts as a group of isometries on Λ and hence acts as a group of isometries (with $\mathbb{Q}$-coefficients) of the lattice

$$H^2(Y; \mathbb{Q}) = (\Lambda \otimes \mathbb{Q}) \oplus \bigoplus_i \mathbb{Q}[D_i],$$

fixing the classes $[D_i]$. Also, any isometry of Λ that is trivial on the discriminant group $\Lambda^\vee/\Lambda$ extends to an integral isometry of $H^2(Y; \mathbb{Z})$ fixing the $[D_i]$. Concretely, the discriminant form $\Lambda^\vee/\Lambda \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$. If $\mu = 10 + 3\sqrt{11}$, then it is easy to check that the automorphism of Λ corresponding to $\mu^2 = 199 + 60\sqrt{11}$ acts trivially on $\Lambda^\vee/\Lambda$ and hence defines an isometry f of $H^2(Y; \mathbb{Z})$ fixing the $[D_i]$. Then f acts freely on $(\mathscr{C}^+ \cap \Lambda)/\mathbb{R}^+$, which is just a copy of $\mathbb{R}$ (and f acts on it via translation). But the intersection of the generic ample cone with Λ has the nontrivial wall $W^{E_{11}}$ so that the intersection cannot be all of $\mathscr{C}^+ \cap \Lambda$. It follows that $f^{\pm 1}$ does not preserve the generic ample cone. Explicitly, let $(\hat{Y}, \hat{D})$ be the surface obtained by contracting E_{11} and let $\hat{G}_1 = 4G_1 - G_2 = 10H - 3\sum_{i=1}^{10} E_i$ be the pullback of the positive generator of $\Lambda(\hat{Y}, \hat{D})$. Thus, $\hat{G}_1$ is nef and big so that $\hat{G}_1 \in \overline{\mathscr{A}}_{\text{gen}}$. Clearly $\hat{G}_1 \in W^{E_{11}}$. If $A = \left(\begin{smallmatrix} a & 11b \\ b & a \end{smallmatrix}\right)$ is the isometry of Λ corresponding to multiplication by the unit $a + b\sqrt{11}$, then $A(G_1) = aG_1 + bG_2$, $A(G_2) = 11bG_1 + aG_2$, and $A(\hat{G}_1) = (4a - 11b)G_1 + (4b - a)G_2$. Thus,

$$E_{11} \cdot A(\hat{G}_1) = (4a - 11b) + 4(4b - a) = 5b.$$

Hence, $E_{11}\cdot A(\hat{G}_1)<0$ if $b<0$. Taking f^{-1}, which corresponds to $199-60\sqrt{11}$, we see that $f^{-1}(\hat{G}_1)\notin \overline{\mathcal{A}}_{\text{gen}}$.

Example 4.4. In this example, the rank of Λ is 2 and $R=\varnothing$, but there exist infinitely many $\beta\in\Lambda$ such that $\beta^2=-2$. The condition $f(R)=R$ is again automatic for every isometry f, and reflection about every $\beta\in\Lambda$ with $\beta^2=-2$ is an isometry that preserves $\mathcal{C}^+$ and the classes $[D_i]$ but not the generic ample cone.

As in the previous example, let $(\overline{Y},\overline{D})$ be the anticanonical pair obtained by making nine infinitely near blowups starting with the double point of a nodal cubic. Thus, $\overline{D}=\overline{D}_0+\cdots+\overline{D}_9$, where $\overline{D}_0=3H-2E_1-\sum_{i=2}^9 E_i$, $\overline{D}_i=E_i-E_{i+1}$, $1\le i\le 8$, and $\overline{D}_9=E_9$. Make two more blowups, one at a point p_{10} on $\overline{D}_9$ and one at a point p_{11} on $\overline{D}_0$. This yields an anticanonical pair (Y,D) with $D_0=3H-2E_1-\sum_{i=2}^9 E_i-E_{11}$ and $D_i=E_i-E_{i+1}$, $1\le i\le 9$. Thus,

$$(-d_0,\dots,-d_9)=(4,2,2,2,2,2,2,2,2,2),$$

i.e., D is of type $\left(\begin{smallmatrix}4\\9\end{smallmatrix}\right)$, with dual cycle $\left(\begin{smallmatrix}12\\1\end{smallmatrix}\right)$ in the notation of [Friedman and Miranda 1983]. Set

$$G_1=10H-3\sum_{i=1}^{10}E_i \quad\text{and}\quad G_2=3H-\sum_{i=1}^{10}E_i+E_{11}.$$

It is straightforward to check that $(G_i\cdot D_j)=0$ for $i=1,2$ and $0\le j\le 9$. Hence, $G_1,G_2\in\Lambda$. Also,

$$G_1^2=10,\quad G_2^2=-2,\quad\text{and}\quad G_1\cdot G_2=0.$$

The corresponding quadratic form

$$q(n,m)=(nG_1+mG_2)^2=10n^2-2m^2$$

has discriminant $-20=-2^2\cdot 5$. Note that this is consistent with the fact that the discriminant of the dual cycle is

$$\det\begin{pmatrix}-12 & 2\\ 2 & -2\end{pmatrix}=20.$$

It is easy to see that G_1 and G_2 are linearly independent mod 2 and hence span a primitive lattice, which must therefore equal Λ.

To give a partial description of $\overline{\mathcal{A}}_{\text{gen}}\cap\Lambda$, note that (as for $\hat{G}_1$ in the previous example) G_1 is the pullback to Y of a positive generator for $\Lambda(\hat{Y},\hat{D})$, where $\hat{Y}$ denotes the surface obtained by contracting E_{11}. Thus, G_1 is nef and big so that $G_1\in\overline{\mathcal{A}}_{\text{gen}}$ and also $G_1\in W^{E_{11}}$. Hence,

$$\mathcal{C}^+\cap\Lambda=\{nG_1+mG_2: 5n^2-m^2>0,\ n>0\},$$

i.e., $n > 0$ and $-n\sqrt{5} < m < n\sqrt{5}$. The condition $E_{11} \cdot (nG_1 + mG_2) \geq 0$ gives $m \leq 0$. To get a second inequality on n and m, let

$$E' = 5H - 4E_{11} - \sum_{i=1}^{10} E_i.$$

Then $(E')^2 = E' \cdot K_Y = -1$, and $H \cdot E' > 0$. Hence, E' is effective. (In fact, one can show that E' is generically the class of an exceptional curve.) Thus, for all $nG_1 + mG_2 \in \overline{\mathscr{A}}_{\text{gen}}$,

$$E' \cdot (nG_1 + mG_2) = 20n + 9m \geq 0;$$

hence,

$$\overline{\mathscr{A}}_{\text{gen}} \cap \Lambda \subseteq \{nG_1 + mG_2 : n > 0,\ -\tfrac{20}{9}n \leq m \leq 0\}.$$

Next we describe the classes $\beta \in \Lambda$ with $\beta^2 = -2$. The element $\beta = aG_1 + bG_2 \in \Lambda$ satisfies $\beta^2 = -2$ if and only if $5a^2 - b^2 = -1$, i.e., if and only if $b + a\sqrt{5}$ is a unit in the (nonintegrally closed) ring $\mathbb{Z}[\sqrt{5}]$. For example, the class G_2 corresponds to 1; as we have seen, the wall $W^{G_2} = W^{E_{11}}$. The fundamental unit in $\mathbb{Z}[\sqrt{5}]$ is easily checked to be $9 + 4\sqrt{5}$. However, since we are only concerned with walls that are rays in the fourth quadrant $\{(nG_1 + mG_2) : n > 0,\ m < 0\}$, we shall consider instead $\pm(9 - 4\sqrt{5})$ and shall choose the sign corresponding to $\beta = 4G_1 - 9G_2$. Note that

$$\beta \cdot (nG_1 + mG_2) = 40n + 18m = 0 \Longleftrightarrow E' \cdot (nG_1 + mG_2) = 0.$$

Hence, $W^{\beta} = W^{E'}$. Moreover, for every $\gamma \in \Lambda$ such that $\gamma^2 = -2$ and such that the wall W^{γ} passes through the fourth quadrant, either $W^{\gamma} = W^{\beta}$ or the corresponding ray W^{γ} lies below W^{β}. Thus, for every $\gamma \in \Lambda$ with $\gamma^2 = -2$, r_{γ} does not preserve $\overline{\mathscr{A}}_{\text{gen}} \cap \Lambda$. Hence, $R = \varnothing$.

Note that, aside from the isometries r_{β}, where $\beta^2 = -2$, one can also construct isometries of infinite order preserving $\mathscr{C}^+$ and the classes $[D_i]$ that do not preserve $\overline{\mathscr{A}}_{\text{gen}}$ using multiplication by fundamental units in $\mathbb{Z}[\sqrt{5}]$ as in the previous example.

Remark 4.5. The exceptional curve E' used in the above example is part of a general series of such. For $n \geq 0$, let Y be the blowup of $\mathbb{P}^2$ at $2n + 1$ points $p_0, \ldots, p_{2n}$ with corresponding exceptional curves $E_0, \ldots, E_{2n}$, and consider the divisor

$$A = nH - (n-1)E_0 - \sum_{i=1}^{2n} E_i.$$

Then $A^2 = A \cdot K_Y = -1$, and it is easy to see that there exist $p_0, \ldots, p_{2n}$ such that A is the class of an exceptional curve. In fact, if $\mathbb{F}_1$ is the blowup of $\mathbb{P}^2$ at p_0, then $\Sigma = nH - (n-1)E_0$ is very ample on $\mathbb{F}_1$ and, for an anticanonical divisor $D \in |-K_{\mathbb{F}_1}| = |3H - E_0|$, $\Sigma \cdot D = 2n + 1$. From this, it is easy to see that we

can choose the points $p_1, \ldots, p_{2n}$ to lie on the image of D in $\mathbb{P}^2$, and hence, we can arrange the blowup Y to have (for example) an irreducible anticanonical nodal curve.

Acknowledgements

It is a pleasure to thank Mark Gross, Paul Hacking, and Sean Keel for access to their manuscript [Gross et al. 2013] and for extremely stimulating correspondence and conversations about these and other matters and Radu Laza for many helpful discussions.

References

[Bourbaki 1981] N. Bourbaki, *Groupes et algèbres de Lie*, Chapter 4, 5 et 6, Masson, Paris, 1981. MR 83g:17001 Zbl 0483.22001

[Coxeter 1973] H. S. M. Coxeter, *Regular polytopes*, 3rd ed., Dover, New York, 1973. MR 51 #6554 Zbl 0118.35902

[Demazure 1980a] M. Demazure, "Surfaces de Del Pezzo, II: Éclater n points dans P^2", pp. 23–35 in *Séminaire sur les singularités des surfaces* (Palaiseau, 1976–1977), edited by M. Demazure et al., Lecture Notes in Mathematics **777**, Springer, Berlin, 1980. MR 82d:14021 Zbl 0444.14024

[Demazure 1980b] M. Demazure, "Surfaces de Del Pezzo, III: Positions presque générales", pp. 36–49 in *Séminaire sur les singularités des surfaces* (Palaiseau, 1976–1977), edited by M. Demazure et al., Lecture Notes in Mathematics **777**, Springer, Berlin, 1980. MR 82d:14021 Zbl 0444.14024

[Demazure 1980c] M. Demazure, "Surfaces de Del Pezzo, IV: Systèmes anticanoniques", pp. 50–60 in *Séminaire sur les singularités des surfaces* (Palaiseau, 1976–1977), edited by M. Demazure et al., Lecture Notes in Mathematics **777**, Springer, Berlin, 1980. MR 82d:14021 Zbl 0444.14024

[Demazure 1980d] M. Demazure, "Surfaces de Del Pezzo, V: Modèles anticanoniques", pp. 61–69 in *Séminaire sur les singularités des surfaces* (Palaiseau, 1976–1977), edited by M. Demazure et al., Lecture Notes in Mathematics **777**, Springer, Berlin, 1980. MR 82d:14021 Zbl 0444.14024

[Du Val 1934] P. Du Val, "On isolated singularities of surfaces which do not affect the conditions of adjunction, II", *Proc. Camb. Philos. Soc.* **30**:4 (1934), 460–465. Zbl 0010.17603

[Du Val 1937] P. Du Val, "On the Kantor group of a set of points in a plane", *Proc. London Math. Soc.* (2) **42**:1 (1937), 18–51. MR 1577027 Zbl 0015.20302

[Friedman 1983] R. Friedman, "Linear systems on anticanonical pairs", pp. 162–171 in *The birational geometry of degenerations*, edited by R. Friedman and D. Morrison, Progress in Mathematics **29**, Birkhäuser, Boston, 1983. Appendix to a paper of N. I. Shepherd-Barron.

[Friedman 1984] R. Friedman, "The mixed Hodge structure of an open variety", 1984. Unpublished manuscript.

[Friedman and Miranda 1983] R. Friedman and R. Miranda, "Smoothing cusp singularities of small length", *Math. Ann.* **263**:2 (1983), 185–212. MR 85c:14003 Zbl 0488.14006

[Friedman and Morgan 1988] R. Friedman and J. W. Morgan, "On the diffeomorphism types of certain algebraic surfaces, I", *J. Differential Geom.* **27**:2 (1988), 297–369. MR 89d:57046 Zbl 0669.57016

[Friedman and Scattone 1986] R. Friedman and F. Scattone, "Type III degenerations of $K3$ surfaces", *Invent. Math.* **83**:1 (1986), 1–39. MR 87k:14044 Zbl 0613.14030

[Gross et al. 2013] M. Gross, P. Hacking, and S. Keel, "Moduli of surfaces with an anti-canonical cycle", preprint, 2013. arXiv 1211.6367

[Looijenga 1980] E. Looijenga, "Invariant theory for generalized root systems", *Invent. Math.* **61**:1 (1980), 1–32. MR 82f:17011 Zbl 0436.17005

[Looijenga 1981] E. Looijenga, "Rational surfaces with an anticanonical cycle", *Ann. of Math.* (2) **114**:2 (1981), 267–322. MR 83j:14030 Zbl 0509.14035

[Manin 1986] Y. I. Manin, *Cubic forms: algebra, geometry, arithmetic*, 2nd ed., North-Holland Mathematical Library **4**, North-Holland, Amsterdam, 1986. MR 87d:11037 Zbl 0582.14010

[Miranda and Persson 1986] R. Miranda and U. Persson, "On extremal rational elliptic surfaces", *Math. Z.* **193**:4 (1986), 537–558. MR 88a:14044 Zbl 0652.14003

Communicated by Ravi Vakil
Received 2012-08-02 Revised 2012-11-27 Accepted 2013-01-03

rf@math.columbia.edu *Department of Mathematics, Columbia University, 2990 Broadway, New York, NY, 10027, United States*

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1505

Commuting involutions of Lie algebras, commuting varieties, and simple Jordan algebras

Dmitri I. Panyushev

Let σ_1 and σ_2 be commuting involutions of a connected reductive algebraic group G with $\mathfrak{g} = \mathrm{Lie}(G)$. Let

$$\mathfrak{g} = \bigoplus_{i,j=0,1} \mathfrak{g}_{ij}$$

be the corresponding $\mathbb{Z}_2 \times \mathbb{Z}_2$-grading. If $\{\alpha, \beta, \gamma\} = \{01, 10, 11\}$, then $[\ ,\ ]$ maps $\mathfrak{g}_\alpha \times \mathfrak{g}_\beta$ into $\mathfrak{g}_\gamma$, and the zero fiber of this bracket is called a $\vec{\sigma}$-commuting variety. The commuting variety of $\mathfrak{g}$ and commuting varieties related to one involution are particular cases of this construction. We develop a general theory of such varieties and point out some cases, when they have especially good properties. If G/G^{σ_1} is a Hermitian symmetric space of tube type, then one can find three conjugate pairwise commuting involutions σ_1, σ_2, and $\sigma_3 = \sigma_1\sigma_2$. In this case, any $\vec{\sigma}$-commuting variety is isomorphic to the commuting variety of the simple Jordan algebra associated with σ_1. As an application, we show that if $\mathfrak{J}$ is the Jordan algebra of symmetric matrices, then the product map $\mathfrak{J} \times \mathfrak{J} \to \mathfrak{J}$ is equidimensional, while for all other simple Jordan algebras equidimensionality fails.

MSC2010: primary 14L30; secondary 17B08, 17B40, 17C20, 22E46.
Keywords: semisimple Lie algebra, commuting variety, Cartan subspace, quaternionic decomposition, nilpotent orbit, Jordan algebra.

Introduction

The ground field $\Bbbk$ is algebraically closed and $\operatorname{char}\Bbbk = 0$. Let G be a connected reductive algebraic group with $\operatorname{Lie}(G) = \mathfrak{g}$. Richardson [1979] proved that any pair of commuting elements of $\mathfrak{g}$ can be approximated by pairs of commuting semisimple elements. More precisely, if $\mathfrak{t} \subset \mathfrak{g}$ is a Cartan subalgebra (CSA), then

$$\{(x, y) \in \mathfrak{g} \times \mathfrak{g} \mid [x, y] = 0\} = \overline{G \cdot (\mathfrak{t} \times \mathfrak{t})}, \tag{0-1}$$

where a bar indicates the Zariski closure. The left-hand side is called the *commuting variety* of $\mathfrak{g}$, denoted $\mathfrak{C}(\mathfrak{g})$. That is, $\mathfrak{C}(\mathfrak{g})$ is the zero fiber of the multiplication map

$$\mathfrak{g} \times \mathfrak{g} \xrightarrow{[\,,\,]} \mathfrak{g}.$$

It follows from (0-1) that $\mathfrak{C}(\mathfrak{g})$ is irreducible and $\dim \mathfrak{C}(\mathfrak{g}) = \dim \mathfrak{g} + \operatorname{rk} \mathfrak{g}$. For arbitrary Lie algebras, for example, for Borel subalgebras of $\mathfrak{g}$, the commuting variety can be reducible [Vasconcelos 1994, p. 237].

There are several directions to take in generalizing Richardson's work.

First, for given subvarieties $U, V \subset \mathfrak{g}$, one can consider the restriction of $[\ ,\ ]$ to $U \times V$ and study properties of $\mathfrak{C}(\mathfrak{g}) \cap (U \times V)$. For instance:

- Let σ be an involution of $\mathfrak{g}$ with the corresponding $\mathbb{Z}_2$-grading $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$. Taking $U = V = \mathfrak{g}_1$ yields the commuting variety $\mathfrak{C}(\mathfrak{g}_1) := \mathfrak{C}(\mathfrak{g}) \cap (\mathfrak{g}_1 \times \mathfrak{g}_1)$, which was considered first in [Panyushev 1994b]. Here the structure of $\mathfrak{C}(\mathfrak{g}_1)$ heavily depends on σ. If $\mathfrak{g}_1$ contains a CSA of $\mathfrak{g}$, then $\mathfrak{C}(\mathfrak{g}_1)$ is an irreducible normal complete intersection [Panyushev 1994b]. At the other extreme, if the symmetric space G/G_0 is of rank 1, then $\mathfrak{C}(\mathfrak{g}_1)$ is often reducible. In [Panyushev and Yakimova 2007], the question of irreducibility of $\mathfrak{C}(\mathfrak{g}_1)$ is resolved for all but three involutions of simple Lie algebras, and the remaining cases are settled in [Bulois 2011]. It seems, however, that there is no simple rule to distinguish the involutions for which $\mathfrak{C}(\mathfrak{g}_1)$ is irreducible.
- Another natural possibility is to take $U = V = \mathcal{N}$, where $\mathcal{N}$ is the set of nilpotent elements of $\mathfrak{g}$. This leads to the *nilpotent commuting variety* of $\mathfrak{g}$, $\mathfrak{C}(\mathcal{N})$, which is often reducible. However, $\mathfrak{C}(\mathcal{N})$ is equidimensional, $\dim \mathfrak{C}(\mathcal{N}) = \dim \mathfrak{g}$, and the structure of irreducible components is well understood [Premet 2003].
- An interesting situation with $U \neq V$ occurs if $\mathfrak{g} = \bigoplus_{i \in \mathbb{Z}} \mathfrak{g}(i)$ is $\mathbb{Z}$-graded, $U = \mathfrak{g}(i)$, and $V = \mathfrak{g}(-i)$, see [Panyushev 1999, §3].

