Coregular spaces and genus one curves

Manjul Bhargava[*] and Wei Ho[†]

A coregular space is a representation of an algebraic group for which the ring of polynomial invariants is freely generated. We show that the orbits of many coregular irreducible representations of algebraic groups where the number of generating invariants is at least two, over a (not necessarily algebraically closed) field k, correspond to genus one curves over k together with line bundles, vector bundles, and/or points on their Jacobian curves. In particular, we give explicit descriptions of certain moduli spaces of genus one curves with extra structure as quotients by algebraic groups of open subsets of affine spaces.

In most cases, we also describe how the generators of the invariant rings are geometrically manifested, often as coefficients for the Jacobian families of elliptic curves for the genus one curves. We also show how many of the correspondences, including their proofs, are special cases of two general constructions related to Hermitian matrices and cubic Jordan algebras.

In forthcoming work, we use these orbit parametrizations to determine the average sizes of Selmer groups for various families of elliptic curves.

1. Introduction

In 1963, Birch and Swinnerton-Dyer [BSD63] carried out a seminal study of the moduli space of genus one curves equipped with degree 2 line bundles, in terms of the orbits of the action of GL_2 on the space $\mathrm{Sym}^4(2)$ of binary quartic forms. This orbit space parametrization was a key ingredient in the explicit 2-descent computations that led them to the celebrated Birch and Swinnerton-Dyer conjecture. The analogues of this parametrization for line bundles of degree 3, 4, and 5 (i.e., "elliptic normal curves" of degrees 3, 4, and 5) were subsequently investigated in the important works of Cassels [Cas62], and more recently, Cremona [Cre99], Cremona–Fisher–Stoll [CFS10], and Fisher [Fis10]. These works have, in particular, enabled explicit 3-, 4-, and 5-descent computations on elliptic curves analogous to the original 2-descent computations of Birch and Swinnerton-Dyer. Recently, these parametrizations of elliptic normal curves have also been used to obtain bounds on the average rank and Selmer ranks of elliptic curves (see [BS15a, BS15b]).

   The important consequences and the elegance of these classical orbit parametrizations naturally raise the question as to whether further such correspondences exist that could shed light on other data attached to genus one curves. The purpose of this article is to develop additional such correspondences. In fact, we will show that the classical representations described

above for elliptic normal curves are only four among at least 20 such representations whose orbits parametrize nontrivial data on genus one curves—such as line bundles, vector bundles, points on the Jacobian, as well as more exotic structures.

The underlying philosophy is the use of orbit spaces to parametrize algebraic or geometric objects. In 1801, Gauss gave perhaps the first nontrivial example of such a parametrization in his celebrated Disquisitiones Arithmeticae [Gau01], where he studied integral binary quadratic forms under a certain action of the group $GL_2(\mathbb{Z})$. Although the space of binary quadratic forms is a *prehomogeneous vector space*, meaning that it has only one open orbit over $\mathbb{C}$, the rational and especially the integral orbits are in bijection with quite nontrivial arithmetic objects, namely, quadratic fields and ideal classes in quadratic rings, respectively.

In [WY92], Wright and Yukie showed that orbits of many prehomogeneous vector spaces over a field k correspond to field extensions of k. The series of papers [Bha04a, Bha04b, Bha04c, Bha08, Bha] describes how the integral orbits of most prehomogeneous vector spaces parametrize arithmetic objects, such as rings of low rank together with ideals and modules. These parametrizations were used in [Bha05, Bha10], for example, to determine the density of discriminants of quartic and quintic fields, thus completing the original program of Wright and Yukie (see [WY92, §1]) of using prehomogeneous representations to determine densities of arithmetic objects.

It is natural to ask whether representations having more than one invariant might also similarly lead to parametrizations of arithmetic interest. In this paper, we study a natural series of *coregular* representations, that is, representations for which the ring of relative invariants is a polynomial ring (an example is the space of binary quartic forms). We show that the orbits of "most" such coregular representations of semisimple groups that have more than one generating invariant—i.e., are not prehomogeneous—parametrize data involving *genus one curves*, thus extending the aforementioned work of Birch and Swinnerton-Dyer.

Just as the space of $2 \times 2 \times 2$ cubes and $2 \times 3 \times 3$ boxes played a central role in the study of prehomogeneous vector spaces [Bha04a, Bha04b], here the spaces of $2 \times 2 \times 2 \times 2$ hypercubes and $3 \times 3 \times 3$ cubes play a central role in the theory, from which we are then able to derive various other irreducible coregular spaces corresponding to genus one curves via suitable invariant-theoretic procedures. Also, analogous to the prehomogeneous cases, the invariant theory of our spaces plays a crucial role in constructing and describing the corresponding geometric data. Indeed, in many cases, our bijections yield natural geometric interpretations for the generators of

the invariant ring. While there are many similarities between the prehomogeneous cases and the coregular cases, e.g., the interpretation of certain representations as spaces of "boxes", in most cases the ideas required to prove these parametrizations and construct the invariants are new.

A summary of the parametrizations we obtain is provided in Table 1. In this table, the first and second columns list the representations in question; for simplicity, we list a semisimple group G^{ss}, which has a map to the desired group G (with finite kernel and solvable cokernel), since some of the actions of the relevant groups are not completely standard. The third column lists the geometric data (up to isomorphism) arising from a general orbit of this representation: the data in every case includes a genus one curve C. The curve may also be equipped with line bundles, denoted by L_d, L'_d, L''_d, etc., where d is the degree of the line bundle, or with a vector bundle, denoted by $M_{r,d}$, where r is the rank and d is the degree of the vector bundle. The notation P or P' indicates a rational point on the Jacobian of C (often in a certain arithmetic subgroup of $\mathrm{Jac}(C)$), and P_e indicates that the point is a nontrivial rational torsion point of order e. The notation $\sim$ indicates that the data on the two sides are equivalent and are both suitable interpretations for the moduli problem. There may be some additional mild (open) conditions on the geometric data not indicated in column three. The fourth column gives the degrees of the invariants of the representation of the semisimple group, and the fifth contains the extended or affine Dynkin diagram associated with the representation (see Section 7). Finally, the sixth column indicates the subsection in which that case is proved and/or discussed most carefully, although most of the theorems are previewed in Sections 2 and 3. Note that in many cases, changing the form of the group over K leads to a twisted version of the geometric data in column three.