Second, one may look at commuting varieties related to other types of algebras. If $\mathcal{A}$ is any algebra, then $\mathfrak{C}(\mathcal{A})$ is defined to be the zero fiber of the multiplication map $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$. It is a natural task to study the commuting variety of a simple Jordan algebra. As far as I know, this problem has not been addressed before.

In this article, we elaborate on both directions outlined above. We study certain "commuting varieties" associated with $\mathbb{Z}_2 \times \mathbb{Z}_2$-gradings of $\mathfrak{g}$ (the first direction). It turns out that, for some gradings, these new commuting varieties are isomorphic to the commuting variety of simple Jordan algebras (the second direction). To describe our results more precisely, we need some notation. Let σ_1 and σ_2 be different commuting involutions of a connected reductive algebraic group G. This yields a $\mathbb{Z}_2 \times \mathbb{Z}_2$-grading of $\mathfrak{g}$:

$$\mathfrak{g} = \bigoplus_{i,j=0,1} \mathfrak{g}_{ij}, \text{ where } \mathfrak{g}_{ij} = \{x \in \mathfrak{g} \mid \sigma_1(x) = (-1)^i x \text{ and } \sigma_2(x) = (-1)^j x\}. \quad (0\text{-}2)$$

Then σ_1, σ_2, and $\sigma_3 = \sigma_1\sigma_2$ are pairwise commuting involutions, and following [Vergne 1995] we say that (0-2) is a *quaternionic decomposition* of $\mathfrak{g}$. For, if (α, β, γ) is any permutation of the set of indices $\{01, 10, 11\}$, then $[\mathfrak{g}_{00}, \mathfrak{g}_\alpha] \subset \mathfrak{g}_\alpha$ and $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subset \mathfrak{g}_\gamma$. The conjugacy classes of pairs of commuting involutions are classified, see [Kollross 2009] and references therein. Therefore, it is not difficult to write down explicitly all the quaternionic decompositions of simple Lie algebras. This article is a continuation of [Panyushev 2013], where we developed some theory on Cartan subspaces related to (0-2) and studied invariants of degenerations of isotropy representations involved.

Set $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, and let G_{00} denote the connected subgroup of G with Lie algebra $\mathfrak{g}_{00}$. A *$\vec{\sigma}$-commuting variety* is the zero fiber of the bracket $[\ ,\ ] : \mathfrak{g}_\alpha \times \mathfrak{g}_\beta \to \mathfrak{g}_\gamma$. Associated with (0-2), one has three essentially different such varieties that are parameterized by the choice of $\gamma \in \{01, 10, 11\}$. All these mappings are G_{00}-equivariant, and all $\vec{\sigma}$-commuting varieties are G_{00}-varieties. The above-mentioned varieties $\mathfrak{C}(\mathfrak{g}_1)$ can be obtained as a special case of this construction, see Example 3.1. We usually stick to one particular choice of the commutator, $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}$, and try to realize what assumptions on $\vec{\sigma}$ imply good properties of $\mathfrak{C} := \varphi^{-1}(0)$ and other fibers of φ. Clearly, φ can be regarded as a quadratic map from $\mathfrak{g}_{1\star} := \mathfrak{g}_{10} \oplus \mathfrak{g}_{11}$ to $\mathfrak{g}_{01}$. Let $\mathfrak{c}_{1\star}$ be a Cartan subspace (CSS) in $\mathfrak{g}_{1\star}$. Say that $\mathfrak{c}_{1\star}$ is *homogeneous* if it is σ_2-stable (or, equivalently, σ_3-stable), that is, if $\mathfrak{c}_{1\star} = \mathfrak{a}_{10} \oplus \mathfrak{a}_{11}$ with $\mathfrak{a}_{1j} \subset \mathfrak{g}_{1j}$. We prove:

- If $\mathfrak{c}_{1\star}$ is a homogeneous CSS, then the closure of $G_{00}{\cdot}\mathfrak{c}_{1\star}$ is an irreducible component of $\mathfrak{C}$ (Theorem 3.4). (Such irreducible components are said to be *standard*). However, there can be several standard components, of different dimensions, and there can also exist some "nonstandard" irreducible components.
- All homogeneous CSS in $\mathfrak{g}_{1\star}$ are G_{00}-conjugate (that is, $\mathfrak{C}$ has only one standard component) if and only if $\dim \mathfrak{c}_{1\star} = \dim \mathfrak{c}_{10} + \dim \mathfrak{c}_{11}$, where $\mathfrak{c}_{1j}$ are CSS in $\mathfrak{g}_{1j}$ (Theorem 3.7).

- The commutator map φ is dominant if and only if there exist $x \in \mathfrak{g}_{10}$ and $y \in \mathfrak{g}_{11}$ such that $\mathfrak{z}_{\mathfrak{g}}(x)_{01} \cap \mathfrak{z}_{\mathfrak{g}}(y)_{01} = \{0\}$.

However, one cannot expect really good properties for φ and $\mathfrak{E}$ without extra assumptions. One natural assumption is that some of involutions in $\vec{\sigma}$ are conjugate. Another possibility is that some of the σ_i possess prescribed properties. Our more specific results are:

(1) If σ_1 and σ_2 are conjugate, then φ is surjective and $\dim \varphi^{-1}(\xi) \geqslant \dim \mathfrak{g}_{11}$ for all $\xi \in \mathfrak{g}_{01}$ (Proposition 3.8). We also provide a method for detecting subvarieties of $\mathfrak{E}$ whose dimension is larger than $\dim \mathfrak{g}_{11}$. This exploits certain restricted root systems related to decomposition (0-2), see Section 5.

(2) If σ_1 and σ_2 are involutions of maximal rank (hence they are conjugate), then φ is surjective and equidimensional, each irreducible component of $\mathfrak{E}$ is standard, and the scheme $\varphi^{-1}(0)$ is a reduced complete intersection (Theorem 4.1).

(3) Let $\mathfrak{g}$ be simple and σ a Hermitian involution (that is, $\mathfrak{g}^{\sigma}$ is not semisimple). If the Hermitian symmetric space G/G^{σ} is of tube type, then there exists a commuting triple $\vec{\sigma}$ such that each σ_i is conjugate to σ, and in this case $\mathfrak{E}$ is isomorphic to the commuting variety of the corresponding simple Jordan algebra, see Section 6.

(4) The relationship with $\vec{\sigma}$-commuting varieties implies that the multiplication map $\mathcal{J} \times \mathcal{J} \xrightarrow{\circ} \mathcal{J}$ is equidimensional if and only if $\mathcal{J}$ is the Jordan algebra of symmetric matrices. The commuting variety of a simple Jordan algebra $\mathcal{J}$ is reducible, since $\mathcal{J} \times \{0\}$ and $\{0\} \times \mathcal{J}$ are always irreducible components, and there are certainly some other components.

(5) The results stated in (2) rely on an interesting property of $\mathbb{Z}_2$-gradings. For any $e \in \mathfrak{g}_0$, its centralizer in $\mathfrak{g}$ is also $\mathbb{Z}_2$-graded: $\mathfrak{g}^e = \mathfrak{g}_0^e \oplus \mathfrak{g}_1^e$. Then we prove that

$$\dim \mathfrak{g}_0^e + \mathrm{rk}\, \mathfrak{g} \geqslant \dim \mathfrak{g}_1^e$$

and the equality occurs only if $e = 0$ and σ is of maximal rank. However, the proof of this inequality (Theorem 4.4) is not quite uniform, and a better proof is welcome! The required case-by-case calculations are lengthy and tedious, so not all of them are actually presented, and a part is placed in the Appendix. We hope that an a priori proof of this inequality might be related to a geometric property of centralizers of nilpotent elements in $\mathfrak{g}_0$, see Conjecture 4.6.

– Throughout, G is a connected reductive algebraic group and $\mathfrak{g} = \mathsf{Lie}(G)$. Then $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{a})$ is the centralizer of a subspace $\mathfrak{a} \subset \mathfrak{g}$, and the centralizer of $x \in \mathfrak{g}$ is denoted by $\mathfrak{z}_{\mathfrak{g}}(x)$ or $\mathfrak{g}^x$.

– $\mathsf{R}(\lambda)$ is a simple finite-dimensional G-module with highest weight λ.

– Algebraic groups are denoted by capital Roman letters and their Lie algebras are denoted by the corresponding lower-case Gothic letters.

1. Preliminaries on involutions and commuting varieties

The set of all involutions of $\mathfrak{g}$ is denoted by $\mathsf{Inv}(\mathfrak{g})$. The group of inner automorphisms $\mathsf{Int}(G) \simeq G/Z(G)$ acts on $\mathsf{Inv}(\mathfrak{g})$ by conjugation. Two involutions are said to be *conjugate* if they lie in the same $\mathsf{Int}(G)$-orbit. If $\sigma \in \mathsf{Inv}(\mathfrak{g})$, then $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$ is the corresponding $\mathbb{Z}_2$-grading of $\mathfrak{g}$, where $\mathfrak{g}_i = \{x \in \mathfrak{g} \mid \sigma(x) = (-1)^i x\}$. We also say that $(\mathfrak{g}, \mathfrak{g}_0)$ is a *symmetric pair*. Whenever we wish to stress that $\mathfrak{g}_0$ and $\mathfrak{g}_1$ are determined by σ, we write $\mathfrak{g}^\sigma$ and $\mathfrak{g}_1^{(\sigma)}$ for them. We assume that σ is induced by an involution of G, which is denoted by the same letter. The connected subgroup of G with Lie algebra $\mathfrak{g}_0$ is denoted by G_0. Hence G_0 is the identity component of $G^\sigma = \{g \in G \mid \sigma(g) = g\}$. The representation of G_0 in $\mathfrak{g}_1$ is the *isotropy representation* of the symmetric space G/G_0.

We freely use the invariant-theoretic results on the G_0-action on $\mathfrak{g}_1$ obtained in [Kostant and Rallis 1971]. A *Cartan subspace* (CSS) is a maximal subspace of $\mathfrak{g}_1$ consisting of pairwise commuting semisimple elements. The Cartan subspaces are characterized by the following property:

> *Suppose that a subspace $\mathfrak{a} \subset \mathfrak{g}_1$ consists of pairwise commuting semisimple elements. Then $\mathfrak{a}$ is a CSS if and only if $\mathfrak{z}_\mathfrak{g}(\mathfrak{a}) \cap \mathfrak{g}_1 = \mathfrak{a}$* [Kostant and Rallis 1971, Chapter I]. (1-1)

An element $x \in \mathfrak{g}_1$ is called *G_0-regular* if the orbit $G_0{\cdot}x$ is of maximal dimension. Let $\mathfrak{c}$ be a CSS of $\mathfrak{g}_1$. Below, we summarize some basic properties of the Cartan subspaces and isotropy representations:

- All CSS of $\mathfrak{g}_1$ are G_0-conjugate and $G_0{\cdot}\mathfrak{c}$ is dense in $\mathfrak{g}_1$.
- Every semisimple element of $\mathfrak{g}_1$ is G_0-conjugate to an element of $\mathfrak{c}$.
- A semisimple element $x \in \mathfrak{g}_1$ is G_0-regular $\iff$ $\mathfrak{z}_\mathfrak{g}(x) \cap \mathfrak{g}_1$ is a CSS.
- The orbit $G_0{\cdot}x$ is closed if and only if x is semisimple.
- The closure of $G_0{\cdot}x$ contains the origin if and only if x is nilpotent.
- The number of nilpotent G_0-orbits in $\mathfrak{g}_1$ is finite.

We say that $\sigma \in \mathsf{Inv}(\mathfrak{g})$ is *of maximal rank* if $\mathfrak{g}_1$ contains a Cartan subalgebra of $\mathfrak{g}$.

The following facts are well known:

(1) $\dim \mathfrak{g}_1 - \dim \mathfrak{g}_0 \leqslant \mathsf{rk}\, \mathfrak{g}$ for any σ, and the equality holds if and only if σ is of maximal rank.

(2) All involutions of maximal rank are conjugate.

(3) The involutions of maximal rank are inner *if and only if* all exponents of $\mathfrak{g}$ are odd.

Lemma 1.1 [Kostant and Rallis 1971, Proposition 5]. *For any $x \in \mathfrak{g}_1$, one has* $\dim \mathfrak{g}_0 - \dim \mathfrak{g}_0^x = \dim \mathfrak{g}_1 - \dim \mathfrak{g}_1^x$. *Equivalently,* $\dim G{\cdot}x = 2 \dim G_0{\cdot}x$ *for all* $x \in \mathfrak{g}_1$.

Consequently, if σ is of maximal rank, then

$$\dim \mathfrak{g}_1^x = \dim \mathfrak{g}_0^x + \mathrm{rk}\, \mathfrak{g}. \tag{1-2}$$

The property of having maximal rank is inheritable in the following sense.

Lemma 1.2. *Let σ be of maximal rank and $x \in \mathfrak{g}_1$ semisimple. Then the restriction of σ to $\mathfrak{g}^x$ and $[\mathfrak{g}^x, \mathfrak{g}^x]$ is also of maximal rank.*

The *commuting variety* associated with σ is

$$\mathfrak{C}(\mathfrak{g}_1) = \{(x, y) \in \mathfrak{g}_1 \times \mathfrak{g}_1 \mid [x, y] = 0\}. \tag{1-3}$$

That is, $\mathfrak{C}(\mathfrak{g}_1)$ is the zero fiber of the commutator map $[\ ,\ ]_1 : \mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathfrak{g}_0$. The following is known:

- $\overline{G_0{\cdot}(\mathfrak{c} \times \mathfrak{c})}$ is always an irreducible component of $\mathfrak{C}(\mathfrak{g}_1)$ [Panyushev 1994b, Proposition 3.7].
- If σ is of maximal rank, then $\overline{G_0{\cdot}(\mathfrak{c} \times \mathfrak{c})} = \mathfrak{C}(\mathfrak{g}_1)$ and $\mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathfrak{g}_0$ is equidimensional [Panyushev 1994b, Theorem 3.2]; moreover, all the fibers of $[\ ,\ ]_1$ are irreducible and normal [Panyushev 1994b, Corollary 4.4].
- $\mathfrak{C}(\mathfrak{g}_1)$ can be reducible [Panyushev 1994b, Example 3.5].

Example 1.3. Suppose that $\tilde{\mathfrak{g}} = \mathfrak{g} \oplus \mathfrak{g}$ and $\sigma(x, y) = (y, x)$. Then $\tilde{\mathfrak{g}}_0 = \Delta(\mathfrak{g})$ and $\tilde{\mathfrak{g}}_1 = \{(x, -x) \mid x \in \mathfrak{g}\}$. Here the commutator $\tilde{\mathfrak{g}}_1 \times \tilde{\mathfrak{g}}_1 \to \tilde{\mathfrak{g}}_0$ coincides with the usual commutator $\mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ and $\mathfrak{C}(\tilde{\mathfrak{g}}_1)$ is isomorphic to the usual commuting variety of a semisimple Lie algebra $\mathfrak{g}$. By a result of Richardson [1979], $\mathfrak{C}(\mathfrak{g})$ is irreducible and $\dim \mathfrak{C}(\mathfrak{g}) = \dim \mathfrak{g} + \mathrm{rk}\, \mathfrak{g}$.

A torus S of G is called *σ-anisotropic* if $\sigma(s) = s^{-1}$ for all $s \in S$. All maximal σ-anisotropic tori are G_0-conjugate, and if $C \subset G$ is a maximal σ-anisotropic torus, then $\mathsf{Lie}(C)$ is a CSS in $\mathfrak{g}_1$. Recall that a *restricted root* of C is any nontrivial weight in the decomposition of $\mathfrak{g}$ into the sum of weight spaces of C. Write $\Psi^C(G/G_0)$ or just $\Psi(G/G_0)$ for the set of all restricted roots. Then

$$\mathfrak{g} = \mathfrak{g}^C \oplus \Big(\bigoplus_{\gamma \in \Psi(G/G_0)} \mathfrak{g}_\gamma \Big). \tag{1-4}$$

We use additive notation for the operation in $\mathfrak{X}(C)$, the character group of C, and regard $\Psi(G/G_0)$ as a subset of the vector space $\mathfrak{X}(C) \otimes_{\mathbb{Z}} \mathbb{R}$. The set $\Psi(G/G_0)$ satisfies the usual axioms of finite root systems [Helgason 1978]. The notable difference from the structure theory of split semisimple Lie algebras is that the

root system $\Psi(G/G_0)$ can be nonreduced and that multiplicities $m_\gamma = \dim \mathfrak{g}_\gamma$ ($\gamma \in \Psi(G/G_0)$) can be greater than 1.

For all involutions of simple Lie algebras, the restricted root systems and the respective multiplicities are known, see [Helgason 1978, Chapter X, Table VI].

2. Commuting involutions and quaternionic decompositions

Let σ_1 and σ_2 be different commuting involutions of $\mathfrak{g}$. Then the corresponding $\mathbb{Z}_2 \times \mathbb{Z}_2$-grading of $\mathfrak{g}$ is

$$\mathfrak{g} = \bigoplus_{i,j=0,1} \mathfrak{g}_{ij}, \text{ where } \mathfrak{g}_{ij} = \{x \in \mathfrak{g} \mid \sigma_1(x) = (-1)^i x \text{ and } \sigma_2(x) = (-1)^j x\}. \quad (2\text{-}1)$$

We also say that it is a *quaternionic decomposition* of $\mathfrak{g}$ (determined by σ_1 and σ_2). Set $\sigma_3 := \sigma_1\sigma_2$ and $\vec{\boldsymbol{\sigma}} = (\sigma_1, \sigma_2, \sigma_3)$. The pairwise commuting involutions σ_1, σ_2, and σ_3 are said to be *big*. The induced involutions on the fixed-point subalgebras $\mathfrak{g}^{\sigma_1}$, $\mathfrak{g}^{\sigma_2}$, and $\mathfrak{g}^{\sigma_3}$ are said to be *little*. The same terminology applies to the corresponding $\mathbb{Z}_2$-gradings, isotropy representations, and CSS. Thus, associated with (2-1), one has three big and three little $\mathbb{Z}_2$-gradings. It is convenient for us to organize the summands of (2-1) in a 2×2 "matrix":

$$\mathfrak{g} = \begin{array}{c|c} \mathfrak{g}_{00} & \mathfrak{g}_{01} \\ \hline \mathfrak{g}_{10} & \mathfrak{g}_{11} \end{array} \quad \begin{matrix} \\ \sigma_1 \end{matrix}. \qquad (2\text{-}2)$$

$$\sigma_2$$

Here the horizontal (resp. vertical) dotted line separates the eigenspaces of σ_1 (resp. σ_2), whereas two diagonals of this matrix represent the eigenspaces of σ_3. Hence the first row, first column, and main diagonal represent the three little $\mathbb{Z}_2$-gradings (of $\mathfrak{g}^{\sigma_1}$, $\mathfrak{g}^{\sigma_2}$, and $\mathfrak{g}^{\sigma_3}$, respectively).

We repeatedly use the following notation for the eigenspaces of σ_1 and σ_2:

$$\mathfrak{g}^{\sigma_1} = \mathfrak{g}_{0\star} := \mathfrak{g}_{00} \oplus \mathfrak{g}_{01}, \ \mathfrak{g}_{1\star} := \mathfrak{g}_{10} \oplus \mathfrak{g}_{11}, \quad \mathfrak{g}^{\sigma_2} = \mathfrak{g}_{\star 0} := \mathfrak{g}_{00} \oplus \mathfrak{g}_{10}, \ \mathfrak{g}_{\star 1} := \mathfrak{g}_{01} \oplus \mathfrak{g}_{11}.$$

Likewise, $G_{0\star}$ (resp. $G_{\star 0}$) is the connected subgroup of G corresponding to $\mathfrak{g}_{0\star}$ (resp. $\mathfrak{g}_{\star 0}$), G_{00} is the connected subgroup of G corresponding to $\mathfrak{g}_{00}$, etc. If $\mathfrak{q}$ is a $\vec{\boldsymbol{\sigma}}$-stable subalgebra of $\mathfrak{g}$, then $\mathfrak{q} = \bigoplus_{i,j} \mathfrak{q}_{ij}$ is the induced quaternionic decomposition of $\mathfrak{q}$, and Q and Q_{00} are the corresponding connected subgroups.

Following [Vinberg 2005, 0.3], we say that a triple $\{\sigma_1, \sigma_2, \sigma_3\} \subset \mathsf{Inv}(\mathfrak{g})$ is a *triad* if all three involutions are conjugate and $\sigma_1\sigma_2 = \sigma_3$. A complete classification of triads is obtained in [Vinberg 2005, §3]. The triads lead to the "most symmetric" quaternionic decompositions. In [Panyushev 2013], we considered less restrictive conditions on the σ_i. We say that $\{\sigma_1, \sigma_2\} \subset \mathsf{Inv}(\mathfrak{g})$ is a *dyad* if σ_1 and σ_2 are conjugate and $\sigma_1\sigma_2 = \sigma_2\sigma_1$ (no conditions on σ_3!).

The product of two conjugate involutions (not necessarily commuting) is always an inner automorphism of $\mathfrak{g}$. For, if $\sigma_2 = \mathrm{Int}(g)\cdot\sigma_1\cdot\mathrm{Int}(g^{-1})$, then $\sigma_1\sigma_2 = \mathrm{Int}(\sigma_1(g)g^{-1})$. Therefore, any triad consists of inner involutions. (But not every inner involution gives rise to a triad!) Any involution can be a member of a dyad [Panyushev 2013, Proposition 2.4]. But the third involution, σ_3, is then necessarily inner.

Proposition 2.1 (see [Panyushev 2013, Proposition 2.2(1)]). *Suppose that $\mu \in \mathsf{Inv}(\mathfrak{g})$ is inner. Then there are commuting involutions of maximal rank, σ_1 and σ_2, such that $\mu = \sigma_1\sigma_2$. Moreover, σ_1 and σ_2 induce an involution of maximal rank of $\mathfrak{g}^{\mu}$.*

For $(ij) \neq (00)$, let $\mathfrak{c}_{ij}$ be a CSS of $\mathfrak{g}_{ij}$; that is, a little CSS related to the little $\mathbb{Z}_2$-grading $\mathfrak{g}_{00} \oplus \mathfrak{g}_{ij}$. There are also big CSS in the (-1)-eigenspaces of three big involutions:

$$\mathfrak{c}_{1\star} \subset \mathfrak{g}_{1\star}, \quad \mathfrak{c}_{\star 1} \subset \mathfrak{g}_{\star 1}, \quad \mathfrak{c}_{\star,1-\star} \subset \mathfrak{g}_{\star,1-\star} := \mathfrak{g}_{01} \oplus \mathfrak{g}_{10}.$$

Each little CSS can be included in two big CSS. For example, because $\mathfrak{g}_{10} \subset \mathfrak{g}_{1\star}$ and $\mathfrak{g}_{10} \subset \mathfrak{g}_{\star,1-\star}$, one can choose Cartan subspaces $\mathfrak{c}_{1\star}$ and $\mathfrak{c}_{\star,1-\star}$ such that $\mathfrak{c}_{10} \subset \mathfrak{c}_{1\star}$ and $\mathfrak{c}_{10} \subset \mathfrak{c}_{\star,1-\star}$. If at least one equality occurs among all such inclusions, then this will be referred to as a *coincidence* of CSS (for a given quaternionic decomposition).

In [Panyushev 2013], we obtained two sufficient conditions for a coincidence of CSS:

Theorem 2.2 (see [Panyushev 2013, Theorems 3.3 and 3.7]).

(1) *Suppose that σ_1 is of maximal rank. Then*
- *any little CSS $\mathfrak{c}_{11} \subset \mathfrak{g}_{11}$ is also a CSS in $\mathfrak{g}_{\star 1}$, that is, for σ_2, and*
- *any little CSS $\mathfrak{c}_{10} \subset \mathfrak{g}_{10}$ is also a CSS in $\mathfrak{g}_{10} \oplus \mathfrak{g}_{01}$, that is, for σ_3.*

(2) *Suppose that $\{\sigma_1, \sigma_2\}$ is a dyad. Then any little CSS $\mathfrak{c}_{11} \subset \mathfrak{g}_{11}$ is also a CSS in $\mathfrak{g}_{1\star}$ or $\mathfrak{g}_{\star 1}$, that is, for σ_1 or σ_2.*

The coincidences of CSS in Theorem 2.2(2) can formally be expressed as $\mathfrak{c}_{11} = \mathfrak{c}_{1\star}$ or $\mathfrak{c}_{11} = \mathfrak{c}_{\star 1}$, and likewise in all other possible cases. In view of (1-1), any coincidence of CSS can be restated as certain property of the little CSS in question. For instance, the first coincidence in Theorem 2.2(1) means that if $x \in \mathfrak{g}_{11}$ is a generic semisimple element (that is, x belong to a unique little CSS), then $\mathfrak{z}_{\mathfrak{g}}(x)_{\star 1} = \mathfrak{z}_{\mathfrak{g}}(x)_{11} = \mathfrak{c}_{11}$, and hence $\mathfrak{z}_{\mathfrak{g}}(x)_{01} = 0$.

3. Commuting varieties and homogeneous Cartan subspaces

Consider a quaternionic decomposition (2-2). For any permutation (α, β, γ) of the set $\{01, 10, 11\}$, there is the commutator mapping $\varphi^{\gamma}_{\alpha,\beta} : \mathfrak{g}_{\alpha} \times \mathfrak{g}_{\beta} \to \mathfrak{g}_{\gamma}$. Clearly,

$\varphi^{\gamma}_{\alpha,\beta}$ is G_{00}-equivariant. As our main interest is in fibers of this mapping, we do not distinguish $\varphi^{\gamma}_{\alpha,\beta}$ and $\varphi^{\gamma}_{\beta,\alpha}$. We concentrate on the following problems:

- When is $\varphi^{\gamma}_{\alpha,\beta}$ dominant?
- What is the dimension of $(\varphi^{\gamma}_{\alpha,\beta})^{-1}(0)$?
- How to describe the irreducible components of $(\varphi^{\gamma}_{\alpha,\beta})^{-1}(0)$?
- When is $\varphi^{\gamma}_{\alpha,\beta}$ equidimensional?

The variety $\mathfrak{E}^{\gamma}_{\alpha,\beta} = (\varphi^{\gamma}_{\alpha,\beta})^{-1}(0)$ is said to be a $\vec{\sigma}$-*commuting variety*. For general quaternionic decompositions, one has three such varieties, and their properties can be rather different. We mainly restrict ourselves to considering the test case:

$$\varphi = \varphi^{01}_{10,11} : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}. \tag{3-1}$$

and also write $\mathfrak{E}$ in place of $\mathfrak{E}^{01}_{10,11}$. Note that we can regard φ as a quadratic map from $\mathfrak{g}_{1\star}$ to $\mathfrak{g}_{01}$, and $\mathfrak{E}$ as subvariety of $\mathfrak{g}_{1\star}$. The following example shows that the commuting variety in (1-3) is a particular case of this construction.

Example 3.1. Let $\mathfrak{g}$ be a reductive Lie algebra and σ an involution of $\mathfrak{g}$ with the corresponding $\mathbb{Z}_2$-grading $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$. Set $\tilde{\mathfrak{g}} = \mathfrak{g} \oplus \mathfrak{g}$ and define three involutions of $\tilde{\mathfrak{g}}$ as follows:

$$\sigma_1(x_1, x_2) = (\sigma(x_1), \sigma(x_2)), \quad \sigma_2(x_1, x_2) = (x_2, x_1), \quad \sigma_3 = \sigma_1\sigma_2.$$

Then $\tilde{\mathfrak{g}}^{\sigma_1} = \mathfrak{g}_0 \oplus \mathfrak{g}_0$; $\tilde{\mathfrak{g}}^{\sigma_2} = \Delta(\mathfrak{g})$, the diagonal in $\mathfrak{g} \oplus \mathfrak{g}$; and $\tilde{\mathfrak{g}}^{\sigma_3} = \{(x, \sigma(x)) \mid x \in \mathfrak{g}\}$. Set $\Delta_-(M) := \{(m, -m) \mid m \in M\}$ for any subspace $M \subset \mathfrak{g}$. Then the corresponding quaternionic decomposition is

$$\tilde{\mathfrak{g}} = \begin{array}{c|c} \Delta(\mathfrak{g}_0) & \Delta_-(\mathfrak{g}_0) \\ \hline \Delta(\mathfrak{g}_1) & \Delta_-(\mathfrak{g}_1) \end{array} \quad \begin{array}{l} \\ \sigma_1. \end{array}$$

σ_2

Upon the obvious identifications $\Delta(\mathfrak{g}_1) \simeq \Delta_-(\mathfrak{g}_1) \simeq \mathfrak{g}_1$, etc., our test commutator map $\tilde{\mathfrak{g}}_{10} \times \tilde{\mathfrak{g}}_{11} \to \tilde{\mathfrak{g}}_{01}$ becomes the commutator $\mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathfrak{g}_0$ associated with $\sigma \in \mathsf{Inv}(\mathfrak{g})$; whereas two other commutator maps are identified with the bracket $\mathfrak{g}_0 \times \mathfrak{g}_1 \to \mathfrak{g}_1$. Therefore, the concept of a $\vec{\sigma}$-commuting variety provides a uniform setting for studying the fibers of both $\mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathfrak{g}_0$ and $\mathfrak{g}_0 \times \mathfrak{g}_1 \to \mathfrak{g}_1$.

Lemma 3.2. *The commutator map* (3-1) *is dominant if and only if there exist* $x \in \mathfrak{g}_{10}$ *and* $y \in \mathfrak{g}_{11}$ *such that* $\mathfrak{z}_{\mathfrak{g}}(x)_{01} \cap \mathfrak{z}_{\mathfrak{g}}(y)_{01} = \{0\}$.

Proof. A morphism of irreducible varieties is dominant if and only if its differential at some point is onto. As φ is bilinear, an easy computation shows that $d\varphi_{(x,y)}(\xi, \eta) = [x, \eta] + [\xi, y]$, $\xi \in \mathfrak{g}_{10}$, $\eta \in \mathfrak{g}_{11}$. Hence $\operatorname{Im} d\varphi_{(x,y)} = [\mathfrak{g}_{11}, x] + [\mathfrak{g}_{10}, y]$, and taking

the orthogonal complement with respect to the restriction of the Killing form to $\mathfrak{g}_{01}$ yields $(\operatorname{Im} d\varphi_{(x,y)})^{\perp} = \mathfrak{z}_{\mathfrak{g}}(x)_{01} \cap \mathfrak{z}_{\mathfrak{g}}(y)_{01}$. □

As we see below, certain CSS in $\mathfrak{g}_{1\star}$ play an important role in describing irreducible components of $\mathfrak{E}$.

Definition 1. A big CSS $\mathfrak{c}_{1\star} \subset \mathfrak{g}_{1\star}$ is said to be *homogeneous* if it is σ_2-stable (or, equivalently, σ_3-stable). In other words, if one has $\mathfrak{c}_{1\star} = \mathfrak{a}_{10} \oplus \mathfrak{a}_{11}$ with $\mathfrak{a}_{1j} \subset \mathfrak{g}_{1j}$.

Remark. A coincidence of CSS means that there is a homogeneous CSS of special form. For instance, if $\mathfrak{c}_{11} = \mathfrak{c}_{1\star}$, then $\mathfrak{c}_{11}$ is a homogeneous CSS in $\mathfrak{g}_{1\star}$, with trivial $\mathfrak{g}_{10}$-component.

Lemma 3.3. (1) *Homogeneous CSS always exist.*

(2) *Moreover, if $x \in \mathfrak{g}_{10}$ and $y \in \mathfrak{g}_{11}$ are commuting semisimple elements, then there exists a homogeneous CSS in $\mathfrak{g}_{1\star}$ containing both of them.*

Proof. (1) Take a little CSS $\mathfrak{c}_{10}$ and consider the $\vec{\sigma}$-stable reductive subalgebra $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{10})$. If $\tilde{\mathfrak{a}}_{11}$ is a little CSS in $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{10})_{11}$, then $\mathfrak{c}_{10} \oplus \tilde{\mathfrak{a}}_{11}$ is a homogeneous CSS in $\mathfrak{g}_{1\star}$.

(2) Consider the $\vec{\sigma}$-stable reductive subalgebra $\mathfrak{l} = \mathfrak{z}_{\mathfrak{g}}(x) \cap \mathfrak{z}_{\mathfrak{g}}(y)$. By the previous part, there exists a homogeneous CSS in $\mathfrak{l}_{1\star}$, say $\tilde{\mathfrak{c}}_{1\star}$. Since x and y are central in $\mathfrak{l}$, we have $x, y \in \tilde{\mathfrak{c}}_{1\star}$. It is also clear that $\tilde{\mathfrak{c}}_{1\star}$ is a CSS in $\mathfrak{g}_{1\star}$. □

If $\mathfrak{c}_{1\star} = \mathfrak{a}_{10} \oplus \mathfrak{a}_{11}$ is a homogeneous CSS, then $[\mathfrak{a}_{01}, \mathfrak{a}_{11}] = 0$ and hence $\overline{G_{00}\cdot\mathfrak{c}_{1\star}} \subset \mathfrak{E}$. However, a stronger result is true.

Theorem 3.4. (i) *Let $\mathfrak{c}_{1\star}$ be a homogeneous CSS in $\mathfrak{g}_{1\star}$. Then $\overline{G_{00}\cdot\mathfrak{c}_{1\star}} \subset \mathfrak{E}$ is an irreducible component of $\mathfrak{E}$.*

(ii) *If two homogeneous CSS in $\mathfrak{g}_{1\star}$ are not G_{00}-conjugate, then the corresponding irreducible components are different.*

Proof. (i) The centralizer of $\mathfrak{c}_{1\star}$ is $\vec{\sigma}$-stable. Hence $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{1\star}) = \bigoplus_{i,j=0,1} \mathfrak{a}_{ij}$, and here $\mathfrak{c}_{1\star} = \mathfrak{a}_{10} \oplus \mathfrak{a}_{11}$. Recall that $\overline{G_{0\star}\cdot\mathfrak{c}_{1\star}} = \mathfrak{g}_{1\star}$. Therefore, $\dim \mathfrak{c}_{1\star} + \dim G_{0\star} - \dim \mathfrak{a}_{00} - \dim \mathfrak{a}_{01} = \dim \mathfrak{g}_{1\star}$. It follows that

$$\dim \overline{G_{00}\cdot\mathfrak{c}_{1\star}} = \dim \mathfrak{c}_{1\star} + \dim G_{00} - \dim \mathfrak{a}_{00} = \dim \mathfrak{g}_{1\star} - \dim \mathfrak{g}_{01} + \dim \mathfrak{a}_{01}. \quad (3\text{-}2)$$

On the other hand, let $x + y \in \mathfrak{c}_{1\star}$ ($x \in \mathfrak{g}_{10}$, $y \in \mathfrak{g}_{11}$). The proof of Lemma 3.2 shows that $\dim(\operatorname{Im} d\varphi_{(x,y)}) = \dim \mathfrak{g}_{01} - \dim(\mathfrak{z}_{\mathfrak{g}}(x)_{01} \cap \mathfrak{z}_{\mathfrak{g}}(y)_{01})$. Now, if $x + y \in \mathfrak{c}_{1\star}$ is generic, then $\mathfrak{z}_{\mathfrak{g}}(x) \cap \mathfrak{z}_{\mathfrak{g}}(y) = \mathfrak{z}_{\mathfrak{g}}(x + y) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{1\star})$. Hence $\dim(\operatorname{Im} d\varphi_{(x,y)}) = \dim \mathfrak{g}_{01} - \dim \mathfrak{a}_{01}$. This means that any irreducible component of $\mathfrak{E}$ containing (x, y) has dimension at most

$$\dim \mathfrak{g}_{1\star} - \dim(\operatorname{Im} d\varphi_{(x,y)}) = \dim \mathfrak{g}_{1\star} - \dim \mathfrak{g}_{01} + \dim \mathfrak{a}_{01}.$$

Comparing with (3-2) shows that $\overline{G_{00}\cdot\mathfrak{c}_{1\star}}$ is an irreducible component of $\mathfrak{E}$ containing (x, y), and (x, y) is a smooth point of $\overline{G_{00}\cdot\mathfrak{c}_{1\star}}$.

(ii) As we have just shown, if $x + y \in \mathfrak{c}_{1\star}$ is generic, then it belongs to a unique irreducible component of $\mathfrak{E}$ (and to a unique CSS in $\mathfrak{g}_{1\star}$). □

Claim 3.5. *The number of G_{00}-orbits of homogeneous CSS in $\mathfrak{g}_{1\star}$ is finite.*

First proof. Since the number of irreducible components is finite, this readily follows from Theorem 3.4. However, it can also be proved in a different way. As the second proof has its own merits, we provide it below.