For example, line 3 of Table 1 corresponds to the case of $2 \times 2 \times 2 \times 2$ hypercubical matrices over a field K ($\mathrm{char}(K) \neq 2, 3$). We show that the nondegenerate $\mathrm{GL}_2(K)^4$-orbits of $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ correspond to the data (C, L, P, P'), where: C is a genus one curve over K; L is a degree 2 line bundle on C; and P and P' are non-identity K-points in a certain arithmetic subgroup of the Jacobian of C. (More symmetrically, we in fact recover three non-identity points P, P', and P'' that sum to zero.) Meanwhile, the ring of polynomial invariants for the action of $\mathrm{SL}_2(K)^4$ on $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ is freely generated by four invariants a_2, a_4, a'_4, and a_6, having degrees 2, 4, 4, and 6, respectively. In terms of the geometric data, if we write the Jacobian of C as a Weierstrass elliptic curve $y^2 = x^3 + Ax + B$ on which the points P, P', P'' lie, then: a_2 can be interpreted as the slope of the line connecting

	Group (s.s.)	Representation	Geometric Data	Invariants	Dynkin	§
1.	SL_2	$\mathrm{Sym}^4(2)$	(C, L_2)	$2,3$	$A_2^{(2)}$	4.1
2.	SL_2^2	$\mathrm{Sym}^2(2) \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L_2') \sim (C, L_2, P)$	$2,3,4$	$D_3^{(2)}$	6.1
3.	SL_2^4	$2 \otimes 2 \otimes 2 \otimes 2$	$(C, L_2, L_2', L_2'') \sim (C, L_2, P, P')$	$2,4,4,6$	$D_4^{(1)}$	6.2
4.	SL_2^3	$2 \otimes 2 \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L_2') \sim (C, L_2, P)$	$2,4,6$	$B_3^{(1)}$	6.3.1
5.	SL_2^2	$\mathrm{Sym}^2(2) \otimes \mathrm{Sym}^2(2)$	$(C, L_2, L_2') \sim (C, L_2, P)$	$2,3,4$	$D_3^{(2)}$	6.3.3
6.	SL_2^2	$2 \otimes \mathrm{Sym}^3(2)$	(C, L_2, P_3)	$2,6$	$G_2^{(1)}$	6.3.2
7.	SL_2	$\mathrm{Sym}^4(2)$	(C, L_2, P_3)	$2,3$	$A_2^{(2)}$	6.3.4
8.	$\mathrm{SL}_2^2 \times \mathrm{SL}_4$	$2 \otimes 2 \otimes \wedge^2(4)$	$(C, L_2, M_{2,4})$	$2,4,6,8$	$D_5^{(1)}$	6.6.1
9.	$\mathrm{SL}_2 \times \mathrm{SL}_6$	$2 \otimes \wedge^3(6)$	$(C, L_2, M_{3,6})$ with $L^{\otimes 3} \cong \det M$	$2,6,8,12$	$E_6^{(1)}$	6.6.2
10.	$\mathrm{SL}_2 \times \mathrm{Sp}_6$	$2 \otimes \wedge_0^3(6)$	$(C, L_2, (M_{3,6}, \varphi))$ with $L^{\otimes 3} \cong \det M$	$2,6,8,12$	$E_6^{(2)}$	6.6.3
11.	$\mathrm{SL}_2 \times \mathrm{Spin}_{12}$	$2 \otimes S^+(32)$	$(C \to \mathbb{P}^1(\mathscr{H}_3(\mathbb{H})), L_2)$	$2,6,8,12$	$E_7^{(1)}$	6.6.3
12.	$\mathrm{SL}_2 \times E_7$	$2 \otimes 56$	$(C \to \mathbb{P}^1(\mathscr{H}_3(\mathbb{O})), L_2)$	$2,6,8,12$	$E_8^{(1)}$	6.6.3
13.	SL_3	$\mathrm{Sym}^3(3)$	(C, L_3)	$4,6$	$D_4^{(3)}$	4.2
14.	SL_3^3	$3 \otimes 3 \otimes 3$	$(C, L_3, L_3') \sim (C, L_3, P)$	$6,9,12$	$E_6^{(1)}$	5.1
15.	SL_3^2	$3 \otimes \mathrm{Sym}^2(3)$	(C, L_3, P_2)	$6,12$	$F_4^{(1)}$	5.2.1
16.	SL_3	$\mathrm{Sym}^3(3)$	(C, L_3, P_2)	$4,6$	$D_4^{(3)}$	5.2.2
17.	$\mathrm{SL}_3 \times \mathrm{SL}_6$	$3 \otimes \wedge^2(6)$	$(C, L_3, M_{2,6})$ with $L^{\otimes 2} \cong \det M$	$6,12,18$	$E_7^{(1)}$	5.5
18.	$\mathrm{SL}_3 \times E_6$	$3 \otimes 27$	$(C \hookrightarrow \mathbb{P}^2(\mathbb{O}), L_3)$	$6,12,18$	$E_8^{(1)}$	5.4
19.	$\mathrm{SL}_2 \times \mathrm{SL}_4$	$2 \otimes \mathrm{Sym}^2(4)$	(C, L_4)	$8,12$	$E_6^{(2)}$	4.3
20.	$\mathrm{SL}_5 \times \mathrm{SL}_5$	$\wedge^2(5) \otimes 5$	(C, L_5)	$20,30$	$E_8^{(1)}$	4.4

Table 1: Table of coregular representations and their moduli interpretations

P, P' and P''; a_4 and a_4' are the x-coordinates of the points P and P'; and a_6 is the y-coordinate of P.

Similarly, line 14 of Table 1 corresponds to the case of $\mathrm{GL}_3(K)^3$ acting on the space $K^3 \otimes K^3 \otimes K^3$ of $3 \times 3 \times 3$ cubical matrices over K. We prove that the nondegenerate orbits parametrize data consisting of a triple (C, L, P), where C is a genus one curve over K, L is a degree 3 line bundle on C defined over K, and P is a non-identity point in an arithmetic subgroup of the Jacobian of C. The three generators b_6, b_9, and b_{12} of the $\mathrm{SL}_3(K)^3$-invariant ring have degrees 6, 9, and 12, respectively. If we again write the Jacobian of C as a Weierstrass elliptic curve $y^2 = x^3 + Ax + B$, then $P = (b_6, b_9)$ and $A = b_{12}$.

In both of these examples, we introduce new methods to construct and interpret the invariants. In particular, there are certain noncommutative diagrams (see §2.3.4 and §3.2.3) that play a crucial role in understanding the invariant theory and describing these moduli spaces.

We briefly describe some forthcoming applications of these parametrizations. In [BS15a, BS15b], an implementation of certain geometric counting techniques (building on those in [Bha10]) for integral orbits of the representations in lines 1 and 13 of Table 1 has led to results on the average sizes of the 2- and 3-Selmer groups of the family of all elliptic curves over $\mathbb{Q}$ (when ordered by height), and corresponding (finite) upper bounds on the average rank of all elliptic curves. By developing these counting techniques further, so that they may be applied to other cases in Table 1, we determine in [BH12] the average sizes of the 2- and 3-Selmer groups for various families of elliptic curves, e.g., those with marked points. These results lead to corresponding average rank bounds for the curves in these families. For example, the space of $3 \times 3 \times 3$ cubes allows us to show that the average size of the 3-Selmer group in the family of elliptic curves

$$y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x$$

having a marked point at $(0,0)$ is 12. As a result, we show that the (limsup of the) average rank of this family of elliptic curves is finite (indeed, at most $2\frac{1}{6}$), and that a positive proportion of curves in this family have rank one. Analogous results for average sizes of Selmer groups in families of elliptic curves with one marked point of order 3 or 2 (using lines 6 and 15, respectively, of Table 1) and elliptic curves with two general marked points (using line 3, the space of hypercubes) are also obtained.