Second proof. Recall that $G_{00} \subset G_{0\star}$ are connected reductive groups and *all* big CSS in $\mathfrak{g}_{1\star}$ form a single $G_{0\star}$-orbit. Let $\mathfrak{c}_{1\star}$ be a homogeneous CSS. Set

$$N = \{g \in G_{0\star} \mid g\cdot\mathfrak{c}_{1\star} = \mathfrak{c}_{1\star}\}, \qquad \mathcal{M} = \{g \in G_{0\star} \mid g\cdot\mathfrak{c}_{1\star} \text{ is homogeneous }\}.$$

Note that N is reductive, but not connected, since N is mapped onto the (finite) little Weyl group associated with $\mathfrak{c}_{1\star}$. If $g \in \mathcal{M}$, $s \in G_{00}$, and $z \in N$, then $sgz \in \mathcal{M}$. Therefore, $\mathcal{M}$ is a union of (G_{00}, N)-cosets, and our task is to prove that $G_{00}\backslash\mathcal{M}/N$ is finite.

If $g \in \mathcal{M}$, then $g\cdot\mathfrak{c}_{1\star} = \sigma_2(g)\mathfrak{c}_{1\star}$. Hence $g^{-1}\sigma_2(g) \in N$. Since $G_{00} \subset G^{\sigma_2}$, the map

$$\psi_{\mathcal{M}} : G_{00}\backslash\mathcal{M} \to N, \quad G_{00}g \mapsto g^{-1}\sigma_2(g),$$

is well defined. Note that N is σ_2-stable and the range of $\psi_{\mathcal{M}}$ belongs to the closed subset

$$\mathcal{Q} = \mathcal{Q}(N) = \{g \in N \mid \sigma_2(g) = g^{-1}\}.$$

The twisted N-action on N is defined by $z \star x = zx\sigma_2(z)^{-1}$. Obviously, $\mathcal{Q}$ is stable under the twisted action of N. Moreover, $\psi_{\mathcal{M}}(gz) = z^{-1}\psi_{\mathcal{M}}(g)\sigma_2(z)$. Hence $\mathrm{Im}(\varphi_{\mathcal{M}}) \subset \mathcal{Q}$ is the union of twisted N-orbits, and each twisted N-orbit gives rise to a G_{00}-orbit of homogeneous CSS. It follows from [Richardson 1982, §9] that $\mathcal{Q}$ is a finite union of twisted N-orbits, which is sufficient for our purpose. (See also the remark below.) □

Remark 3.6. Richardson's results on twisted orbits [Richardson 1982, §9], specifically Proposition 9.1, are stated for a *connected* reductive group G, whereas we apply them to the reductive nonconnected group N (in place of G). But his argument can easily be adjusted to cover the case of nonconnected reductive groups. That is, one can give a version of Richardson's Proposition 9.1 for nonconnected groups G.

Definition 2. For a homogeneous CSS $\mathfrak{c}_{1\star} \subset \mathfrak{g}_{1\star}$, the irreducible component $\overline{G_{00}\cdot\mathfrak{c}_{1\star}}$ of $\mathfrak{E}$ is said to be *standard*.

Since all big CSS in $\mathfrak{g}_{1\star}$ are $G_{0\star}$-conjugate, their centralizers in $\mathfrak{g}_{0\star}$ are essentially "the same". The centralizer in $\mathfrak{g}_{0\star}$ of a homogeneous CSS splits, and these splittings can be quite different. That is, $\dim \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{1\star})_{01}$ can be different for different homogeneous CSS, and this leads to a new phenomenon that standard irreducible components of $\mathfrak{E}$ may have different dimensions, see (3-2). Moreover, there can also be some "nonstandard" irreducible components of $\mathfrak{E}$ that contain no semisimple elements at all.

By Theorem 3.4, a necessary condition for $\mathfrak{E}$ to be irreducible is that all homogeneous CSS in $\mathfrak{g}_{1\star}$ are G_{00}-conjugate, that is, there is only one standard component. If $\mathfrak{c}_{1\star} = \mathfrak{a}_{10} \oplus \mathfrak{a}_{11}$ is a homogeneous CSS with $\dim \mathfrak{a}_{1i} = d_i$, then (d_0, d_1) is called the *dimension vector*. Obviously, two homogeneous CSS with different dimension vectors are not G_{00}-conjugate.

Theorem 3.7. (1) *If* $\mathfrak{c}_{1\star} = \mathfrak{a}_{10} \oplus \mathfrak{a}_{11}$ *is a homogeneous CSS with dimension vector* (d_0, d_1), *then* $d_0 \leqslant \dim \mathfrak{c}_{10}$ *and* $d_1 \leqslant \dim \mathfrak{c}_{11}$; *hence* $\dim \mathfrak{c}_{1\star} \leqslant \dim \mathfrak{c}_{10} + \dim \mathfrak{c}_{11}$.

(2) *All homogeneous CSS in* $\mathfrak{g}_{1\star}$ *are* G_{00}*-conjugate if and only if* $\dim \mathfrak{c}_{1\star} = \dim \mathfrak{c}_{10} + \dim \mathfrak{c}_{11}$.

Proof. (1) Being a toral subalgebra of $\mathfrak{g}_{1j}$, $\mathfrak{a}_{1j}$ is contained in a little CSS in $\mathfrak{g}_{1j}$.

(2) *"If" part.* Let $\mathfrak{c}_{1\star}$ and $\tilde{\mathfrak{c}}_{1\star} = \tilde{\mathfrak{a}}_{10} \oplus \tilde{\mathfrak{a}}_{11}$ be two homogeneous CSS. By part (1), $\dim \mathfrak{a}_{01} = \dim \tilde{\mathfrak{a}}_{01} = \dim \mathfrak{c}_{10}$. Therefore, both $\mathfrak{a}_{01}$ and $\tilde{\mathfrak{a}}_{01}$ are little CSS, they are both G_{00}-conjugate, and we may assume that $\mathfrak{a}_{01} = \tilde{\mathfrak{a}}_{01}$. Consider then the $\vec{\sigma}$-stable reductive algebra $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{a}_{10})$. As $\mathfrak{a}_{10}$ is a central toral subalgebra, $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{a}_{10}) = \mathfrak{a}_{10} \oplus \mathfrak{s}$, where $\mathfrak{s}$ is reductive and $\vec{\sigma}$-stable. By construction, $\mathfrak{s}_{10} = \{0\}$ and $\mathfrak{a}_{11}, \tilde{\mathfrak{a}}_{11} \subset \mathfrak{s}_{11}$. Moreover, these are little CSS in $\mathfrak{s}_{11}$ (otherwise, $\mathfrak{c}_{1\star}$ or $\tilde{\mathfrak{c}}_{1\star}$ wouldn't be maximal). Therefore, $\mathfrak{a}_{01}$ and $\tilde{\mathfrak{a}}_{01}$ are S_{00}-conjugate, which implies that $\mathfrak{c}_{1\star}$ and $\tilde{\mathfrak{c}}_{1\star}$ and G_{00}-conjugate.

"Only if" part. Assuming that $\dim \mathfrak{c}_{1\star} < \dim \mathfrak{c}_{10} + \dim \mathfrak{c}_{11}$, we construct two homogeneous CSS with different dimension vectors. First, let us take a little CSS $\mathfrak{c}_{10}$ and choose a little CSS in $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{10})_{11}$, say $\tilde{\mathfrak{a}}_{11}$. This yields a homogeneous CSS with dimension vector $(\dim \mathfrak{c}_{10}, \dim \mathfrak{c}_{1\star} - \dim \mathfrak{c}_{10})$. On the other hand, one can start with a little CSS $\mathfrak{c}_{11}$, etc., which yields a homogeneous CSS with dimension vector $(\dim \mathfrak{c}_{1\star} - \dim \mathfrak{c}_{11}, \dim \mathfrak{c}_{11})$. □

Note that $\dim \mathfrak{c}_{ij} > 0$ whenever $\mathfrak{g}_{ij} \neq \{0\}$. Therefore, a coincidence of CSS of the form $\mathfrak{c}_{11} = \mathfrak{c}_{1\star}$ or $\mathfrak{c}_{10} = \mathfrak{c}_{1\star}$ certainly excludes the possibility of having a unique standard component of $\mathfrak{E}$. For our test commutator (3-1), one may envisage several examples of good behavior (not necessarily all together):

(1) All irreducible components of $\mathfrak{E}$ are standard (possibly of different dimension).

(2) φ is surjective and equidimensional, and hence flat.

(3) $\mathfrak{E}$ has a unique standard component, but there may be other components too.

Property (3) always holds in the setting of Example 3.1, with any σ; and for σ of maximal rank, one gets a rare situation, where all three properties are satisfied. All quaternionic decompositions of simple Lie algebras can be written out explicitly, and then the presence of (3) amounts to a routine verification of the equality in Theorem 3.7(2).

Proposition 3.8. *Let* $\{\sigma_1, \sigma_2\}$ *be a dyad. Then* $\dim \mathfrak{g}_{10} = \dim \mathfrak{g}_{01}$ *and* $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}$ *is onto. (Therefore,* $\dim \varphi^{-1}(\xi) \geqslant \dim \mathfrak{g}_{11}$ *for all* $\xi \in \mathfrak{g}_{01}$.*) Moreover,* $\{0\} \times \mathfrak{g}_{11}$ *is a standard irreducible component of* $\mathfrak{E}$ *of minimal dimension.*

Proof. Since $\dim \mathfrak{g}^{\sigma_1} = \dim \mathfrak{g}^{\sigma_2}$, we have $\dim \mathfrak{g}_{10} = \dim \mathfrak{g}_{01}$. By Theorem 2.2(2), any little CSS $\mathfrak{c}_{11} \subset \mathfrak{g}_{11}$ is also a big CSS in $\mathfrak{g}_{1\star}$. Therefore, $\mathfrak{c}_{11}$ is a homogeneous CSS and $\overline{G_{00}\cdot\mathfrak{c}_{11}} = \mathfrak{g}_{11}$ is an irreducible component of $\mathfrak{E}$. Furthermore, if $x \in \mathfrak{c}_{11}$ is generic, then $\mathfrak{z}_{\mathfrak{g}}(x) \cap \mathfrak{g}_{1\star} = \mathfrak{c}_{11}$, that is, $\mathfrak{z}_{\mathfrak{g}}(x) \cap \mathfrak{g}_{10} = \{0\}$. Therefore, $\dim[\mathfrak{g}_{10}, x] = \dim \mathfrak{g}_{10}$, that is, $[\mathfrak{g}_{10}, x] = \mathfrak{g}_{01}$. □

4. Dyads of maximal rank and commuting varieties

Let $\{\sigma_1, \sigma_2\}$ be a dyad of maximal rank, that is, both σ_1 and σ_2 are of maximal rank. Recall that this implies that $\sigma_3 = \sigma_1\sigma_2$ is inner, $\dim \mathfrak{g}_{01} = \dim \mathfrak{g}_{10}$, and, by Proposition 2.1, $\mathfrak{g}^{\sigma_3} = \mathfrak{g}_{00} \oplus \mathfrak{g}_{11}$ is a $\mathbb{Z}_2$-grading of maximal rank. In particular, $\mathfrak{g}_{11}$ contains a CSA of $\mathfrak{g}$ and any CSS in $\mathfrak{g}_{1\star}$ or $\mathfrak{g}_{\star 1}$ is a CSA. The main result of this section is the following.

Theorem 4.1. *Let* $\{\sigma_1, \sigma_2\}$ *be a dyad of maximal rank. Then*

(i) *the commutator mapping* $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}$ *is surjective and equidimensional,*

(ii) *each irreducible component of* $\mathfrak{E} = \varphi^{-1}(0)$ *is standard, that is, is the closure of the* G_{00}*-saturation of a homogeneous CSS in* $\mathfrak{g}_{1\star}$*, and*

(iii) *the ideal of* $\mathfrak{E}$ *is generated by quadrics* $\varphi^{\#}(\mathfrak{g}_{01}^*)$*, where* $\varphi^{\#} : \Bbbk[\mathfrak{g}_{01}] \to \Bbbk[\mathfrak{g}_{10}] \otimes \Bbbk[\mathfrak{g}_{11}]$ *is the comorphism (that is, the scheme* $\varphi^{-1}(0)$ *is a reduced complete intersection).*

Proof. If $\mathfrak{q}$ is a $\vec{\sigma}$-stable reductive subalgebra of $\mathfrak{g}$, then $\mathfrak{E}_{\mathfrak{q}}$ stands for the zero fiber of the commutator $\mathfrak{q}_{10} \times \mathfrak{q}_{11} \to \mathfrak{q}_{01}$. Clearly, $\mathfrak{E}_q \subset \mathfrak{E} = \mathfrak{E}_{\mathfrak{g}}$. Since σ_1 and σ_2 are of maximal rank, the center of $\mathfrak{g}$, $\mathfrak{z}(\mathfrak{g})$, is contained in $\mathfrak{g}_{11}$. Consequently, $\mathfrak{E}_{\mathfrak{g}} \simeq \mathfrak{E}_{[\mathfrak{g},\mathfrak{g}]} \times \mathfrak{z}(\mathfrak{g})$ and without loss of generality, we may assume that $\mathfrak{g}$ is semisimple.

By Proposition 3.8, φ is onto and $\dim \mathfrak{E} \geqslant \dim \mathfrak{g}_{11}$. In this situation, φ is equidimensional if and only if $\dim \mathfrak{E} = \dim \mathfrak{g}_{11}$. If $\mathfrak{c}_{1\star}$ is a homogeneous CSS, then it is necessarily a CSA of $\mathfrak{g}$. That is, $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{1\star})_{01} = 0$ for *all* homogeneous CSS and $\dim \overline{G_{00}\cdot\mathfrak{c}_{1\star}} = \dim \mathfrak{g}_{11}$. Hence all the standard components of $\mathfrak{E}$ have the same (expected) dimension, and for (i) and (ii) it suffices to prove that there are no other irreducible components.

To this end, we argue by induction on $\mathsf{rk}\,\mathfrak{g} = \dim \mathfrak{c}_{11}$.

– If $\dim \mathfrak{c}_{11} = 1$, then $\mathfrak{g} = \mathfrak{sl}_2$ and the assertion is true.

– Suppose that $\mathsf{rk}\,\mathfrak{g} > 1$ and the assertion holds for all dyads of maximal rank for semisimple algebras of rank smaller than $\mathsf{rk}\,\mathfrak{g}$.

(1) Take $(x, y) \in \mathfrak{E}$ and $y \in \mathfrak{g}_{11}$, and let $y = y_s + y_n$ be the Jordan decomposition. Then $[x, y_s] = 0$. If $y_s \neq 0$, then $y_n \in \mathfrak{s} := [\mathfrak{z}_{\mathfrak{g}}(y_s), \mathfrak{z}_{\mathfrak{g}}(y_s)]$ and $\mathsf{rk}\,\mathfrak{s} < \mathsf{rk}\,\mathfrak{g}$. By Lemma 1.2, $\sigma_i|_{\mathfrak{s}}$, $i = 1, 2$, are again involutions of maximal rank. Let $\mathfrak{z}$ denote the center of $\mathfrak{z}_{\mathfrak{g}}(y_s)$, so that $\mathfrak{z}_{\mathfrak{g}}(y_s) = \mathfrak{z} \oplus \mathfrak{s}$ and $y_s \in \mathfrak{z}$. Since both σ_1 and σ_2 are of maximal rank, $\mathfrak{z} \subset \mathfrak{g}_{11}$ and hence $x \in \mathfrak{s}$. By the induction assumption, $(x, y_n) \in \mathfrak{s}_{10} \oplus \mathfrak{s}_{11}$ lies in a standard irreducible component of $\mathfrak{E}_{\mathfrak{s}}$. Obviously, adding a central summand does not affect this property, hence (x, y) lies in a standard component of $\mathfrak{E}_{\mathfrak{z}_{\mathfrak{g}}(y_s)}$. As $\mathsf{rk}\,\mathfrak{z}_{\mathfrak{g}}(y_s) = \mathsf{rk}\,\mathfrak{g}$, this also means that (x, y) lies in a standard component of $\mathfrak{E}$.

(2) Hence it suffices to consider the case in which $y = y_n$. Write $\mathcal{N}_{11}$ for the closed set of all nilpotent elements in $\mathfrak{g}_{11}$. Let $\mathcal{K}$ be an irreducible component of $\mathfrak{E}$, hence $\dim \mathcal{K} \geqslant \dim \mathfrak{g}_{11}$. Then $\mathcal{K}_1 := \mathcal{K} \cap (\mathfrak{g}_{10} \times \mathcal{N}_{11})$ is a closed subvariety of $\mathcal{K}$. If $\mathcal{K}_1 \neq \mathcal{K}$, then, by part (1), all the points in $\mathcal{K} \setminus \mathcal{K}_1$ belong to standard irreducible components. Consequently, $\mathcal{K}$ must be one of the standard components.

(3) The next possibility is that $\mathcal{K} = \mathcal{K}_1$. Let $p : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{11}$ be the projection. Then $p(\mathcal{K}) \subset \mathcal{N}_{11}$, and therefore $\overline{p(\mathcal{K})} = \overline{G_{00} \cdot y}$ is the closure of a nilpotent G_{00}-orbit.

If $y = 0$, then $\mathcal{K} = \mathfrak{g}_{10} \times \{0\}$. Let $\mathfrak{c}_{10}$ be a little CSS. The fact that $\overline{G_{00} \cdot (\mathfrak{c}_{10} \times \{0\})} = \mathfrak{g}_{10} \times \{0\}$ is an irreducible component of $\mathfrak{E}$ implies that $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{10})_{11} = \{0\}$, whence $\mathfrak{c}_{10}$ is also a CSS in $\mathfrak{g}_{1\star}$. That is, $\mathfrak{c}_{10}$ is a CSA of $\mathfrak{g}$. (Incidentally, this means that the (-1)-eigenspace of σ_3 contains a CSA, that is, $\{\sigma_1, \sigma_2, \sigma_3\}$ is actually a triad.) Anyway, we see that if $y = 0$, then such $\mathcal{K}$ appears to be a standard component.

(4) Finally, we prove that the case in which $\mathcal{K} = \mathcal{K}_1$ and $y \neq 0$ is impossible. Assuming the contrary, we would have

$$\begin{aligned}\dim \mathfrak{g}_{11} &\leqslant \dim \mathcal{K} \leqslant \dim G_{00} \cdot y + \dim p^{-1}(y)\\ &= \dim \mathfrak{g}_{00} - \dim \mathfrak{z}_{\mathfrak{g}}(y)_{00} + \dim \mathfrak{z}_{\mathfrak{g}}(y)_{10} = \dim \mathfrak{g}_{11} - \dim \mathfrak{z}_{\mathfrak{g}}(y)_{11} + \dim \mathfrak{z}_{\mathfrak{g}}(y)_{10}.\end{aligned}$$

The last equality uses Lemma 1.1. Hence, the existence of such a component $\mathcal{K}$ would imply that $\dim \mathfrak{z}_{\mathfrak{g}}(y)_{11} \leqslant \dim \mathfrak{z}_{\mathfrak{g}}(y)_{10}$ for some nonzero $y \in \mathcal{N}_{11} \subset \mathfrak{g}_{11}$. One can rewrite the last condition so that it will only depend on the (inner) involution σ_3. Since $\{\sigma_1, \sigma_2\}$ is a dyad, we have $\dim \mathfrak{z}_{\mathfrak{g}}(y)_{10} = \dim \mathfrak{z}_{\mathfrak{g}}(y)_{01}$; and since σ_3 is inner and $\mathfrak{g}^{\sigma_3} = \mathfrak{g}_{00} \oplus \mathfrak{g}_{11}$ is a $\mathbb{Z}_2$-grading of maximal rank, we have $\dim \mathfrak{z}_{\mathfrak{g}}(y)_{11} = \dim \mathfrak{z}_{\mathfrak{g}}(y)_{00} + \mathsf{rk}\,\mathfrak{g}^{\sigma_3} = \dim \mathfrak{z}_{\mathfrak{g}}(y)_{00} + \mathsf{rk}\,\mathfrak{g}$, see (1-2). Then

$$\begin{aligned}\dim \mathfrak{z}_{\mathfrak{g}}(y)_{11} + \dim \mathfrak{z}_{\mathfrak{g}}(y)_{00} + \mathsf{rk}\,\mathfrak{g} &= 2 \dim \mathfrak{z}_{\mathfrak{g}}(y)_{11} \leqslant 2 \dim \mathfrak{z}_{\mathfrak{g}}(y)_{10}\\ &= \dim \mathfrak{z}_{\mathfrak{g}}(y)_{10} + \dim \mathfrak{z}_{\mathfrak{g}}(y)_{01}.\end{aligned}$$

In other words, if the assumption were true, we would have

$$\dim(\mathfrak{z}_{\mathfrak{g}}(y)\cap\mathfrak{g}^{\sigma_3})+\operatorname{rk}\mathfrak{g}\leqslant\dim(\mathfrak{z}_{\mathfrak{g}}(y)\cap\mathfrak{g}_1^{(\sigma_3)}) \tag{4-1}$$

for some nonzero nilpotent $y\in\mathfrak{g}_{11}$. (Note that since $\mathfrak{g}^{\sigma_3}=\mathfrak{g}_{00}\oplus\mathfrak{g}_{11}$ is a $\mathbb{Z}_2$-grading of maximal rank, $\mathfrak{g}_{11}$ meets all nilpotent orbits in $\mathfrak{g}^{\sigma_3}$ [Antonyan 1982]. Therefore, a priori, y can be any nonzero nilpotent element of $\mathfrak{g}^{\sigma_3}$.) However, Theorem 4.4 shows that (4-1) is never satisfied if $y\neq 0$. This completes the proof of parts (i) and (ii).

For (iii), it suffices to prove that each irreducible component of $\mathfrak{E}$ contains a point (x, y) such that $d\varphi_{(x,y)}$ is onto, that is, $\operatorname{Im} d\varphi_{(x,y)}=\mathfrak{g}_{01}$, see [Richardson 1981, Lemma 2.3]. Since each irreducible component of $\mathfrak{E}$ is the closure of the G_{00}-saturation of a homogeneous CSA, it contains a point (x, y) such that $\mathfrak{z}_{\mathfrak{g}}(x)_{01}\cap\mathfrak{z}_{\mathfrak{g}}(y)_{01}=\{0\}$ and then $d\varphi_{(x,y)}$ is onto, as shown in the proof of Lemma 3.2. □

Remark 4.2. (1) For any inner $\sigma\in\mathsf{Inv}(\mathfrak{g})$, there exist commuting involutions of maximal rank σ_1 and σ_2 such that $\sigma=\sigma_1\sigma_2$, see Proposition 2.1. Therefore, there are sufficiently many quaternionic decompositions, where Theorem 4.1 applies.

(2) For an arbitrary dyad $\{\sigma_1,\sigma_2\}$, it can happen that all irreducible components of $\mathfrak{E}$ are standard, but they have different dimensions. That is, $\varphi:\mathfrak{g}_{10}\times\mathfrak{g}_{11}\to\mathfrak{g}_{01}$ is not equidimensional, but still any pair of commuting elements in $\mathfrak{g}_{10}\times\mathfrak{g}_{11}$ can be approximated by a pair of commuting *semisimple* elements.

Example 4.3. Let σ_1 be an involution of $\mathfrak{g}=\mathfrak{so}_n$ such that $\mathfrak{g}^{\sigma_1}=\mathfrak{so}_{n-1}$. This can be included in a dyad $\{\sigma_1,\sigma_2\}$ such that $\mathfrak{g}^{\sigma_3}=\mathfrak{so}_{n-2}\times\mathfrak{so}_2$. The quaternionic decomposition is

$$\mathfrak{g}=\begin{array}{cc}\mathfrak{so}_{n-2} & \mathsf{R}(\varpi_1)\\ \mathsf{R}(\varpi_1) & \mathsf{R}(0)\end{array}\ \begin{array}{l}\sigma_1,\\ \sigma_2\end{array}$$

where the trivial $\mathfrak{so}_{n-2}$-module $\mathsf{R}(0)$ is just the central torus $\mathfrak{so}_2$ in $\mathfrak{g}^{\sigma_3}$. Here $\dim\mathfrak{c}_{10}=\dim\mathfrak{c}_{11}=1$ and the zero fiber of multiplication $\mathfrak{g}_{10}\times\mathfrak{g}_{11}\to\mathfrak{g}_{01}$ consists of two irreducible components, $\mathfrak{g}_{10}\times\{0\}\simeq\Bbbk^{n-2}$ and $\{0\}\times\mathfrak{g}_{11}\simeq\Bbbk$. Both components are standard.

The following auxiliary result does not refer to quaternionic decompositions; it concerns the case of a sole involution.

Theorem 4.4. *Let σ be an arbitrary involution of $\mathfrak{g}$ and $\mathfrak{g}=\mathfrak{g}_0\oplus\mathfrak{g}_1$ the corresponding $\mathbb{Z}_2$-grading. For any nonzero $x\in\mathfrak{g}_0$, we have*

$$\dim\mathfrak{g}_0^x+\operatorname{rk}\mathfrak{g}-\dim\mathfrak{g}_1^x>0. \tag{4-2}$$

More precisely, one always has $\dim \mathfrak{g}_0^x + \mathrm{rk}\,\mathfrak{g} - \dim \mathfrak{g}_1^x \geqslant 0$ *and the equality only occurs if* $x = 0$ *and* σ *is of maximal rank.*

Remark 4.5. For application to Theorem 4.1, we only need the case when x is nilpotent and σ is inner. But, surprisingly, the assertion appears to be absolutely general. Unfortunately, our proof is not conceptual, after all. Having successfully reduced the problem to noneven nilpotent elements of $\mathfrak{g}_0$, we then resort to case-by-case considerations. Certainly, there must be a better proof!

Proof. Note that $\dim G{\cdot}x$ is even and, therefore, the left-hand side in (4-2) is always even; hence the more accurate assertion is that $\dim \mathfrak{g}_0^x + \mathrm{rk}\,\mathfrak{g} - \dim \mathfrak{g}_1^x \geqslant 2$ for all nonzero $x \in \mathfrak{g}_0$.

(1) If $x = 0$, then we have $\dim \mathfrak{g}_0 + \mathrm{rk}\,\mathfrak{g} - \dim \mathfrak{g}_1 \geqslant 0$, and the equality holds if and only if σ is of maximal rank.

(2) If x is nonzero semisimple, then $\mathfrak{g}^x$ is a σ-stable reductive subalgebra and x is a central element of $\mathfrak{g}^x$ that belongs to $\mathfrak{g}_0^x$. Write $\mathfrak{g}^x = \mathfrak{z} \oplus \mathfrak{s}$, where $\mathfrak{s} = [\mathfrak{g}^x, \mathfrak{g}^x]$ and $\mathfrak{z}$ is the center. Then $\dim \mathfrak{z}_0 > 0$ and

$$\dim \mathfrak{g}_0^x + \mathrm{rk}\,\mathfrak{g} - \dim \mathfrak{g}_1^x = (\dim \mathfrak{s}_0 + \mathrm{rk}\,\mathfrak{s} - \dim \mathfrak{s}_1) + 2\dim \mathfrak{z}_0 \geqslant 2.$$

(3) If x is nonnilpotent, then using the Jordan decomposition $x = x_s + x_n$, we reduce the problem to the same property for the nilpotent element x_n in the σ-stable reductive subalgebra $\mathfrak{z}_{\mathfrak{g}}(x_s)$.

(4) From now on, we assume that $x = e \in \mathfrak{g}_0$ is nonzero and nilpotent. Choose an $\mathfrak{sl}_2$-triple $\{e, h, f\} \subset \mathfrak{g}_0$. Suppose that e is even in $\mathfrak{g}$, that is, the eigenvalues of $\mathrm{ad}\,h$ in $\mathfrak{g}$ are even. Then $\dim \mathfrak{g}^h = \dim \mathfrak{g}^e$ and $\dim \mathfrak{g}_0^h = \dim \mathfrak{g}_0^e$. Thus, the assertion is reduced to the same assertion for $h \in \mathfrak{g}_0$ and we are again in the setting of part (2).

(5) Suppose that e is even in $\mathfrak{g}_0$, but not in $\mathfrak{g}$. That is, the eigenvalues of $\mathrm{ad}\,h$ in $\mathfrak{g}_0$ are even, but $\mathrm{ad}\,h$ has also some odd eigenvalues in $\mathfrak{g}_1$. Decomposing $\mathfrak{g}$ into the sum of σ-stable ideals, we may assume that either $\mathfrak{g}$ is simple or $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{s}$, where $\mathfrak{s}$ is simple and σ is the permutation involution. In the second case, if e is even in $\mathfrak{g}_0 = \Delta(\mathfrak{s})$, then e is also even in $\mathfrak{g}$. Therefore, without loss of generality, we may assume that $\mathfrak{g}$ is simple.

Let us decompose $\mathfrak{g}_1$ according to the parity of $\mathrm{ad}\,h$-eigenvalues: $\mathfrak{g}_1 = \mathfrak{g}_1^{\mathrm{odd}} \oplus \mathfrak{g}_1^{\mathrm{even}}$. By assumption, $\mathfrak{g}_1^{\mathrm{odd}} \neq 0$. Then $\tilde{\mathfrak{g}} := [\mathfrak{g}_1^{\mathrm{odd}}, \mathfrak{g}_1^{\mathrm{odd}}] \oplus \mathfrak{g}_1^{\mathrm{odd}}$ is an ideal of $\mathfrak{g}$ that does not meet $\mathfrak{g}_1^{\mathrm{even}}$. Therefore, $\tilde{\mathfrak{g}} = \mathfrak{g}$ and $\mathfrak{g}_1^{\mathrm{even}} = 0$. Hence $\mathfrak{g}_0^e = (\mathfrak{g}^e)^{\mathrm{even}}$ and $\mathfrak{g}_1^e = (\mathfrak{g}^e)^{\mathrm{odd}}$. Consider the $\mathbb{Z}$-grading of $\mathfrak{g}$ determined by the eigenvalues of h, $\mathfrak{g} = \bigoplus_{i \in \mathbb{Z}} \mathfrak{g}(i)$. The $\mathfrak{sl}_2$-theory shows that $\dim(\mathfrak{g}^e)^{\mathrm{even}} = \dim \mathfrak{g}(0)$ and $\dim(\mathfrak{g}^e)^{\mathrm{odd}} = \dim \mathfrak{g}(1)$. Hence $\dim \mathfrak{g}_0^e = \dim \mathfrak{g}(0)$ and $\dim \mathfrak{g}_1^e = \dim \mathfrak{g}(1)$. Finally, it follows from Vinberg's lemma [Vinberg 1976, §2.3] that the group $G(0)$ has finitely many orbits in $\mathfrak{g}(1)$, whence

$\dim \mathfrak{g}(1) \leqslant \dim \mathfrak{g}(0)$. Thus, in this case the stronger inequality $\dim \mathfrak{g}_0^e \geqslant \dim \mathfrak{g}_1^e$ holds.

(6) Thus, it remains to handle the case in which a nilpotent element $e \in \mathfrak{g}_0$ is not even. Here we do not know an a priori argument and resort to the case-by-case considerations.

(7) If $\mathfrak{g}$ is a classical Lie algebra, then the nilpotent orbits in $\mathfrak{g}$ and $\mathfrak{g}_0$ are parameterised by partitions, and we use the explicit formulae for $\dim \mathfrak{g}^e$ and $\dim \mathfrak{g}_0^e$ in terms of partitions. Some of these calculations are presented in the Appendix.

(8) If $\mathfrak{g}$ is an exceptional simple Lie algebra, then, for any noneven nilpotent element $e \in \mathfrak{g}_0$, we determine the corresponding nilpotent orbit in $\mathfrak{g}$ and then compare the dimensions of $\mathfrak{g}_0^e$ and $\dim \mathfrak{g}^e$. While rather boring, the verification is, however, not very difficult.

For σ inner, we use the seminal work [Dynkin 1952, Tables 16–20], in which Dynkin computed, for all simple three-dimensional subalgebras in exceptional Lie algebras, the "minimal including regular semisimple subalgebras" and the corresponding weighted Dynkin diagrams. See also comments on this article in [Dynkin 2000, pp. 309–312], where a few errors occurring in [Dynkin 1952] are corrected.

To convey the idea, consider some examples related to an (inner) involution of $\mathfrak{g} = \mathbf{E}_8$ with $\mathfrak{g}_0 = \mathbf{D}_8 = \mathfrak{so}_{16}$. There are 33 noneven nilpotent orbits in $\mathfrak{g}_0$. (Recall that $e \in \mathfrak{so}_{16}$ is noneven if and only if the partition of e contains both odd and even parts.)

(a) Let $e \in \mathfrak{so}_{16}$ be a nilpotent element corresponding to the partition $(11, 2, 2, 1)$. Using [Hesselink 1976, Corollary 3.8(a)] or [Kraft and Procesi 1982, Proposition 2.4], we obtain $\dim \mathfrak{g}_0^e = 16$. This partition also shows that a minimal including regular semisimple subalgebra of $\mathbf{D}_8$ containing e is of type $\mathbf{D}_6 + \mathbf{A}_1$. (Here $(11, 1)$ is the partition of the regular nilpotent element of $\mathbf{D}_6$ and any pair of equal parts (n, n) gives rise to the simple summand $\mathbf{A}_{n-1}$.) Then using [Dynkin 1952, Table 20], we detect the simple three-dimensional subalgebra in $\mathbf{E}_8$ with minimal including regular semisimple subalgebra of type $\mathbf{D}_6 + \mathbf{A}_1$. The corresponding nilpotent orbit has the modern label $\mathbf{E}_7(a_3)$ and here $\dim \mathfrak{g}^e = 28$. Hence $\dim \mathfrak{g}_1^e = 12$ and (4-2) holds.

(b) Let $e \in \mathfrak{so}_{16}$ correspond to the partition $(7, 5, 2, 2)$. By [Hesselink 1976, Corollary 3.8(a)], $\dim \mathfrak{g}_0^e = 22$. Here a minimal including regular semisimple subalgebra is of type $\mathbf{D}_6(a_2) + \mathbf{A}_1$, because the partition $(7, 5)$ determines the distinguished nilpotent orbit in $\mathbf{D}_6$, which is denoted by $\mathbf{D}_6(a_2)$. Using [Dynkin 1952, Table 20], we detect the corresponding nilpotent orbit in $\mathfrak{g}$. This orbit is denoted nowadays by $\mathbf{E}_7(a_5)$ and here $\dim \mathfrak{g}^e = 42$.

(c) Let $e \in \mathfrak{so}_{16}$ correspond to the partition $(7,4,4,1)$. By [Hesselink 1976, Corollary 3.8(a)], $\dim \mathfrak{g}_0^e = 22$. Here a minimal including regular semisimple subalgebra is of type $\mathbf{D}_4 + \mathbf{A}_3$. Using [Dynkin 1952, Table 20], we detect the corresponding nilpotent orbit in $\mathfrak{g}$. This orbit is denoted nowadays by $\mathbf{D}_6(a_2)$ and here $\dim \mathfrak{g}^e = 44$.

If σ is outer, then $\mathfrak{g}$ is of type $\mathbf{E}_6$. In the respective two cases, we use the information on $e \in \mathfrak{g}_0$ for decomposing $\mathfrak{g}_1$ as a $\langle e, h, f\rangle$-module, which allows us to compute $\dim \mathfrak{g}_1^e$. □

A case-free proof of Theorem 4.4 might be derived from the following conjectural invariant-theoretic property of centralizers. Recall that $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$ and $e \in \mathfrak{g}_0$. Let G_0^e be the connected subgroup of G_0 with Lie algebra $\mathfrak{g}_0^e$. Then G_0^e acts on $(\mathfrak{g}_1^e)^*$ and we write $\Bbbk((\mathfrak{g}_1^e)^*)^{G_0^e}$ for the field of G_0^e-invariant rational functions on $(\mathfrak{g}_1^e)^*$.

Conjecture 4.6. *For any $e \in \mathfrak{g}_0 \cap \mathcal{N}$, we have* $\operatorname{trdeg} \Bbbk((\mathfrak{g}_1^e)^*)^{G_0^e} \leqslant \operatorname{rk} \mathfrak{g}$.

By Rosenlicht's theorem [Brion 2000, Chapter I.6],

$$\operatorname{trdeg} \Bbbk((\mathfrak{g}_1^e)^*)^{G_0^e} = \dim \mathfrak{g}_1^e - \max_{\xi \in (\mathfrak{g}_1^e)^*} \dim G_0^e \cdot \xi .$$

If $e \neq 0$, then the one-dimensional unipotent group $\exp(te)$, $t \in \Bbbk$, acts trivially on $\mathfrak{g}_1^e$ and hence $\max_{\xi \in (\mathfrak{g}_1^e)^*} \dim G_0^e \cdot \xi \leqslant \dim \mathfrak{g}_0^e - 1$. Therefore, if the conjecture were true, we would obtain $\dim \mathfrak{g}_1^e - \dim \mathfrak{g}_0^e + 1 \leqslant \operatorname{rk} \mathfrak{g}$, as required. Perhaps, this can be related to the Elashvili conjecture, which asserts that $\operatorname{trdeg} \Bbbk((\mathfrak{g}^e)^*)^{G^e} = \operatorname{rk} \mathfrak{g}$ for all $e \in \mathcal{N}$.

Remark 4.7. Inequality (4-2) can be written as $\dim \mathfrak{g}_0^x > \dim \mathcal{B}_x$, where $\mathcal{B}_x$ is the variety of Borel subalgebras of $\mathfrak{g}$ containing x (the Springer fiber of x). (Recall that $\dim \mathcal{B}_x = (\dim \mathfrak{g}^x - \operatorname{rk} \mathfrak{g})/2$.)

5. Commuting varieties and restricted root systems

Here we assume that $\{\sigma_1, \sigma_2\}$ is a dyad. As above, we consider the commutator map $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}$ and the $\vec{\sigma}$-commuting variety $\mathfrak{E} = \varphi^{-1}(0)$. Then $\dim \mathfrak{E} \geqslant \dim \mathfrak{g}_{11}$ and $\mathfrak{E}$ has a standard irreducible component of expected dimension $\dim \mathfrak{g}_{11}$; namely, $\{0\} \times \mathfrak{g}_{11}$, see Proposition 3.8.

In this section, we describe a method for detecting subvarieties of $\mathfrak{E}$ of large dimension. This method is based on comparing restricted root systems for little and big symmetric spaces related to the quaternionic decomposition in question.