Outline. The organization of this paper is as follows. Sections 2 and 3 form an extended introduction in which we describe the basic constructions and

parametrizations corresponding to $2 \times 2 \times 2 \times 2$ hypercubes and $3 \times 3 \times 3$ cubes, respectively, and how many of the various other coregular space orbit parametrizations in Table 1 may be (at least heuristically) derived from them. These introductory sections also highlight the relationship between the constructions in this paper and previous work.

Section 4 describes orbit parametrizations for the moduli spaces of genus one curves with degree n line bundles, for $2 \leq n \leq 5$. Many of the ideas in this section are classical or well known, at least over algebraically closed fields, but our constructions generalize to other fields and more general base schemes. We also show that the stabilizers of elements in these representations are naturally isomorphic to the automorphism group of a genus one curve with a degree n line bundle, which is related to the so-called Heisenberg theta group. These results about stabilizers play a central role in the works [BS15a, BS15b]. The parametrizations of elliptic normal curves of degree n, especially for $n = 2$ and $n = 3$, will also be used extensively in the later parts of the paper.

In Section 5, we concentrate on the coregular spaces whose orbits are related to a genus one curve and a degree 3 line bundle, possibly with additional data. We first discuss some of the fundamental cases, such as the aforementioned space of $3 \times 3 \times 3$ cubical matrices. In each case, we construct the invariants of the representation, and show that they are closely related to the geometric data, and in particular, to the Jacobian of the genus one curve that arises.

We then study spaces of the form $V \otimes J$, where V is a 3-dimensional vector space and J is a certain type of cubic Jordan algebra (to be specified), up to the natural action of a group which we denote by $\mathrm{GL}(V) \times \mathrm{SL}(J)$. In each case, the group $(\mathbb{G}_m \times)\mathrm{SL}(J)$ acting on J is a prehomogeneous vector space, equipped with a relative invariant cubic norm form and an adjoint map. We prove a *uniform* theorem about the orbits of these type of representations, by stratifying the elements of the Jordan algebras geometrically (using ideas from the theory of cubic Jordan algebras, representation theory, and algebraic geometry, especially the tangent and secant varieties of Severi varieties). We then specialize to specific J to recover a number of the introductory cases as well as other interesting moduli problems.

Section 6 develops further ideas in order to study orbits that parametrize genus one curves with degree 2 line bundles and additional data. We begin by discussing the most fundamental representations, including the space of bidegree $(2, 2)$ forms on $\mathbb{P}^1 \times \mathbb{P}^1$ and the aforementioned space of $2 \times 2 \times 2 \times 2$ hypercubical matrices. We show that the invariants of each representation are again closely related to the corresponding geometric data.

As in the case of degree 3 line bundles, we then study a more general situation. In particular, we consider the tensor product of a two-dimensional vector space V and a space $\mathscr{C}(J)$ of "Hermitian cubes" with respect to a cubic Jordan algebra J, under the action of a group which we denote by $\mathrm{SL}_2(V) \times \mathrm{SL}_2(J)$; the space $\mathscr{C}(J)$ has a quartic norm form and a natural adjoint map. Again, we study representations of this kind uniformly by understanding these spaces $\mathscr{C}(J)$ geometrically; the algebraic geometry required here is slightly more technical than in §5, partly because the relevant genus one curves are naturally double covers of the projective line instead of curves embedded in the projective plane. Specializing to specific $\mathscr{C}(J)$ then recovers many of the earlier fundamental cases as well as several new moduli problems.

In Section 7, we describe how all of the representations we study are related to exceptional Lie algebras. In particular, these representations all arise from Vinberg's theory of θ-groups [Vin76]; his constructions give a wide class of coregular spaces. In his recent Harvard Ph.D. thesis, J. Thorne [Tho12] studies some canonical constructions in invariant theory arising from Vinberg theory, and it is thus an interesting question as to how his more representation-theoretic constructions are related to our geometric ones. Finally, we also describe how our spaces are closely related to the representations found in the Deligne-Gross Magic Triangle [DG02].

The "certain arithmetic subgroup" of the Jacobian of the genus one curve C arising in many of our moduli problems is the group $\mathrm{Pic}^0(C)$ of degree 0 divisors or line bundles (up to equivalence) on C. When working over an algebraically closed field, it is isomorphic to the group of rational points of the entire Jacobian, but in general, when working over number fields, it is a finite-index subgroup of the Jacobian, whose rational points correspond to all rational degree 0 divisor classes.

2. Main results I: Genus one curves and $2 \times 2 \times 2 \times 2$ hypercubes

In this section, we discuss the space of $2 \times 2 \times 2 \times 2$ hypercubical matrices over K, and we describe the various parametrizations of genus one curves

with extra data that may be obtained from this perspective. No proofs or details are given in this section. Here, we simply describe in an elementary way the constructions of the genus one curves and extra data from the orbits of our representations, and state the main theorems related to these cases. Further details, more functorial descriptions of the constructions, and proofs may be found in Section 6.

2.1. Preliminaries on $2 \times 2 \times 2$ cubes

Before studying $2 \times 2 \times 2 \times 2$ hypercubical matrices, we first review the case of $2 \times 2 \times 2$ cubical matrices (see [Bha04a] for more details).

Let K be a field with char$(K) \neq 2$. Let $\mathcal{C}_2(K)$ denote the space $K^2 \otimes K^2 \otimes K^2$. Then each element of $\mathcal{C}_2(K)$ can naturally be represented as a cubical matrix $A = (a_{ijk})$ with entries in K, where $i, j, k \in \{1, 2\}$:

(1)

$$
\begin{array}{ccc}
 & a_{211} \text{———} a_{212} & \\
 & \diagup \quad | \qquad \diagup \quad | & \\
a_{111} \text{———} a_{112} & & \\
| \qquad | \qquad | \qquad | & & \\
 & a_{221} \text{———} a_{222} & \\
 & \diagup \qquad \diagup & \\
a_{121} \text{———} a_{122} & &
\end{array}
\quad .
$$

If we denote by $\{e_1, e_2\}$ the standard basis of K^2, then the element of $\mathcal{C}_2(K)$ described by (1) is

$$
\sum_{i,j,k} a_{ijk} \, e_i \otimes e_j \otimes e_k.
$$

As the cubical matrix representation is both more intuitive and more convenient, we shall identify $\mathcal{C}_2(K)$ with the space of $2 \times 2 \times 2$ matrices with entries in K, or the space of *cubes over K*.

Now a cube A over K may be naturally sliced into two 2×2 matrices over K in three different ways. Namely, the cube $A = (a_{ijk})$ given by (1) may be partitioned into the two 2×2 matrices M_ℓ and N_ℓ, for $\ell = 1, 2, 3$, as follows:

1) $M_1 = (a_{1jk})$ is the front face and $N_1 = (a_{2jk})$ is the back face of A;
2) $M_2 = (a_{i1k})$ is the top face and $N_2 = (a_{i2k})$ is the bottom face of A;
3) $M_3 = (a_{ij1})$ is the left face and $N_3 = (a_{ij2})$ is the right face of A.