Take a little CSS $\mathfrak{c}_{11} \subset \mathfrak{g}_{11}$. Then, by Theorem 2.2(2), $\mathfrak{c}_{11}$ is also a CSS in $\mathfrak{g}_{1\star}$ and $\mathfrak{g}_{\star 1}$, which is equivalent to that $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})_{10} = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})_{01} = \{0\}$ and $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})_{11} = \mathfrak{c}_{11}$. Our idea is to replace $\mathfrak{c}_{11}$ with a proper subspace $\tilde{\mathfrak{c}}$ such that

$$\tilde{\mathfrak{c}} \text{ still contains } G_{00}\text{-regular elements.} \tag{5-1}$$

Then we consider $\hat{\mathfrak{c}} := \mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})_{10} \times \tilde{\mathfrak{c}} \subset \mathfrak{E}$ and compute the dimension of $G_{00}{\cdot}\hat{\mathfrak{c}}$. Since $\overline{G_{00}{\cdot}\mathfrak{c}_{11}} = \mathfrak{g}_{11}$, we have

$$\dim G_{00} + \dim \mathfrak{c}_{11} - \dim \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})_{00} = \dim \mathfrak{g}_{11}.$$

Set $\mathfrak{T}_{00}(\hat{\mathfrak{c}}) = \{g \in G_{00} \mid g{\cdot}y \in \hat{\mathfrak{c}} \text{ for generic } y \in \hat{\mathfrak{c}}\}$, and likewise for $\mathfrak{c}_{11}$. In view of (5-1), we have $\dim \mathfrak{T}_{00}(\hat{\mathfrak{c}}) = \dim \mathfrak{T}T_{00}(\mathfrak{c}_{11}) = \dim \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})_{00}$. Then

$$\begin{aligned}\dim G_{00}{\cdot}\hat{\mathfrak{c}} &= \dim G_{00} + \dim \hat{\mathfrak{c}} - \dim \mathfrak{T}_{00}(\hat{\mathfrak{c}}) \\ &= (\dim G_{00} + \dim \mathfrak{c}_{11} - \dim \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})_{00}) + (\dim \mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})_{10} - \dim \mathfrak{c}_{11} + \dim \tilde{\mathfrak{c}}) \\ &= \dim \mathfrak{g}_{11} + (\dim \hat{\mathfrak{c}} - \dim \mathfrak{c}_{11}). \qquad (5\text{-}2)\end{aligned}$$

Thus, we obtain a subvariety of larger dimension, if $\dim \mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})_{10} + \dim \tilde{\mathfrak{c}} > \dim \mathfrak{c}_{11}$. Of course, it is not always possible to construct such a $\tilde{\mathfrak{c}}$. Our sufficient condition exploits restricted root systems. Set $\mathfrak{h} = \mathfrak{g}^{\sigma_3}$, and let H denote the corresponding connected (reductive) subgroup of G. Write $\bar{\sigma}$ for the restriction to H of σ_1 or σ_2.

Let $C_{11} = \exp(\mathfrak{c}_{11}) \subset H \subset G$ be the corresponding torus. The coincidence of CSS means that C_{11} is a maximal σ_1-anisotropic torus in G and a maximal $\bar{\sigma}$-anisotropic torus in H. Accordingly, one obtains the inclusion of two restricted root systems relative to C_{11}:

$$\Psi(H/G_{00}) \subset \Psi(G/G_{0\star}).$$

Identifying restricted roots and their differentials, one may consider restricted roots as linear forms on $\mathfrak{c}_{11}$. Then the set of G_{00}-regular elements of $\mathfrak{c}_{11}$ is

$$\{x \in \mathfrak{c}_{11} \mid \mu(x) \neq 0 \text{ for all } \mu \in \Psi(H/G_{00})\}$$

and the set of $G_{0\star}$-regular elements is $\{x \in \mathfrak{c}_{11} \mid \mu(x) \neq 0 \text{ for all } \mu \in \Psi(G/G_{0\star})\}$.

Proposition 5.1. *Assume that $\mu \in \Psi(G/G_{0\star})$ and $r\mu \notin \Psi(H/G_{00})$ for any $r \in \mathbb{Q}$. If $m_\mu > 1$, then $\dim \mathfrak{E} \geqslant \dim \mathfrak{g}_{11} + m_\mu - 1 > \dim \mathfrak{g}_{11}$.*

Proof. Under this assumption, $\tilde{\mathfrak{c}} := \operatorname{Ker}(\mu) \subset \mathfrak{c}_{11}$ still contains G_{00}-regular elements, and $\dim \tilde{\mathfrak{c}} = \dim \mathfrak{c}_{11} - 1$. Furthermore, $\mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})$ is $\vec{\boldsymbol{\sigma}}$-stable and $\mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}}) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11}) \oplus \mathfrak{g}_{\mu} \oplus \mathfrak{g}_{-\mu}$. Recall that $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{c}_{11})$ is contained in $\mathfrak{g}_{00} \oplus \mathfrak{g}_{11}$. Clearly, $\mathfrak{g}_{\mu} \oplus \mathfrak{g}_{-\mu}$ is also $\vec{\boldsymbol{\sigma}}$-stable and is contained in $\mathfrak{g}_{01} \oplus \mathfrak{g}_{10}$.

Since $\{\sigma_1, \sigma_2\}$ is a dyad, $\dim(\mathfrak{g}_{\mu} \oplus \mathfrak{g}_{-\mu}) \cap \mathfrak{g}_{10} = \dim(\mathfrak{g}_{\mu} \oplus \mathfrak{g}_{-\mu}) \cap \mathfrak{g}_{01} = m_\mu$. Hence $\dim \mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})_{10} = m_\mu$, and the assertion follows from (5-2). □

Remark 5.2. (1) Such a construction gives nothing, if all root multiplicities in $\Psi(G/G_{0\star})$ are equal to 1. For instance, if σ_1 is of maximal rank.

(2) The procedure described in the previous proof admits obvious modifications. Roughly speaking, if there are linearly independent roots $\mu_1, \mu_2, \ldots,$ in $\Psi(G/G_{0\star})$, with large multiplicities, such that $\mathbb{Q} - span\{\mu_1, \mu_2, \ldots\} \cap \Psi(H/G_{00}) = \varnothing$, then one can take $\tilde{\mathfrak{c}} = \operatorname{Ker}(\mu_1, \mu_2, \ldots)$, see Proposition 6.5.

Although it is convenient to stick to one specific $\vec{\sigma}$-commuting variety in theoretical considerations, it may happen that in concrete examples different $\vec{\sigma}$-commuting varieties exhibit different good (or bad) properties.

Example 5.3. Let σ_1 be an outer involution of $\mathfrak{g} = \mathfrak{sl}_{2n}$ with $\mathfrak{g}^{\sigma_1} = \mathfrak{sp}_{2n}$. In [Panyushev 2013, §2], we gave a method for describing all the dyads including σ_1, which exploits the restricted root system $\Psi(G/G^{\sigma_1})$. This implies that one can find σ_2 conjugated σ_1 such that the inner involution $\sigma_3 = \sigma_1\sigma_2$ has the fixed-point subalgebra $\mathfrak{h} = \mathfrak{sl}_{2m} \oplus \mathfrak{sl}_{2n-2m} \oplus \mathfrak{t}_1$. The corresponding quaternionic decomposition is

$$\mathfrak{sl}_{2n} = \begin{array}{c} \mathfrak{sp}_{2m} \oplus \mathfrak{sp}_{2n-2m} \\ \hline \mathsf{R}(\varpi_1)\mathsf{R}(\varpi_1') \end{array} \oplus \begin{array}{c} \mathsf{R}(\varpi_1)\mathsf{R}(\varpi_1') \\ \hline \mathsf{R}(\varpi_2)+\mathsf{R}(\varpi_2')+\mathsf{R}(0) \end{array} \quad \begin{array}{l} \sigma_1, \\ \\ \sigma_2 \end{array}$$

where ϖ_i (resp. ϖ_i') are fundamental weights of $\mathfrak{sp}_{2m}$ (resp. $\mathfrak{sp}_{2n-2m}$), and $\mathsf{R}(\lambda)$ is a simple module of the respective simple Lie algebra with highest weight λ.

• Here $G = \mathrm{SL}_{2n}$, $G_{0\star} = \mathrm{Sp}_{2n}$, $H = \mathrm{SL}_{2m} \times \mathrm{SL}_{2(n-m)} \times T_1$, and $G_{00} = Sp_{2m} \times Sp_{2(n-m)}$. According to [Helgason 1978, Chapter X, Table VI], we have $\Psi(G/G_{0\star}) = \mathbf{A}_{n-1}$, $\Psi(H/G_{00}) = \mathbf{A}_{m-1} + \mathbf{A}_{n-m-1}$, and all root multiplicities in $\Psi(G/G_{0\star})$ equal 4. Since $\Psi(H/G_{00})$ has fewer roots, Proposition 5.1 implies that $\mathfrak{E}$ has an irreducible component of dimension greater than $\dim \mathfrak{g}_{11} + (4-1)$ and our test map $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}$ is not equidimensional.

• Here $\dim \mathfrak{c}_{01} = \dim \mathfrak{c}_{10} = \min\{m, n-m\}$ and any big CSS in $\mathfrak{g}_{10} \oplus \mathfrak{g}_{01}$ is of dimension $2\min\{m, n-m\}$. By Theorem 3.7(2), this means that all homogeneous CSS in $\mathfrak{g}_{10} \oplus \mathfrak{g}_{01}$ are G_{00}-conjugate, and therefore the $\vec{\sigma}$-commuting variety related to the commutator $\mathfrak{g}_{10} \oplus \mathfrak{g}_{01} \to \mathfrak{g}_{11}$ has a unique standard component.

Example 5.4. Let σ be an involution of $\mathfrak{g} = \mathbf{E}_7$ with $\mathfrak{g}^{\sigma} = \mathbf{D}_6 \times \mathbf{A}_1$. It can be included in two nonconjugate triads [Kollross 2009]. One of them has $\mathfrak{g}_{00} = \mathbf{D}_4 \times \mathbf{A}_1^3$, with quaternionic decomposition

$$\mathbf{E}_7 = \begin{array}{c} \mathbf{D}_4 \times \mathbf{A}_1^3 \\ \hline \mathsf{R}(\varpi_3)\mathsf{R}(\varpi)\mathsf{R}(\varpi') \end{array} \oplus \begin{array}{c} \mathsf{R}(\varpi_4)\mathsf{R}(\varpi)\mathsf{R}(\varpi'') \\ \hline \mathsf{R}(\varpi_1)\mathsf{R}(\varpi')\mathsf{R}(\varpi'') \end{array} \quad \begin{array}{l} \sigma_1, \\ \\ \sigma_2 \end{array}$$

where ϖ, ϖ', and ϖ'' are the fundamental weights of the simple factors of $\mathbf{A}_1^3$, and ϖ_i are fundamental weights of $\mathbf{D}_4$. Here $\dim \mathfrak{g}_{ij} = 32$ for $(ij) \neq (00)$ and our test commutator map is

$$\varphi : \mathsf{R}(\varpi_3)\mathsf{R}(\varpi)\mathsf{R}(\varpi') \times \mathsf{R}(\varpi_1)\mathsf{R}(\varpi')\mathsf{R}(\varpi'') \to \mathsf{R}(\varpi_4)\mathsf{R}(\varpi)\mathsf{R}(\varpi'').$$

Using [Helgason 1978, Chapter X, Table VI], we find that $\mathrm{rk}(\mathbf{E}_7/\mathbf{D}_6\times\mathbf{A}_1)=4$ and the restricted root system $\Psi(\mathbf{E}_7/\mathbf{D}_6\times\mathbf{A}_1)$ is of type $\mathbf{F}_4$; whereas $\mathrm{rk}(\mathbf{D}_6\times\mathbf{A}_1/\mathbf{D}_4\times\mathbf{A}_1^3)=\mathrm{rk}(\mathbf{D}_6/\mathbf{D}_4\times\mathbf{A}_1^2)=4$ and the corresponding root system is of type $\mathbf{B}_4$. The long (resp. short) roots of $\mathbf{B}_4$ are also long (resp. short) roots of $\mathbf{F}_4$, and the multiplicities are $m_{\mathrm{long}}=1$ and $m_{\mathrm{short}}=4$. However, the root system $\mathbf{B}_4$ has fewer short roots than $\mathbf{F}_4$. Therefore, Proposition 5.1 applies here, and $\mathfrak{E}$ has an irreducible component of dimension at least $\mathfrak{m}_{\mathrm{short}}-1+\dim\mathfrak{g}_{11}=35$.

Example 5.5. Let σ be an involution of $\mathfrak{g}=\mathbf{F}_4$ with $\mathfrak{g}^\sigma=\mathbf{B}_4=\mathfrak{so}_9$. Up to conjugacy, this involution can be included in a unique triad [Kollross 2009], with quaternionic decomposition

$$\mathbf{F}_4=\begin{array}{c|c}\mathbf{D}_4 & \mathsf{R}(\varpi_4)\\ \hline \mathsf{R}(\varpi_3) & \mathsf{R}(\varpi_1)\end{array}\ \begin{array}{l}\sigma_1,\\ \\ \sigma_2\end{array}$$

where $\dim\mathsf{R}(\varpi_i)=8$ and the main diagonal represents the little involution of $\mathfrak{g}^{\sigma_3}=\mathbf{B}_4=\mathfrak{so}_9$. Our test commutator is the bilinear $\mathbf{D}_4$-equivariant mapping $\mathsf{R}(\varpi_3)\times\mathsf{R}(\varpi_1)\to\mathsf{R}(\varpi_4)$. Here $\mathrm{rk}(\mathbf{F}_4/\mathbf{B}_4)=1$ and the restricted root system $\Psi(\mathbf{F}_4/\mathbf{B}_4)$ is of type $\mathbf{BC}_1$. The restricted root system $\Psi(\mathbf{B}_4/\mathbf{D}_4)$ is of type $\mathbf{C}_1$. Since all little and big CSS are one-dimensional, Proposition 5.1 does not help here. Actually, the only standard components of $\mathfrak{E}$ are $\mathfrak{g}_{10}\times\{0\}$ and $\{0\}\times\mathfrak{g}_{11}$, both of dimension eight. Below, we describe an "intermediate" nonstandard irreducible component of dimension eleven.

Let $x\in\mathfrak{g}_{11}\simeq\mathsf{R}(\varpi_1)$ be a nonzero nilpotent element. All such elements form a sole seven-dimensional SO_8-orbit. By Lemma 1.1, $\dim\mathrm{SO}_9{\cdot}x=2{\cdot}7=14$ and hence $\dim(\mathfrak{so}_9)^x=22$. The only nilpotent SO_9-orbit of dimension fourteen in $\mathfrak{so}_9$ is the orbit of short root vectors. The short roots of $\mathfrak{g}^{\sigma_3}=\mathbf{B}_4$ are also short roots of $\mathfrak{g}=\mathbf{F}_4$. Therefore, a minimal including regular semisimple subalgebra is $\tilde{\mathbf{A}}_1$ in Dynkin's notation. This implies that $\dim\mathfrak{z}_\mathfrak{g}(x)=30$ and completely determines the dimension matrix of the spaces $\mathfrak{z}_\mathfrak{g}(x)_{ij}$:

$$\begin{array}{c|c}21 & 4\\ \hline 4 & 1\end{array}.$$

Here the one-dimensional space $\mathfrak{g}_{11}$ is just the line $\Bbbk x$. Then $\dim\overline{G_{00}\cdot(\mathfrak{z}_\mathfrak{g}(x)_{10}\oplus\Bbbk x)}=4+7=11$. Using the projection $\mathfrak{E}\to\mathfrak{g}_{11}$, one can prove that $\overline{G_{00}\cdot(\mathfrak{z}_\mathfrak{g}(x)_{10}\oplus\Bbbk x)}$ is the only new irreducible component of $\mathfrak{E}$. It is contained in $\mathcal{N}_{10}\times\mathcal{N}_{11}$. Thus, $\mathfrak{E}$ has three irreducible components.

6. Triads of Hermitian involutions and simple Jordan algebras

In this section, $\mathfrak{g}$ is assumed to be simple. We say that $\sigma\in\mathsf{Inv}(\mathfrak{g})$ is *Hermitian* if $\mathfrak{g}_0$ is not semisimple. All these involutions are associated with $\mathbb{Z}$-gradings of $\mathfrak{g}$ with

only three nonzero terms (*short gradings*), that is, with parabolic subalgebras with abelian nilpotent radical. Let $\mathfrak{g} = \mathfrak{g}(-1) \oplus \mathfrak{g}(0) \oplus \mathfrak{g}(1)$ be a short grading. Then $\mathfrak{p} = \mathfrak{g}(0) \oplus \mathfrak{g}(1)$ is a (maximal) parabolic subalgebra with abelian nilpotent radical, and one defines a Hermitian involution σ by letting $\mathfrak{g}^{\sigma} = \mathfrak{g}(0)$ and $\mathfrak{g}_1^{(\sigma)} = \mathfrak{g}(-1) \oplus \mathfrak{g}(1)$.

Since $\mathfrak{g}$ is simple, the center of $\mathfrak{g}(0)$ is one-dimensional and there is a *unique* $h \in \mathfrak{g}(0)$ such that $\mathfrak{g}(i) = \{x \in \mathfrak{g} \mid [h, x] = 2ix\}$. By [Vinberg 1976, §2.3], the reductive group $G(0)$ has finitely many orbits in $\mathfrak{g}(1)$. Let $\mathcal{O}$ be the dense $G(0)$-orbit in $\mathfrak{g}(1)$ and $e \in \mathcal{O}$. Set $\mathfrak{g}(i)^e = \mathfrak{g}(i) \cap \mathfrak{g}^e$.

For future reference, we provide a proof of the following well-known assertion.

Lemma 6.1. *$h \in [\mathfrak{g}, e] \iff \mathfrak{g}(0)^e$ is reductive.*

Proof. (1) If $h \in [\mathfrak{g}, e]$, then $h = [e, f]$ for some $f \in \mathfrak{g}(-1)$ and therefore, $\{e, h, f\}$ is an $\mathfrak{sl}_2$-triple. Then $\mathfrak{g}(0)^e = \mathfrak{z}_{\mathfrak{g}}(e, h, f)$, which is reductive.

(2) For $e \in \mathcal{O}$, we have $\dim \mathfrak{g}(0)^e = \dim \mathfrak{g}(0) - \dim \mathfrak{g}(1)$. Using the Kirillov–Kostant form associated with e, we see that $\dim \mathfrak{g}(-1) - \dim \mathfrak{g}(-1)^e = \dim \mathfrak{g}(0) - \dim \mathfrak{g}(0)^e$. Hence $\mathfrak{g}(-1)^e = 0$ and $\mathfrak{g}^e = \mathfrak{g}(0)^e \oplus \mathfrak{g}(1)$. Set $\mathfrak{k} = \mathfrak{g}(0)^e$, and let $(\ )^{\perp}$ denote the orthocomplement with respect to the Killing form. Then $[\mathfrak{g}, e] = (\mathfrak{g}^e)^{\perp} = \mathfrak{g}(1) \oplus (\mathfrak{k}^{\perp} \cap \mathfrak{g}(0))$. Now, if $\mathfrak{k}$ is reductive, then the restriction of the Killing form to $\mathfrak{k}$ is nondegenerate and $\mathfrak{m} := \mathfrak{k}^{\perp} \cap \mathfrak{g}(0)$ is a $\mathfrak{k}$-stable complement to $\mathfrak{k}$ in $\mathfrak{g}(0)$. Since $\dim[\mathfrak{g}(-1), e] = \dim \mathfrak{g}(1) = \dim \mathfrak{g}(0) - \dim \mathfrak{k}$, we conclude that $\mathfrak{m} = [\mathfrak{g}(-1), e]$. Thus, e acts on $\mathfrak{g}$ as follows:

$$\begin{cases} \mathfrak{g}(-1) \xrightarrow{\sim} \mathfrak{m} \xrightarrow{\sim} \mathfrak{g}(1) \to 0 \\ \qquad\qquad\ \mathfrak{k} \to 0. \end{cases} \tag{6-1}$$

Let $\{e, \tilde{h}, f\}$ be an $\mathfrak{sl}_2$-triple with $\tilde{h} \in \mathfrak{g}(0)$ and $f \in \mathfrak{g}(-1)$. Such a triple always exists, see [Vinberg 1979, §2]. Then (6-1) shows that $\mathfrak{g}$ is a sum of three-dimensional and one-dimensional $\mathfrak{sl}_2$-modules, and that $\mathfrak{g}^{\tilde{h}} = \mathfrak{k} \oplus \mathfrak{m}$. Since $\mathfrak{g}(0)$ has a one-dimensional center, one must have $\tilde{h} = h$. Thus, $h \in [\mathfrak{g}, e]$. □

Theorem 6.2. *Suppose that a Hermitian involution $\sigma = \sigma_1$ has the property that $\mathfrak{g}(0)^e$ is reductive. Then σ_1 can be included in a triad.*

Proof. Using the notation of the previous proof, we set $\mathfrak{k} = \mathfrak{g}(0)^e$ and take (the unique) $f \in \mathfrak{g}(-1)$ such that $h = [e, f]$. Then $\{e, h, f\}$ is an $\mathfrak{sl}_2$-triple, $[e, \mathfrak{g}(-1)] =: \mathfrak{m}$ is a complementary $\mathfrak{k}$-submodule to $\mathfrak{k}$ in $\mathfrak{g}(0)$, and $[e, [e, \mathfrak{g}(-1)]] = \mathfrak{g}(1)$. This also shows that $\mathfrak{g}(-1)$, $\mathfrak{m}$, and $\mathfrak{g}(1)$ are isomorphic $\mathfrak{k}$-modules.

In this case, $\mathfrak{k}$ is the fixed-point subalgebra of an involution of $\mathfrak{g}(0)$ and for this involution the (-1)-eigenspace is $\mathfrak{m}$ (see [Panyushev 1994a, proof of Proposition 3.3]). Let σ_2 denote this involution of $\mathfrak{g}(0)$. Then $\sigma_2(h) = -h$. We extend σ_2 to the whole of $\mathfrak{g}$ by letting $\sigma_2(e) = f$. Then $\sigma_2([x, e]) = [-x, f]$ for all $x \in \mathfrak{m}$, which defines σ_2 on $\mathfrak{g}(1)$ and shows that $\sigma_2(\mathfrak{g}(1)) \subset \mathfrak{g}(-1)$. Clearly, σ_1 and σ_2 commute. Furthermore, σ_1 and σ_2 are different involutions of the three-dimensional simple

subalgebra $\langle e, h, f\rangle$. This implies that σ_1, σ_2, and $\sigma_3 = \sigma_1\sigma_2$ are already conjugate with respect to $\mathrm{PSL}_2 = \mathrm{Aut}\langle e, h, f\rangle$. In particular, $\{\sigma_1, \sigma_2, \sigma_3\}$ is a triad. □

This theorem can be derived from the classification of triads, but our direct construction allows us to visualize the resulting quaternionic decomposition rather explicitly. We have

$$\mathfrak{g} = \begin{array}{ccc} & \mathfrak{k} & \mathfrak{m} \\ & \cdots\cdots\oplus\cdots\cdots & \\ [\mathfrak{m}, e-f] & & [\mathfrak{m}, e+f] \end{array} \quad \sigma_1, \quad \sigma_2 \tag{6-2}$$

Here $h \in \mathfrak{m} = \mathfrak{g}_{01}$, $e + f \in [\mathfrak{m}, e - f] = \mathfrak{g}_{10}$, and $e - f \in [\mathfrak{m}, e + f] = \mathfrak{g}_{11}$. Note also that $\mathfrak{k} \oplus \mathfrak{m} = \mathfrak{g}(0)$ and $[\mathfrak{m}, e - f] \oplus [\mathfrak{m}, e + f] = \mathfrak{g}(1) \oplus \mathfrak{g}(-1)$.

Remark. If $\mathfrak{g}(0)^e$ is not reductive, then such a triad may not exist. For instance, if $\mathfrak{g} = \mathfrak{sl}_{2n}$ and $\mathfrak{g}_0 = \mathfrak{sl}_m \times \mathfrak{sl}_{2n-m} \times \mathfrak{t}_1$ with $n \neq m$ and m odd, then there is no respective triad, see [Vinberg 2005, 3.2].

As is well known, if $\mathfrak{g}(0)^e$ is reductive, then $\mathfrak{g}(-1)$ has a structure of a simple Jordan algebra. Namely, for $x, y \in \mathfrak{g}(-1)$, we set

$$x \circ y = [x, [e, y]] \in \mathfrak{g}(-1).$$

Then $\{\mathfrak{g}(-1), \circ\}$ is a simple Jordan algebra [Tits 1962; Kantor 1964]. (See also [Kac 1980, §4] for possible generalizations). Here $\mathfrak{k} = \mathfrak{g}_{00}$ is the Lie algebra of derivations of $\{\mathfrak{g}(-1), \circ\}$. The triad constructed in Theorem 6.2 is called a *Jordan triad*.

Definition 3. The *commuting variety* of a Jordan algebra $\{\mathcal{J}, \circ\}$ is

$$\mathfrak{C}(\mathcal{J}) = \{(x, y) \mid x \circ y = 0\} \subset \mathcal{J} \times \mathcal{J}.$$

The Jordan triad (6-2) provides a link between the commutator mapping $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{01}$ and the commuting variety of the simple Jordan algebra $\mathfrak{g}(-1)$.

Theorem 6.3. *The commuting variety of the Jordan algebra* $\{\mathfrak{g}(-1), \circ\}$ *is isomorphic to the zero fiber of the commutator mapping* $\varphi : \mathfrak{g}_{10} \times \mathfrak{g}_{11} = [\mathfrak{m}, e - f] \times [\mathfrak{m}, e + f] \to \mathfrak{m} = \mathfrak{g}_{01}$.

Proof. Any element of $\mathfrak{m}$ can uniquely be written as $[x, e]$ with $x \in \mathfrak{g}(-1)$. So, if $[x, e], [y, e] \in \mathfrak{m}$ are arbitrary, then $[[x, e], e - f] \in \mathfrak{g}_{10}$ and $[[y, e], e + f] \in \mathfrak{g}_{11}$ are arbitrary and φ takes the corresponding pair to $\big[[[x, e], e - f], [[y, e], e + f]\big] \in \mathfrak{m} = \mathfrak{g}_{01}$. It is a good exercise in the Jacobi identity to check that

$$\big[[[x, e], e - f], [[y, e], e + f]\big] = 2\big[[[x, e], y], e\big].$$

(One should use the fact that $h=[e,f]$ is the defining element of the short grading. Hence $[[x,e],f]=2x$, etc.) Since $a=[[x,e],y]\in\mathfrak{g}(-1)$ and $\mathfrak{g}^e\cap\mathfrak{g}(-1)=0$, we have $[a,e]=0$ if and only if $a=0$. Therefore,

$$\begin{aligned}([[x,e],e-f],[[y,e],e+f])\in\varphi^{-1}(0) &\iff [[x,e],y]=0\\ &\iff (x,y)\in\mathfrak{E}(\mathfrak{g}(-1)).\end{aligned}\qquad\square$$

If $\mathcal{J}$ is a simple Jordan algebra, then the operator $L_x:\mathcal{J}\to\mathcal{J}$, $L_x(y)=x\circ y$, is invertible for almost all x. Therefore, $\mathcal{J}\times\{0\}$ and $\{0\}\times\mathcal{J}$ are two irreducible components of $\mathfrak{E}(\mathcal{J})$. Clearly, there are some other irreducible components. It is an interesting problem to determine all the components of $\mathfrak{E}(\mathcal{J})$ and their dimensions.

The list of Hermitian involutions leading to Jordan triads and simple Jordan algebras is given in Table 1. We point out the semisimple subalgebra $\mathfrak{s}=[\mathfrak{g}(0),\mathfrak{g}(0)]$ and the structure of $\mathfrak{g}(1)$ as a $\mathfrak{s}$-module. Here the ϖ_i are the fundamental weights of $\mathfrak{s}$.

Remark. The Jordan multiplication in the space Skew_{2n} of usual skew-symmetric matrices is defined as follows. If $A,B,J\in\mathsf{Skew}_{2n}$ and J is nondegenerate, then $A\circ B=\frac{1}{2}(AJB+BJA)$.

There are some coincidences for small n. Namely,

$$\text{Item 1 } (n=1)\simeq\text{Item 2 } (n=1),\qquad \text{Item 1 } (n=2)\simeq\text{Item 4 } (n=3).$$

Furthermore, if $n=1$ in Item 3, then $\mathfrak{g}$ is not simple. This explains the conditions on n given in the last column. For Item 2, the Hermitian involution (of $\mathfrak{sp}_{2n}$) is of maximal rank and the respective Jordan algebra is the algebra Sym_n of symmetric $n\times n$ matrices. Therefore, by Theorems 4.1 and 6.3, the multiplication morphism $\circ:\mathsf{Sym}_n\times\mathsf{Sym}_n\to\mathsf{Sym}_n$ is equidimensional, that is, $\dim\mathfrak{E}(\mathsf{Sym}_n)=\dim\mathsf{Sym}_n=(n^2+n)/2$.

In all other cases, the multiplication morphism $\mathcal{J}\times\mathcal{J}\to\mathcal{J}$ is not equidimensional, see Proposition 6.5. Before checking this, we give an "elementary" explanation for the Jordan algebra of all matrices (Item 1).

	$\mathfrak{g}$	$\mathfrak{s}$	$\mathfrak{g}(1)$	$\mathfrak{k}$	$\mathcal{J}$	
1	$\mathfrak{sl}_{2n}$	$\mathfrak{sl}_n\oplus\mathfrak{sl}_n$	$\mathsf{R}(\varpi_1)\otimes\mathsf{R}(\varpi_1')$	$\mathfrak{sl}_n$	$n\times n$ matrices	$n\geqslant 1$
2	$\mathfrak{sp}_{2n}$	$\mathfrak{sl}_n$	$\mathsf{R}(2\varpi_1)$	$\mathfrak{so}_n$	symmetric $n\times n$ matrices	$n\geqslant 2$
3	$\mathfrak{so}_{4n}$	$\mathfrak{sl}_{2n}$	$\mathsf{R}(\varpi_2)$	$\mathfrak{sp}_{2n}$	skew-symm. $2n\times 2n$ matrices	$n\geqslant 2$
4	$\mathfrak{so}_{n+2}$	$\mathfrak{so}_n$	$\mathsf{R}(\varpi_1)$	$\mathfrak{so}_{n-1}$	spin-factor	$n\geqslant 4$
5	$\mathbf{E}_7$	$\mathbf{E}_6$	$\mathsf{R}(\varpi_1)$	$\mathbf{F}_4$	the Albert algebra	

Table 1. List of Hermitian involutions leading to Jordan triads and simple Jordan algebras.

Example 6.4. Let M be the associative (and also Lie and Jordan) algebra of all $n \times n$ matrices. That is, we exploit the usual matrix product, the Lie bracket $[A, B] = AB - BA$, and the Jordan product $A \circ B = (AB + BA)/2$. Let $\chi(B) = \det(\lambda I - B) = \sum_i \chi_{n-i}(B)\lambda^i$ be the characteristic polynomial of a matrix B. Let $\mathfrak{z}^{\mathrm{J}}(B)$ and $\mathfrak{z}^{\mathrm{Lie}}(B)$ denote the Jordan and Lie centralizers of B, respectively. Consider the subvariety

$$\mathsf{M}^{\langle 2\rangle} = \{B \in \mathsf{M} \mid \chi_{2i+1}(B) = 0 \text{ for all } i\}.$$

It is an irreducible complete intersection and $\operatorname{codim} \mathsf{M}^{\langle 2\rangle} = [n + 1/2]$ (see [Richardson 1987, Lemma 5.3]). We also need the dense open subset $\mathsf{M}^{\mathrm{reg}}$ of regular elements (in the Lie algebra sense) and the subvariety

$$\mathsf{M}^{\mathrm{ev}} = \{B \in \mathsf{M} \mid B \text{ is conjugate to } -B\}.$$

If $B \in \mathsf{M}^{\mathrm{ev}}$ and $ABA^{-1} = -B$, then $A \in \mathfrak{z}^J(B)$ and the mapping $C \in \mathfrak{z}^{\mathrm{Lie}}(B) \mapsto AC \in \mathfrak{z}^{\mathrm{J}}(B)$ is a linear isomorphism. In particular, $\dim \mathfrak{z}^{\mathrm{J}}(B) = \dim \mathfrak{z}^{\mathrm{Lie}}(B)$. The following is clear:

- $\mathsf{M}^{\langle 2\rangle} \cap \mathsf{M}^{\mathrm{reg}} \neq \varnothing$ (it contains a regular nilpotent element).
- $\mathsf{M}^{\mathrm{ev}} \subset \mathsf{M}^{\langle 2\rangle}$ and $\mathsf{M}^{\mathrm{ev}} \cap \mathsf{M}^{\mathrm{reg}} \neq \varnothing$.

Claim. *We have* $\mathsf{M}^{\langle 2\rangle} \cap \mathsf{M}^{\mathrm{reg}} \subset \mathsf{M}^{\mathrm{ev}}$. *In particular*, $\dim \mathfrak{z}^J(B) = n$ *for almost all* $B \in \mathsf{M}^{\langle 2\rangle}$.

Proof. If $B \in \mathsf{M}^{\langle 2\rangle} \cap \mathsf{M}^{\mathrm{reg}}$, then B and $-B$ are both regular and have the same Jordan blocks and the same eigenvalues. Hence B and $-B$ are conjugate. □

Let $\mathfrak{E}^J(\mathsf{M})$ denote the Jordan commuting variety and $p : \mathfrak{E}^J(\mathsf{M}) \to \mathsf{M}$ the projection to the first factor. The previous analysis implies that

$$\dim p^{-1}(\mathsf{M}^{\langle 2\rangle} \cap \mathsf{M}^{\mathrm{reg}}) = \dim \mathsf{M}^{\langle 2\rangle} + n = n^2 + [n/2].$$

Thus, $\dim \mathfrak{E}^J(\mathsf{M}) \geqslant n^2 + [n/2] > \dim \mathsf{M}$. One can prove that this yields an irreducible component of maximal dimension; that is, $\dim \mathfrak{E}^J(\mathsf{M}) = n^2 + [n/2]$.

Table 2 contains information on the restricted root systems associated with Jordan triads. For a Hermitian involution σ, we point out Lie algebras $\mathfrak{g}$, $\mathfrak{h} = \mathfrak{g}^\sigma$, $\mathfrak{g}_{00} = \mathfrak{k}$, the restricted root systems $\Psi(G/H)$ and $\Psi(H/G_{00})$, and the multiplicity of the short roots in $\Psi(G/H)$, denoted m_{short}. For all items in Table 2, the multiplicity of long roots in $\Psi(G/H)$ equals 1 and $\Psi(H/G_{00})$ is embedded in $\Psi(G/H)$ as a subset of *short* roots.

The root system of type $\mathbf{C}_n$ has some short roots that are not roots of $\mathbf{A}_{n-1}$. Therefore, Proposition 5.1 guarantees the existence of a subvariety in $\mathfrak{E}(\mathcal{J})$ of dimension $\dim \mathcal{J} + m_{\mathrm{short}} - 1$, which is larger than the dimension of a generic fiber if $m_{\mathrm{short}} > 1$. However, a clever choice of $\tilde{\mathfrak{c}} \subset \mathfrak{c}_{11}$ (see Remark 5.2(2)) allows us to get a better lower bound on $\dim \mathfrak{E}(\mathcal{J})$:

	$\mathfrak{g}$	$\mathfrak{h}$	$\mathfrak{g}_{00}$	$\Psi(G/H)$	m_{short}	$\Psi(H/G_{00})$
1	$\mathfrak{sl}_{2n}$	$\mathfrak{sl}_n \oplus \mathfrak{sl}_n \oplus \mathfrak{t}_1$	$\mathfrak{sl}_n$	$\mathbf{C}_n$	2	$\mathbf{A}_{n-1}$
2	$\mathfrak{sp}_{2n}$	$\mathfrak{gl}_n$	$\mathfrak{so}_n$	$\mathbf{C}_n$	1	$\mathbf{A}_{n-1}$
3	$\mathfrak{so}_{4n}$	$\mathfrak{gl}_{2n}$	$\mathfrak{sp}_{2n}$	$\mathbf{C}_n$	4	$\mathbf{A}_{n-1}$
4	$\mathfrak{so}_{n+2}$	$\mathfrak{so}_n \oplus \mathfrak{so}_2$	$\mathfrak{so}_{n-1}$	$\mathbf{C}_2$	$n-2$	$\mathbf{A}_1$
5	$\mathbf{E}_7$	$\mathbf{E}_6 \oplus \mathfrak{t}_1$	$\mathbf{F}_4$	$\mathbf{C}_3$	8	$\mathbf{A}_2$

Table 2. Restricted root systems associated with Jordan triads.

Proposition 6.5. *For all items in Table 2, we have*

$$\dim \mathfrak{E}(\mathcal{J}) \geqslant \dim \mathcal{J} + (m_{\text{short}} - 1)[r/2],$$

where r is the rank of $\Psi(G/H)$.