We may consider the natural action of $\mathrm{SL}_2(K)^3$ on the tensor product $\mathcal{C}_2(K)$, namely for any $\ell \in \{1, 2, 3\}$, the element $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ in the ℓth factor of $\mathrm{SL}_2(K)^3$ acts on the cube A by replacing (M_ℓ, N_ℓ) by $(rM_\ell + sN_\ell, tM_\ell + uN_\ell)$. The actions of these three factors of $\mathrm{SL}_2(K)$ in $\mathrm{SL}_2(K)^3$ commute with each other, analogous to the fact that row and column operations on a rectangular matrix commute. Hence we obtain a natural and well-defined action of $\mathrm{SL}_2(K)^3$ on $\mathcal{C}_2(K)$.

This action turns out to have a single polynomial invariant[1], which we call the *discriminant*. Given a $2 \times 2 \times 2$ cube A over K, for each $\ell \in \{1, 2, 3\}$, we obtain a binary quadratic form

$$(2) \qquad Q_\ell(x, y) = \det(M_\ell x + N_\ell y).$$

The discriminants of these three binary quadratic forms all coincide (see [Bha04a, §2]), and this gives the desired invariant, called the discriminant $\mathrm{disc}(A)$ of the cube A. (These triples of binary quadratic forms with the same discriminant arising from cubes were used to give a simple description of Gauss composition in [Bha04a].) This fundamental invariant of degree four on the space $K^2 \otimes K^2 \otimes K^2$ of cubical matrices over K will play a key role in understanding the next space $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ of hypercubical matrices over K.

2.2. On $2 \times 2 \times 2 \times 2$ hypercubes

Assuming now that K has characteristic not 2 or 3, let $\mathcal{H}_2(K)$ denote the space $K^2 \otimes K^2 \otimes K^2 \otimes K^2$. Then we may identify $\mathcal{H}_2(K)$ with the space of $2 \times 2 \times 2 \times 2$ hypercubical matrices $H = (h_{ijk\ell})$ over K, which we will call the space of *hypercubes over K*. Such hypercubes are somewhat harder to draw on paper; breaking symmetry, we write our hypercube $H = (h_{ijk\ell})$ thus:

(3)

---

[1] We use throughout the standard abuse of terminology "has a single polynomial invariant" (or "has k polynomial invariants") to mean that the corresponding polynomial invariant ring is generated freely by one element (respectively, k elements).

Now just as a cube A over K could be partitioned into two 2×2 matrices in three different ways, a hypercube H over K may be partitioned into two $2 \times 2 \times 2$ matrices in four different ways. More precisely, the hypercube $H = (h_{ijk\ell})$ can be partitioned into two cubes A_m and B_m, for $m \in \{1, 2, 3, 4\}$, as follows:

1) $A_1 = (h_{1jk\ell})$ and $B_1 = (h_{2jk\ell})$;
2) $A_2 = (h_{i1k\ell})$ and $B_2 = (h_{i2k\ell})$;
3) $A_3 = (h_{ij1\ell})$ and $B_3 = (h_{ij2\ell})$;
4) $A_4 = (h_{ijk1})$ and $B_4 = (h_{ijk2})$,

where the first slicing 1) is depicted in (3).

We define a natural action of $\mathrm{SL}_2(K)^4$ on the space of hypercubes so that, for any $i \in \{1, 2, 3, 4\}$, an element $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ in the ith factor of $\mathrm{SL}_2(K)$ acts on the hypercube H by replacing (A_i, B_i) by $(rA_i + sB_i, tA_i + uB_i)$. The actions of these four factors of $\mathrm{SL}_2(K)$ in $\mathrm{SL}_2(K)^4$ again commute with each other, so we obtain a well-defined action of $\mathrm{SL}_2(K)^4$ on $\mathcal{H}_2(K)$.

Now recall that a cube over K naturally yields three binary quadratic forms over K, through its slicings into pairs of 2×2 matrices over K. Namely, for each slicing of a cube A into a pair (M_i, N_i) of 2×2 matrices, we may construct the form $Q_i(x, y) = \det(M_i x + N_i y)$. As is well-known, the determinant function is the unique polynomial invariant for the action of $\mathrm{SL}_2(K)^2$ on 2×2 matrices over K, and since it a degree two invariant, we obtain binary quadratic forms.

Analogously, a hypercube over K naturally yields four binary *quartic* forms via its slicings into pairs of cubes over K. Indeed, we have seen that the action of $\mathrm{SL}_2(K)^3$ on $2 \times 2 \times 2$ cubes over K has a single polynomial invariant, of degree four, given by its discriminant. In analogy with the case of cubes, given a hypercube $H \in \mathcal{H}_2(K)$, for each $i \in \{1, 2, 3, 4\}$, we may construct a binary quartic form

$$(4) \qquad\qquad f_i(x, y) = \mathrm{disc}(A_i x + B_i y),$$

where the (A_i, B_i) denote the four slicings of the hypercube H into pairs of cubes over K.

Note that the form f_1 is invariant under the action of the subgroup $\{\mathrm{id}\} \times \mathrm{SL}_2(K)^3 \subset \mathrm{SL}_2(K)^4$ on $H \in \mathcal{H}_2(K)$, because the action of $\mathrm{SL}_2(K)^3$ on the cube $A_1 x + B_1 y$ of linear forms in x and y fixes $\mathrm{disc}(A_1 x + B_1 y)$. The remaining factor of $\mathrm{SL}_2(K)$ in $\mathrm{SL}_2(K)^4$ then acts in the usual way on the binary quartic form f_1, and it is well known that this action has two independent polynomial invariants, which are traditionally called $I(f_1)$ and

$J(f_1)$ (see §4.1 for more details on binary quartic forms). These invariants have degrees 2 and 3, respectively, in the coefficients of f_1. Since they coincide with the corresponding invariants I and J of f_2, f_3, and f_4 (as an easy calculation shows), this yields well-defined $\mathrm{SL}_2(K)^4$-invariants $I(H)$ and $J(H)$ for all elements $H \in \mathcal{H}_2(K)$. The invariants $I(H)$ and $J(H)$ thus have degrees 8 and 12, respectively, in the entries of H. Unlike for the case of $2 \times 2 \times 2$ boxes, this method does *not* produce all the $\mathrm{SL}_2(K)^4$-invariants on H; in §2.3.4, we will construct a certain noncommutative diagram to produce the others.

The *discriminant* $\mathrm{disc}(f)$ of a binary quartic form f is defined by

$$(5) \qquad \mathrm{disc}(f) := 4I(f)^3 - J(f)^2,$$

which is nonzero precisely when f has four distinct roots in $\mathbb{P}^1(\overline{K})$; such a binary quartic form is called *nondegenerate*. For a hypercube H, since the I and J invariants are the same for all the f_i, so are their discriminants. We may define the *discriminant* of H to be

$$(6) \qquad \mathrm{disc}(H) := 4I(H)^3 - J(H)^2,$$

which is nonzero precisely when any of the binary quartic forms f_i associated to H has four distinct roots in $\mathbb{P}^1(\overline{K})$. We say the hypercube H is *nondegenerate* if its discriminant is nonzero.

We give a conceptual explanation as to why $I(f_i) = I(f_j)$ and $J(f_i) = J(f_j)$ (and thus $\mathrm{disc}(f_i) = \mathrm{disc}(f_j)$) for all i and j in the next subsection.

2.3. Genus one curves from hypercubes

We now explain how a nondegenerate hypercube H gives rise to a number of genus one curves C_i ($1 \le i \le 4$), C_{ij} ($1 \le i < j \le 4$), and C_{ijk} ($1 \le i < j < k \le 4$). We also discuss how these genus one curves are related to each other, and the resulting description of the nondegenerate orbits of $\mathrm{SL}_2(K)^4$ on the space $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ of hypercubes over K.

2.3.1. Genus one curves mapping to $\mathbb{P}^1$. Given a nondegenerate binary quartic form f over K, we may attach to f a genus one curve $C(f)$ over K, namely the normalization of the projectivization of the affine curve $y^2 = f(x, 1)$. It is known (see, e.g., [BSD63, AKM$^+$01]) that the Jacobian of the curve $C(f)$ may be written as a Weierstrass elliptic curve with coefficients involving the invariants $I(f)$ and $J(f)$ of f, namely as

$$(7) \qquad E(f) : y^2 = x^3 - 27I(f) - 27J(f).$$

We always take $E(f)$ as our model for the Jacobian of $C(f)$.

Now given a nondegenerate hypercube $H \in \mathcal{H}_2(K)$, we have seen that we naturally obtain four binary quartic forms f_1, f_2, f_3, f_4 over K from H. Thus each hypercube $H \in \mathcal{H}_2(K)$ yields four corresponding genus one curves C_1, C_2, C_3, C_4 over K, where $C_i = C(f_i)$.

2.3.2. Genus one curves in $\mathbb{P}^1 \times \mathbb{P}^1$.

These genus one curves obtained from a nondegenerate hypercube $H \in \mathcal{H}_2(K)$ may be seen more explicitly in $\mathbb{P}^1 \times \mathbb{P}^1$. Let us first identify $\mathcal{H}_2(K)$ with the space of quadrilinear forms on $W_1 \times W_2 \times W_3 \times W_4$, where each W_i ($i \in \{1, 2, 3, 4\}$) is a 2-dimensional K-vector space. (In this identification, when we write $\mathcal{H}_2(K) = K^2 \otimes K^2 \otimes K^2 \otimes K^2$, then the ith factor of K^2 here is the K-vector space dual to W_i.) Then for any $H \in \mathcal{H}_2(K)$, viewed as such a quadrilinear form, consider the variety

$$C_{12}(K) = \big\{ (w_1, w_2) \in \mathbb{P}(W_1) \times \mathbb{P}(W_2) \, : \, \det(H(w_1, w_2, \cdot, \cdot)) = 0 \big\}$$
$$\subset \mathbb{P}^1 \times \mathbb{P}^1,$$

where we view $H(w_1, w_2, \cdot, \cdot)$ naturally as a bilinear form on $W_3 \times W_4$, whose determinant's vanishing or nonvanishing is thus well-defined.

By definition, $C_{12}(K)$ consists of the set of K-points of a bidegree $(2,2)$ curve C_{12} in $\mathbb{P}^1 \times \mathbb{P}^1$, which is a genus one curve if smooth (precisely when H is nondegenerate). The projections of C_{12} to $\mathbb{P}(W_1)$ or to $\mathbb{P}(W_2)$ then yield the double covers of $\mathbb{P}^1$ corresponding to C_1 and C_2, respectively. Indeed, the points of ramification of the projection $C_{12} \to \mathbb{P}(W_1)$ are the points $(w_1, w_2) \in C_{12} \subset \mathbb{P}(W_1) \times \mathbb{P}(W_2)$ for which $\det(H(w_1, w_2, \cdot, , \cdot))$ has vanishing discriminant as a quadratic form in w_1; this discriminant is precisely the binary quartic form f_1 on W_1!

It follows that C_{12} is isomorphic to both C_1 and C_2, and hence all these genus one curves C_i are isomorphic to each other: for $1 \leq i < j \leq 4$, we have natural isomorphisms

$$C_i \cong C_{ij} \cong C_j.$$

It also follows then that all four binary quartic forms f_i must have the same values for the invariants I and J, as claimed at the end of §2.2. (Indeed, all $I(f_i)$ and all $J(f_i)$ must be the same for all forms f_i—up to scaling by c^2 and c^3, respectively, for some constant c—in order for the Jacobians in (7) to be isomorphic. But then symmetry considerations show that c must be 1.)

2.3.3. Genus one curves in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. The curve C_{12} can in fact be mapped into $\mathbb{P}(W_1) \times \mathbb{P}(W_2) \times \mathbb{P}(W_3) \cong \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$, as follows. For a point $(w_1, w_2) \in C_{12}$, since $H(w_1, w_2, \cdot, \cdot)$ is singular as a bilinear form on $W_3 \times W_4$, the kernel of $H(w_1, w_2, \cdot, \cdot)$ in W_3 is nonempty; if H is nondegenerate, it can be shown that the kernel in W_3 is one-dimensional. We thus obtain a well-defined element $w_3 \in \mathbb{P}(W_3)$ such that $H(w_1, w_2, w_3, \cdot) \equiv 0$. Therefore,

$$C_{123}(K) := \big\{ (w_1, w_2, w_3) \in \mathbb{P}(W_1) \times \mathbb{P}(W_2) \times \mathbb{P}(W_3) : H(w_1, w_2, w_3, \cdot) \equiv 0 \big\}$$

gives the set of K-points of a genus one curve C_{123} in $\mathbb{P}(W_1) \times \mathbb{P}(W_2) \times \mathbb{P}(W_3) \cong \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ defined over K; moreover, the projection of C_{123} onto $\mathbb{P}(W_1) \times \mathbb{P}(W_2)$ gives an isomorphism onto C_{12}. In particular, C_{123} provides us with explicit isomorphisms among the three curves C_{12}, C_{13}, and C_{23}, through projection and un-projection. It is natural to package this information together by keeping track simply of the single curve C_{123} in $\mathbb{P}(W_1) \times \mathbb{P}(W_2) \times \mathbb{P}(W_3)$.