Proof. Using Theorem 6.3, we identify $\mathfrak{E}(\mathcal{J})$ with the zero fiber of the quadratic covariant $\mathfrak{g}_{10} \times \mathfrak{g}_{11} \to \mathfrak{g}_{10}$ and work in the setting of Section 5. Let $\varepsilon_1, \dots, \varepsilon_r$ be the usual basis of $\mathfrak{X}(C_{11}) \otimes \mathbb{Q}$ such that the roots of $\Psi(G/H)$ are $\pm\varepsilon_i \pm \varepsilon_j$ $(i \neq j)$ and $\pm 2\varepsilon_i$. The roots in $\Psi(H/G_{00})$ are $\pm(\varepsilon_i - \varepsilon_j)$. Therefore, $\mathfrak{g}_{10} \oplus \mathfrak{g}_{01}$ is the sum of root spaces corresponding to $\pm(\varepsilon_i + \varepsilon_j)$ and $\pm 2\varepsilon_i$. Set

$$\tilde{\mathfrak{c}} = \left\{ x \in \mathfrak{c}_{11} \;\middle|\; (\varepsilon_i + \varepsilon_{r+1-i})(x) = 0 \text{ for } i = 1, 2, \dots, \left\lceil \frac{r+1}{2} \right\rceil \right\}.$$

Then $\dim \tilde{\mathfrak{c}} = [r/2]$, and we have $2[r/2]$ short roots of $\mathfrak{g}_{10} \oplus \mathfrak{g}_{01}$ vanishing on $\tilde{\mathfrak{c}}$. Moreover, if r is odd, then the long roots $\pm 2\varepsilon_{[r+1/2]}$ also vanish on $\tilde{\mathfrak{c}}$. Therefore,

$$\dim \mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})_{10} = \frac{1}{2} \dim(\mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}}) \cap (\mathfrak{g}_{10} \oplus \mathfrak{g}_{01})) = \begin{cases} m_{\text{short}} \cdot r/2 & \text{if } r \text{ is even,} \\ m_{\text{short}} \cdot [r/2] + 1 & \text{if } r \text{ is odd.} \end{cases}$$

In both cases, this yields $\dim G_{00} \cdot (\mathfrak{z}_{\mathfrak{g}}(\tilde{\mathfrak{c}})_{10} \oplus \tilde{\mathfrak{c}}) = \dim \mathfrak{g}_{11} + (m_{\text{short}} - 1)[r/2]$. □

For the Jordan algebra of all matrices (related to a Hermitian involution of $\mathfrak{sl}_{2n}$), the above construction of $\tilde{\mathfrak{c}}$ gives exactly the subvariety of Example 6.4. It is plausible that the lower bound of Proposition 6.5 provides the exact value of $\dim \mathfrak{E}(\mathcal{J})$.

Remark 6.6. It is curious that, for all Hermitian involutions leading to Jordan triads, the restricted root system is of type $\mathbf{C}_n$; whereas, for all other Hermitian involutions, the restricted root system Ψ is of type $\mathbf{BC}_n$. Namely, the symmetric pairs $\mathfrak{gl}_{n+m} \supset \mathfrak{gl}_n \times \mathfrak{gl}_m \times \mathfrak{t}_1$ $(n < m)$ and $\mathfrak{so}_{4n+2} \supset \mathfrak{gl}_{2n+1}$ lead to $\Psi \simeq \mathbf{BC}_n$; $\mathbf{E}_6 \supset \mathbf{D}_5 \times \mathfrak{t}_1$ leads to $\Psi \simeq \mathbf{BC}_2$.

Appendix: Computations in classical Lie algebras

Here we provide some computations related to the proof of Theorem 4.4 for nilpotent elements in classical Lie algebras.

Let $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_s)$ be a partition and $e \in \mathfrak{gl}_n$ a nilpotent element corresponding to $\boldsymbol{\lambda}$, also denoted by $e \sim \boldsymbol{\lambda}$. Then $\sum \lambda_i = n$ and

$$\dim(\mathfrak{gl}_n)^e = n + 2\sum_{i<j} \min\{\lambda_i, \lambda_j\}, \quad \dim(\mathfrak{sl}_n)^e = \dim(\mathfrak{gl}_n)^e - 1. \tag{A.1}$$

If e is a nilpotent element in $\mathfrak{so}_n$ or $\mathfrak{sp}_{2n}$, with respective parity conditions on $\boldsymbol{\lambda}$, then

$$\dim(\mathfrak{sp}_{2n})^e = \frac{\dim(\mathfrak{gl}_{2n})^e + \#\{i \mid \lambda_i \text{ is odd}\}}{2}, \tag{A.2}$$

$$\dim(\mathfrak{so}_n)^e = \frac{\dim(\mathfrak{gl}_n)^e - \#\{i \mid \lambda_i \text{ is odd}\}}{2}. \tag{A.3}$$

See [Hesselink 1976, (3.8); Kraft and Procesi 1982, 2.4]. Below, we consider several symmetric pairs with classical $\mathfrak{g}$ and check that (4-2) is satisfied for all nonzero nilpotent elements of $\mathfrak{g}_0$. There is no need to consider only noneven nilpotent elements in $\mathfrak{g}_0$, since the computations go through without this assumption.

A.1 $(\mathfrak{g}, \mathfrak{g}_0) = (\mathfrak{sl}_n, \mathfrak{so}_n)$. If $e \in \mathfrak{so}_n$ and $e \sim \boldsymbol{\lambda}$, then using (A.1) and (A.3) yields

$$\dim \mathfrak{g}_0^e = \frac{\dim(\mathfrak{gl}_n)^e - \#\{i \mid \lambda_i \text{ is odd}\}}{2}, \quad \dim \mathfrak{g}_1^e = \frac{\dim(\mathfrak{gl}_n)^e + \#\{i \mid \lambda_i \text{ is odd}\}}{2} - 1.$$

Therefore, $\dim \mathfrak{g}_0^e - \dim \mathfrak{g}_1^e + (n-1) = n - \#\{i \mid \lambda_i \text{ is odd}\}$. Here the parity condition means that each even part of $\boldsymbol{\lambda}$ occurs an even number of times. Since $e \neq 0$, that is, $\boldsymbol{\lambda} \neq (1, \dots, 1)$, the minimal value is 2, and it is attained for $\boldsymbol{\lambda} = (3, 1^{n-3})$.

A.2 $(\mathfrak{g}, \mathfrak{g}_0) = (\mathfrak{sp}_{2n}, \mathfrak{gl}_n)$. If $e \in \mathfrak{gl}_n$ and $e \sim \boldsymbol{\lambda}$, then the partition of e as an element of $\mathfrak{sp}_{2n}$ is obtained by doubling $\boldsymbol{\lambda}$, that is, each part λ_i is replaced with (λ_i, λ_i). Then $\dim \mathfrak{g}_0^e = \dim(\mathfrak{gl}_n)^e$ is given by (A.1), and using (A.2) yields

$$\dim \mathfrak{g}_1^e = 2\sum_i \left[\frac{\lambda_i + 1}{2}\right] + 2\sum_{i<j} \min\{\lambda_i, \lambda_j\}.$$

Hence

$$\dim \mathfrak{g}_0^e - \dim \mathfrak{g}_1^e + n = 2n - 2\sum_i \left[\frac{\lambda_i + 1}{2}\right] = n - \#\{i \mid \lambda_i \text{ is odd}\}.$$

For $e \neq 0$, the minimal value 2 is attained for $\boldsymbol{\lambda} = (2, 1^{n-2})$ or $(3, 1^{n-3})$.

A.3 $(\mathfrak{g}, \mathfrak{g}_0) = (\mathfrak{so}_{2n}, \mathfrak{gl}_n)$. If $e \in \mathfrak{gl}_n$ and $e \sim \boldsymbol{\lambda}$, then $\dim \mathfrak{g}_0^e = \dim(\mathfrak{gl}_n)^e$ is again given by (A.1), using this time (A.3), and we obtain

$$\dim \mathfrak{g}_1^e = 2\sum_i \left[\frac{\lambda_i}{2}\right] + 2\sum_{i<j} \min\{\lambda_i, \lambda_j\}.$$

Hence the result is even better than in the previous case. Indeed, we have here $\dim \mathfrak{g}_0^e - \dim \mathfrak{g}_1^e \geqslant 0$.

A.4 $(\mathfrak{g}, \mathfrak{g}_0) = (\mathfrak{sl}_{n+m}, \mathfrak{sl}_n \times \mathfrak{sl}_m \times \mathfrak{t}_1)$. Here $n, m \geqslant 1$. A nilpotent element $e \in \mathfrak{g}_0$ is determined by two partitions, $e \sim (\boldsymbol{\lambda}; \boldsymbol{\mu}) = ((\lambda_1, \dots, \lambda_k); (\mu_1, \dots, \mu_s))$. Using (A.1), we obtain

$$\dim \mathfrak{g}_0^e = n + m - 1 + 2\sum_{i<j} \min\{\lambda_i, \lambda_j\} + 2\sum_{i<j} \min\{\mu_i, \mu_j\},$$
$$\dim \mathfrak{g}_1^e = 2\sum_{i,j} \min\{\lambda_i, \mu_j\}.$$

Therefore,

$$\dim \mathfrak{g}_0^e - \dim \mathfrak{g}_1^e + (n+m-1) = 2\Big(n + m - 1 + \sum_{i<j} \min\{\lambda_i, \lambda_j\} + \sum_{i<j} \min\{\mu_i, \mu_j\} - \sum_{i,j} \min\{\lambda_i, \mu_j\}\Big).$$

Since $n = \sum_i \lambda_i$, $m = \sum_j \mu_j$, and $\sum_{i<j} \min\{\lambda_i, \lambda_j\} = \sum_{i \geqslant 2}(i-1)\lambda_i$, half of the right-hand side equals

$$\mathcal{F}(\boldsymbol{\lambda}; \boldsymbol{\mu}) := \sum_{i=1}^{k} i\lambda_i + \sum_{j=1}^{s} j\mu_j - 1 - \sum_{i=1}^{k}\sum_{j=1}^{s} \min\{\lambda_i, \mu_j\}.$$

Arguing by induction, we prove that $\mathcal{F}(\boldsymbol{\lambda}; \boldsymbol{\mu}) \geqslant 0$ for all $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$, and if $n + m \geqslant 3$, then $\mathcal{F}(\boldsymbol{\lambda}; \boldsymbol{\mu}) > 0$.

(1) First, $\mathcal{F}(1^n; 1^m) = (n-m)^2/2 + (n+m)/2 - 1$, which is positive if $(n, m) \neq (1, 1)$.

(2) The inequality is easily verified, if $\boldsymbol{\lambda}$ or $\boldsymbol{\mu}$ consists of only one part.

(3) Suppose that $k \geqslant 2$ and $s \geqslant 2$. Write $\boldsymbol{\lambda} = (\lambda_1, \boldsymbol{\lambda}')$ and $\boldsymbol{\mu} = (\mu_1, \boldsymbol{\mu}')$. Then

$$\mathcal{F}(\boldsymbol{\lambda}; \boldsymbol{\mu}) = \mathcal{F}(\boldsymbol{\lambda}'; \boldsymbol{\mu}') + \max\{\lambda_1, \mu_1\} + \sum_{i \geqslant 2}(\lambda_i - \min\{\lambda_i, \mu_1\}) + \sum_{j \geqslant 2}(\mu_j - \min\{\lambda_1, \mu_j\})$$
$$\geqslant \mathcal{F}(\boldsymbol{\lambda}'; \boldsymbol{\mu}') + \max\{\lambda_1, \mu_1\} \geqslant \max\{\lambda_1, \mu_1\}.$$

Here $\max\{\lambda_1, \mu_1\}$ arises as $\lambda_1 + \mu_1 - \min\{\lambda_1, \mu_1\}$.

We omit the computations related to the remaining classical symmetric pairs $(\mathfrak{sl}_{2n}, \mathfrak{sp}_{2n})$, $(\mathfrak{sp}_{2n+2m}, \mathfrak{sp}_{2n} \times \mathfrak{sp}_{2m})$, and $(\mathfrak{so}_{n+m}, \mathfrak{so}_n \times \mathfrak{so}_m)$.

Acknowledgements

Part of this work was done while I was visiting the Max-Planck-Institut für Mathematik (Bonn).

References

[Antonyan 1982] L. V. Antonyan, "О классификации однородных элементов $\mathbb{Z}_2$-градуированных полупростых алгебр Ли", *Vestnik Moskov. Univ. Ser. I Mat. Mekh.* 2 (1982), 29–34. Translated as "Classification of homogeneous elements of $\mathbb{Z}_2$-graded semisimple Lie algebras" in *Moscow Univ. Math. Bulletin*, **37**:2 (1982), 36–43. MR 84c:17006 Zbl 0494.17008

[Brion 2000] M. Brion, "Invariants et covariants des groupes algébriques réductifs", pp. 83–168 in *Théorie des invariants et géométrie des variétés quotients* (Monastir, 1996), edited by G. W. Schwarz and M. Brion, Travaux en Cours **61**, Hermann, Paris, 2000. Zbl 1095.14003

[Bulois 2011] M. Bulois, "Irregular locus of the commuting variety of reductive symmetric Lie algebras and rigid pairs", *Transform. Groups* **16**:4 (2011), 1027–1061. MR 2012i:14061 Zbl 06031650

[Dynkin 1952] E. B. Dynkin, "Полупростые подалгебры полупростых алгебр Ли", *Mat. Sbornik* (*N.S.*) **30(72)** (1952), 349–462. Translated as "Semisimple subalgebras of semisimple Lie algebras", pp. 111–244 in *Five papers on algebra and group theory* by E. B. Dynkin et al., Amer. Math. Soc. Transl. (2) **6**, Amer. Math. Soc., Providence, RI, 1957 (see also [Dynkin 2000, pp. 175–308]). MR 13,904c Zbl 0048.01701

[Dynkin 2000] E. B. Dynkin, *Selected papers of E. B. Dynkin with commentary*, edited by A. A. Yushkevich et al., Amer. Math. Soc., Providence, RI, 2000. MR 2001g:01050 Zbl 1056.01014

[Helgason 1978] S. Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Pure and Applied Mathematics **80**, Academic Press, New York, 1978. MR 80k:53081 Zbl 0451.53038

[Hesselink 1976] W. H. Hesselink, "Singularities in the nilpotent scheme of a classical group", *Trans. Amer. Math. Soc.* **222** (1976), 1–32. MR 55 #2885 Zbl 0332.14017

[Kac 1980] V. G. Kac, "Some remarks on nilpotent orbits", *J. Algebra* **64**:1 (1980), 190–213. MR 81i:17005 Zbl 0431.17007

[Kantor 1964] I. L. Kantor, "Классификация неприводимых транзитивно-дифференциальных групп", *Dokl. Akad. Nauk SSSR* **158**:6 (1964), 1271–1274. Translated as "Classification of irreducible transitively differential groups" in *Sov. Math. Dokl.* **5** (1965), 1404–1407. MR 31 #217 Zbl 0286.17011

[Kollross 2009] A. Kollross, "Exceptional $\mathbb{Z}_2 \times \mathbb{Z}_2$-symmetric spaces", *Pacific J. Math.* **242**:1 (2009), 113–130. MR 2010j:17023 Zbl 1184.53056

[Kostant and Rallis 1971] B. Kostant and S. Rallis, "Orbits and representations associated with symmetric spaces", *Amer. J. Math.* **93** (1971), 753–809. MR 47 #399 Zbl 0224.22013

[Kraft and Procesi 1982] H. Kraft and C. Procesi, "On the geometry of conjugacy classes in classical groups", *Comment. Math. Helv.* **57**:4 (1982), 539–602. MR 85b:14065 Zbl 0511.14023

[Panyushev 1994a] D. I. Panyushev, "Complexity and nilpotent orbits", *Manuscripta Math.* **83**:3-4 (1994), 223–237. MR 95e:14039 Zbl 0822.14024

[Panyushev 1994b] D. I. Panyushev, "The Jacobian modules of a representation of a Lie algebra and geometry of commuting varieties", *Compositio Math.* **94**:2 (1994), 181–199. MR 95m:14030 Zbl 0834.17003

[Panyushev 1999] D. I. Panyushev, "On the conormal bundle of a G-stable subvariety", *Manuscripta Math.* **99**:2 (1999), 185–202. MR 2000e:14081 Zbl 0961.14030

[Panyushev 2013] D. I. Panyushev, "Commuting involutions and degenerations of isotropy representations", *Transform. Groups* **18**:2 (2013), 507–537. MR 3055775

[Panyushev and Yakimova 2007] D. I. Panyushev and O. Yakimova, "Symmetric pairs and associated commuting varieties", *Math. Proc. Cambridge Philos. Soc.* **143**:2 (2007), 307–321. MR 2008k:14090 Zbl 1126.17010

[Premet 2003] A. Premet, "Nilpotent commuting varieties of reductive Lie algebras", *Invent. Math.* **154**:3 (2003), 653–683. MR 2004k:20090 Zbl 1068.17006

[Richardson 1979] R. W. Richardson, "Commuting varieties of semisimple Lie algebras and algebraic groups", *Compositio Math.* **38**:3 (1979), 311–327. MR 80c:17009 Zbl 0409.17006

[Richardson 1981] R. W. Richardson, "An application of the Serre conjecture to semisimple algebraic groups", pp. 141–151 in *Algebra, Carbondale 1980: Lie algebras, group theory, and partially ordered algebraic structures* (Carbondale, IL, 1980), edited by R. K. Amayo, Lecture Notes in Math. **848**, Springer, Berlin, 1981. MR 83j:20047 Zbl 0457.14022

[Richardson 1982] R. W. Richardson, "On orbits of algebraic groups and Lie groups", *Bull. Austral. Math. Soc.* **25**:1 (1982), 1–28. MR 83i:14041 Zbl 0467.14008

[Richardson 1987] R. W. Richardson, "Normality of G-stable subvarieties of a semisimple Lie algebra", pp. 243–264 in *Algebraic groups* (Utrecht, 1986), edited by A. M. Cohen et al., Lecture Notes in Math. **1271**, Springer, Berlin, 1987. MR 90d:14052 Zbl 0632.14011

[Tits 1962] J. Tits, "Une classe d'algèbres de Lie en rélation avec les algèbres de Jordan", *Nederl. Akad. Wetensch. Proc.* (*A*) **65** (1962), 530–535. MR 26 #3753 Zbl 0104.26002

[Vasconcelos 1994] W. V. Vasconcelos, *Arithmetic of blowup algebras*, London Mathematical Society Lecture Note Series **195**, Cambridge University Press, 1994. MR 95g:13005 Zbl 0813.13008

[Vergne 1995] M. Vergne, "Instantons et correspondance de Kostant–Sekiguchi", *C. R. Acad. Sci. Paris* (*I*) *Math.* **320**:8 (1995), 901–906. MR 96c:22026 Zbl 0833.22010

[Vinberg 1976] È. B. Vinberg, "Группа Вейля градуированной алгебры Ли", *Izv. Akad. Nauk SSSR Ser. Mat.* **40**:3 (1976), 488–526. Translated as "The Weyl group of a graded Lie algebra" in *Math. USSR-Izv.* **10** (1976), 463–495. MR 55 #3175 Zbl 0363.20035

[Vinberg 1979] È. B. Vinberg, "Классификация однородных нильпотентных элементов полупростой градуированной алгебры Ли", *Trudy Sem. Vektor. Tenzor. Anal.* 19 (1979), 155–177. Translated as "Classification of homogeneous nilpotent elements of a semisimple graded Lie algebra" in *Selecta Math. Sov.* **6** (1987), 15–35. MR 80k:17006 Zbl 0431.17006

[Vinberg 2005] È. B. Vinberg, "Short SO_3-structures on simple Lie algebras and associated quasielliptic planes", pp. 243–270 in *Lie groups and invariant theory*, edited by È. B. Vinberg, Amer. Math. Soc. Transl. (2) **213**, Amer. Math. Soc., Providence, RI, 2005. MR 2006d:17008 Zbl 1081.17009

Communicated by J. Toby Stafford
Received 2012-09-19 Accepted 2013-01-24

panyushev@iitp.ru *Dobrushin Mathematics Laboratory, Institute for Information Transmission Problems, Russian Academy of Sciences, Bolshoy Karetny per. 19, Moscow, 127994, Russia*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 7 No. 6 2013