2.3.4. The fundamental tetrahedron of isomorphisms. We may thus construct curves C_{123}, C_{124}, C_{134}, and C_{234} in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ from a nondegenerate hypercube $H \in \mathcal{H}_2(K)$. These four genus one curves are all isomorphic to each other, as we have already seen. In fact, we may construct explicit and natural isomorphisms between them, as follows. Given a point (w_1, w_2, w_3) on $C_{123} \subset \mathbb{P}(W_1) \times \mathbb{P}(W_2) \times \mathbb{P}(W_3)$, the bilinear form $H(\cdot, w_2, w_3, \cdot)$ on $W_1 \times W_4$ is singular and of rank 1, so there exists a unique $w_4 \in \mathbb{P}(W_4)$ such that $H(\cdot, w_2, w_3, w_4) \equiv 0$. This implies that $(w_2, w_3, w_4) \in C_{234}(K)$, giving the desired map

$$\tau_{123}^{234} : C_{123} \to C_{234},$$

and similarly we obtain the maps τ_{123}^{134}, τ_{124}^{123}, etc. Note that each of these maps is invertible, since clearly $\tau_{234}^{123} = (\tau_{123}^{234})^{-1}$, etc.

We thus obtain a tetrahedron of maps:

(8)
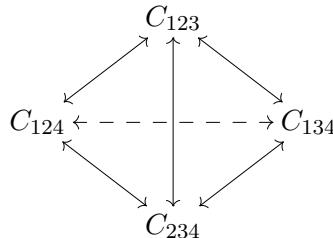
However, these isomorphisms do not all commute with each other! For example, starting at C_{123} and tracing around the triangle of isomorphisms

$\tau_{134}^{123} \circ \tau_{124}^{134} \circ \tau_{123}^{124}$ yields a hyperelliptic involution ι_1 on C_{123}. The quotient of C_{123} by this involution ι_1 yields the double cover of $\mathbb{P}^1$ given by $C_1 : y^2 = f_1(x,1)$. Similarly, the other two triangles of isomorphisms starting at C_{123} yield the involutions ι_2 and ι_3 on C_{123} corresponding to the double covers C_2 and C_3 of $\mathbb{P}^1$ whose branch points are the roots of f_2 and f_3, respectively.

If one instead starts at C_{123} and follows a quadrilateral of isomorphisms involving all four curves, then (viewing the traversal of the quadrilateral as a traversal of two triangles) we obtain the automorphism $\iota_i \circ \iota_j$ of C_{123}, which is a translation of C_{123} by a point P_{ij} on the Jacobian of C_{123}. We thus obtain three points P_{12}, P_{23}, and P_{31} on the Jacobian $E := E(H)$ of $C := C_{123}$. Since $(\iota_1 \circ \iota_2) \circ (\iota_2 \circ \iota_3) \circ (\iota_3 \circ \iota_1) = \mathrm{id}$, we have the relation

$$(9) \qquad\qquad\qquad P_{12} + P_{23} + P_{31} = 0.$$

Moreover, these points P_{ij} are nonzero, and they lie in the subgroup $\mathrm{Pic}^0(C)(K)$ in $E(K)$. The difference is that the points of $\mathrm{Pic}^0(C)(K)$ correspond to the divisor classes of K-rational divisors of degree 0 on C, whereas the points of $E(K)$ correspond to the K-rational divisor classes of degree 0 (that is, where the divisor class is K-rational, but not necessarily any of the divisors in it). Here, these points P_{ij} arise as differences of actual rational divisors and thus lie in $\mathrm{Pic}^0(C)(K)$. Indeed, if D_1, D_2, and D_3 denote the degree two divisors on C_{123} corresponding to the three projections to $\mathbb{P}(W_1)$, $\mathbb{P}(W_2)$, and $\mathbb{P}(W_3)$, respectively, then for a point x on C_{123} we have $\iota_i(x) = D_i - x$. Thus $\iota_i \circ \iota_j(x) = x + (D_i - D_j)$, so that $P_{ij} = D_i - D_j$. This also implies the relation (9).

In summary, we have seen that there is a canonical elliptic curve $E(H)$ attached to any nondegenerate hypercube $H \in \mathcal{H}_2(K)$, namely,

$$(10) \qquad\qquad E(H) : y^2 = x^3 - 27I(H) - 27J(H)$$

with

$$I(H) := I(f_i) \qquad \text{and} \qquad J(H) := J(f_i)$$

for $1 \le i \le 4$, where f_1, f_2, f_3, f_4 are the binary quartic forms naturally arising from H. Furthermore, $E := E(H)$ is canonically the Jacobian of each of the genus one curves C_i ($1 \le i \le 4$) as well as the genus one curves C_{ij} ($1 \le i \le j \le 4$) and C_{ijk} ($1 \le i \le j \le k \le 4$) arising from H. Finally, there is a natural tetrahedron of isomorphisms (8) among the C_{ijk} which does not commute. We thus obtain, in addition to a degree 2 divisor D_1 on the curve C_{123}, three nonzero rational points P_{12}, P_{23}, and P_{31} in $\mathrm{Pic}^0(C_{123})(K)$ that sum to zero.

2.4. Orbit classification of $2 \times 2 \times 2 \times 2$ hypercubes

We will show in §6.2 that the data of a genus one curve $C = C_{123}$, the equivalence class of a degree two rational divisor $D = D_1$ on C, and three nonzero points $P = P_{12}$, $P' = P_{23}$, and $P'' = P_{31}$ (with $P + P' + P'' = 0$) in the subgroup $\mathrm{Pic}^0(C)(K)$ of the Jacobian of C is in fact sufficient to recover the orbit of a hypercube H. We have:

Theorem 2.1. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K)^4$-orbits on the space $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ of hypercubes over K and isomorphism classes of triples $(C, L, (P, P', P''))$, where C is a smooth irreducible genus one curve over K, L is a degree 2 line bundle on C, and P, P', P'' are nonzero K-points that sum to zero in $\mathrm{Pic}^0(C)(K)$.*

It is known (see [Vin76, Lit89]) that the ring of polynomial invariants for the action of $\mathrm{SL}_2(K)^4$ on $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ is freely generated by four polynomials a_2, a_4, a_4', and a_6, having degrees 2, 4, 4, and 6, respectively, in the entries of the hypercube. In terms of the geometric data in Theorem 2.1, we may write the Jacobian of C as a Weierstrass elliptic curve $y^2 = x^3 + a_8 x + a_{12}$, on which the points $P = (a_4, a_6)$, $P' = (a_4', a_6')$, $P'' = (a_4'', a_6'')$ lie, such that a_2 can be interpreted as the slope $\frac{a_6' - a_6}{a_4' - a_4}$ of the line connecting P and P' (and P'').

From these four invariants, the invariant a_6' (i.e., the y-coordinate of P') may be determined:

$$a_6' = a_6 + a_2(a_4' - a_4).$$

The coefficients a_8 and a_{12} of the Weierstrass elliptic curve may also be determined, since there is a unique such elliptic curve passing through the two points P and P'. Indeed, we find

(11)
$$a_8 = a_2(a_6 + a_6') - (a_4^2 + a_4 a_4' + a_4'^2), \qquad \text{and}$$
$$a_{12} = a_6^2 - a_2 a_4(a_6 + a_6') + a_4 a_4'(a_4 + a_4').$$

Finally, the coordinates of $P'' = (a_4'', a_6'')$ may be recovered by finding the third point of intersection of the line $y - a_6 = a_2(x - a_4)$ with the elliptic curve $y^2 = x^3 + a_8 x + a_{12}$; this yields

$$a_4'' = 3a_2^2 - a_4 - a_4', \qquad \text{and}$$
$$a_6'' = a_2^3 - 3(a_2 a_4 - a_6) - a_6 - a_6'.$$

In conclusion, a_2, a_4, a_4', a_4'', a_6, a_6', a_6'', $a_8 = -27I$, and $a_{12} = -27J$ are all fundamental and important polynomial invariants for the action of $\mathrm{SL}_2(K)^4$ on $K^2 \otimes K^2 \otimes K^2 \otimes K^2$; they all have key geometric interpretations and can be expressed as simple polynomials in the four basic invariants a_2, a_4, a_4', and a_6.

2.5. Symmetrization

Just as one may identify the binary quadratic form $ax^2 + 2bxy + cy^2$ with the symmetric 2×2 matrix

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix},$$

and the binary cubic form $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ with the triply symmetric $2 \times 2 \times 2$ matrix

(12)

(see [Bha04a]), one may associate the binary quartic form

(13)
$$ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4$$

with the quadruply-symmetric $2 \times 2 \times 2 \times 2$ matrix

(14)

Using $\mathrm{Sym}_4\, K^2$ to denote the space of binary quartic forms of this type, the above association of the binary quartic form (13) with the hypercube (14) corresponds to the natural inclusion

$$\mathrm{Sym}_4\, K^2 \hookrightarrow K^2 \otimes K^2 \otimes K^2 \otimes K^2$$

of the space of quadruply-symmetric hypercubes into the space of hypercubes.

Such hypercubes lead to geometric data $(C, L, (P, P', P''))$ as in Theorem 2.1, but (due to the symmetry) we also have $P = P' = P''$. Since $P + P' + P'' = 0$, we see that P is a 3-torsion point on the Jacobian of C. Conversely, we will show in §6.3.4 that this is the only constraint on P. Thus we obtain the following theorem classifying the orbits of $\mathrm{GL}_2(K) \times \mathbb{G}_m$ on $\mathrm{Sym}_4 K^2$:

Theorem 2.2. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K) \times \mathbb{G}_m$-orbits on the space $\mathrm{Sym}_4 K^2$ of binary quartic forms over K and isomorphism classes of triples (C, L, P), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and P a nonzero 3-torsion point on the Jacobian of C defined over K.*

We have already noted in §2.3.1 (see §4.1 for further details) that certain $\mathrm{GL}_2(K)$-orbits on $\mathrm{Sym}^4 K^2$ correspond to pairs (X, L), where X is a genus one curve and L is a degree 2 line bundle on X. When $\mathrm{char}(K) \nmid 6$, these two spaces $\mathrm{Sym}_4 K^2$ and $\mathrm{Sym}^4 K^2$ are naturally identified, so we obtain two "dual" moduli interpretations of the space of binary quartic forms in terms of genus one curves. The two genus one curves coming from a binary quartic are *not* the same, however; they are related by a Hessian-type construction (see §6.3.4).

2.6. Triple symmetrization

The orbit description for binary quartic forms in §2.5 was obtained by imposing a symmetry condition on the orbit description for hypercubes. Rather than imposing a fourfold symmetry, we may instead impose only a threefold symmetry. This leads to hypercubes of the form

(15)

That is, these hypercubes can be sliced (in a certain fixed direction) into two triply symmetric cubes, and therefore can naturally be viewed as a pair

of binary cubic forms

$$(16) \qquad (ax^3 + 3bx^2y + 3cxy^2 + dy^3, ex^3 + 3fx^2y + 3gxy^2 + hy^3).$$

The above association of the pair (16) of binary cubic forms with the hypercube (15) corresponds to the natural inclusion map

$$\jmath : K^2 \otimes \mathrm{Sym}_3 K^2 \hookrightarrow K^2 \otimes K^2 \otimes K^2 \otimes K^2.$$

To such nondegenerate triply symmetric hypercubes, we may associate the usual geometric data $(C, L, (P, P', P''))$ as in Theorem 2.1, and as in the fully symmetric case, the symmetry implies that P is a 3-torsion point. We will show in §6.3.2 that this is again the only constraint on P, and so we obtain the following theorem classifying the orbits of $\mathrm{GL}_2(K)^2$ on $K^2 \otimes \mathrm{Sym}_3 K^2$:

Theorem 2.3. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K)^2$-orbits on the space $K^2 \otimes \mathrm{Sym}_3 K^2$ of pairs of binary cubic forms over K and isomorphism classes of triples (C, L, P), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and P a nonzero 3-torsion point on the Jacobian of C defined over K.*

It is interesting that the data parametrized by the orbits on both $\mathrm{Sym}_4 K^2$ and $K^2 \otimes \mathrm{Sym}_3 K^2$ are the same, and our orbit description in fact allows us to determine an explicit linear transformation in $\mathrm{GL}_2(K)^2$ that takes any given nondegenerate element of $K^2 \otimes \mathrm{Sym}_3 K^2$ to an element of $\mathrm{Sym}_4 K^2$.

2.7. Double symmetrization

We may instead impose only a twofold symmetry, leading us to study the space $K^2 \otimes K^2 \otimes \mathrm{Sym}_2 K^2$ of 2×2 matrices of binary quadratic forms. In terms of the geometric data $(C, L, (P, P', P''))$ of Theorem 2.1, we see that P' and P'' coincide, which then determines P by the relation $P + P' + P'' = 0$. Thus only the information of the point P' needs to be retained. Since $P \neq 0$, the point P' cannot be 2-torsion, and so (writing now P' as P) we obtain the following:

Theorem 2.4. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K)^3$-orbits on the space $K^2 \otimes K^2 \otimes \mathrm{Sym}_2 K^2$ of 2×2 matrices of binary quadratic forms over K and isomorphism classes of triples (C, L, P), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and P is a non-2-torsion point of the subgroup $\mathrm{Pic}^0(C)(K)$ of $\mathrm{Jac}(C)(K)$.*

2.8. Double-double symmetrization

We may, in fact, ask for the hypercubes to be symmetric under any subgroup of the symmetric group S_4. One of the interesting cases arises from the hypercubes fixed under the action of $S_2 \times S_2 \subset S_4$, which we call double-double symmetrization:

Theorem 2.5. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K)^2$-orbits on the space $\mathrm{Sym}_2 K^2 \otimes \mathrm{Sym}_2 K^2$ of symmetric 2×2 matrices of binary quadratic forms over K and isomorphism classes of triples (C, L, P), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and P is a non-2-torsion point of the subgroup $\mathrm{Pic}^0(C)(K)$ of $\mathrm{Jac}(C)(K)$.*

Over a field K not of characteristic dividing 6, the space $\mathrm{Sym}^2 K^2 \otimes \mathrm{Sym}^2 K^2$ is isomorphic to the space of the doubly-doubly symmetric hypercubes. Analogous to the case discussed in §2.6, there is a natural "dual" interpretation for the orbits of this space, also involving genus one curves X with degree 2 line bundles and a point in $\mathrm{Jac}^2_X(K)$ (see §6.1); however, the two genus one curves C and X obtained from an element of $\mathrm{Sym}^2 K^2 \otimes \mathrm{Sym}^2 K^2$ are not the same, but are again related by a certain Hessian-type construction (see §6.3.3).

2.9. Double skew-symmetrization

Instead of imposing conditions of symmetry, one may impose conditions of *skew-symmetry* on hypercubes, analogous to those described in [Bha04a, §2.6]. To define these skew-symmetrizations, let us view again our original hypercube space $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ as the space of K-quadrilinear maps $W_1 \times W_2 \times W_3 \times W_4 \to K$, where W_1, W_2, W_3, W_4 are K-vector spaces of dimension 2 (namely, the K-duals of the four factors K^2 in $K^2 \otimes K^2 \otimes K^2 \otimes K^2$). Then given such a quadrilinear map

$$\phi : W_1 \times W_2 \times W_3 \times W_4 \to K$$

in $K^2 \otimes K^2 \otimes K^2 \otimes K^2$, one may naturally construct another K-quadrilinear map

$$\bar{\phi} : W_1 \times W_2 \times (W_3 \oplus W_4) \times (W_3 \oplus W_4) \to K$$

that is skew-symmetric in the third and fourth variables; this map $\bar{\phi} = \mathrm{id} \otimes \mathrm{id} \otimes \wedge_{2,2}(\phi)$ is given by

$$\bar{\phi}\,(r, s, (t, u), (v, w)) = \phi(r, s, t, w) - \phi(r, s, v, u).$$

Thus we have a natural K-linear mapping
(17)
$$\text{id} \otimes \wedge_{2,2} : K^2 \otimes K^2 \otimes K^2 \otimes K^2 \to K^2 \otimes K^2 \otimes \wedge^2(K^2 \oplus K^2) = K^2 \otimes K^2 \otimes \wedge^2 K^4$$

taking $2 \times 2 \times 2 \times 2$ hypercubes to 2×2 matrices of alternating 2-forms in four variables. Explicitly, in terms of fixed bases for W_1, W_2, W_3, W_4, the hypercube (3) maps to the 2×2 matrix of skew-symmetric matrices as follows:

(18)
$$
\left(
\begin{bmatrix}
 & & h_{1111} & h_{1112} \\
 & & h_{1121} & h_{1122} \\
-h_{1111} & -h_{1121} & & \\
-h_{1112} & -h_{1122} & &
\end{bmatrix}
\begin{bmatrix}
 & & h_{1211} & h_{1212} \\
 & & h_{1221} & h_{1222} \\
-h_{1211} & -h_{1221} & & \\
-h_{1212} & -h_{1222} & &
\end{bmatrix}
\right.
$$
$$
\left.
\begin{bmatrix}
 & & h_{2111} & h_{2112} \\
 & & h_{2121} & h_{2122} \\
-h_{2111} & -h_{2121} & & \\
-h_{2112} & -h_{2122} & &
\end{bmatrix}
\begin{bmatrix}
 & & h_{2211} & h_{2212} \\
 & & h_{2221} & h_{2222} \\
-h_{2211} & -h_{2221} & & \\
-h_{2212} & -h_{2222} & &
\end{bmatrix}
\right).
$$

Analogous to the case of double skew-symmetrization of $2 \times 2 \times 2$ cubes, where two ideal classes become replaced with a single rank 2 module, in the geometric data corresponding to a double-skew-symmetric hypercube, two degree 2 line bundles L_3 and L_4 that come from the curves C_3 and C_4 are replaced by a single vector bundle M of rank 2 and degree 4. We thus have the following result (where the nondegeneracy condition on the geometric data is a mild open condition and will be discussed in §6.5).

Theorem 2.6. *For any field K with $\text{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\text{GL}_2(K)^2 \times \text{GL}_4(K)$-orbits on the space $K^2 \otimes K^2 \otimes \wedge^2 K^4$ of 2×2 matrices of alternating quaternary 2-forms over K and isomorphism classes of nondegenerate quadruples (C, L, P, M), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, P is a nonzero point of $\text{Pic}^0(C)(K)$, and M is a rank 2 vector bundle of degree 4 such that $\det M \cong P \otimes L^{\otimes 2}$.*

2.10. Triple skew-symmetrization

We may also impose a triple skew-symmetry on hypercubes. With the same notation as in the previous section, given a quadrilinear map

$$\phi : W_1 \times W_2 \times W_3 \times W_4 \to K,$$

we may construct the K-quadrilinear map

$$\bar{\phi}: W_1 \times (W_2 \oplus W_3 \oplus W_4) \times (W_2 \oplus W_3 \oplus W_4) \times (W_2 \oplus W_3 \oplus W_4) \to K,$$

which is alternating in the last three factors and explicitly given by

$$\bar{\phi}(r, (s_1, s_2, s_3), (t_1, t_2, t_3), (u_1, u_2, u_3)) = \sum_{\sigma \in S_3} (-1)^{\sigma} \phi(r, s_{\sigma(1)}, t_{\sigma(2)}, u_{\sigma(3)}).$$

Thus, we obtain a natural K-linear injection

$$(19) \quad \mathrm{id} \otimes \wedge_{2,2,2} : K^2 \otimes K^2 \otimes K^2 \otimes K^2 \to K^2 \otimes \wedge^3 (K^2 \oplus K^2 \oplus K^2) = K^2 \otimes \wedge^3 K^6$$

from the space of hypercubes to the space of pairs of senary alternating 3-forms. In analyzing the $\mathrm{GL}_2(K) \times \mathrm{GL}_6(K)$-orbits of this larger space, one finds that the degree 2 line bundles L_2, L_3, L_4 coming from C_2, C_3, C_4 are now replaced by a single rank 3 vector bundle (which splits into the direct sum of these line bundles for elements in the image of $\mathrm{id} \otimes \wedge_{2,2,2}$). We thus obtain the following:

Theorem 2.7. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K) \times \mathrm{GL}_6(K)$-orbits on the space $K^2 \otimes \wedge^3 K^6$ of pairs of senary alternating 3-forms over K and isomorphism classes of nondegenerate triples (C, L, M), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and M is a rank 3 vector bundle of degree 6 such that $\det M \cong L^{\otimes 3}$.*

2.11. A simultaneous generalization: triply Hermitian hypercubes

Many of the orbit parametrizations we have discussed in this section can be unified and generalized, via a process we call *Hermitianization*. Just as one can consider square matrices that are Hermitian over a composition algebra, we may consider cubical matrices that are Hermitian over a cubic algebra. The most convenient notion for this purpose is Springer's definition of a *cubic Jordan algebra*, which we discuss in more detail in §5.3. For now, it suffices to say that a cubic Jordan algebra is a generalization of the notion of a cubic field extension, where each element of the cubic Jordan algebra has two other formal conjugates, and there is a well-defined notion of a characteristic polynomial that these conjugate elements all satisfy. Some simple examples of cubic Jordan algebras over a field K include K^3, K^2, K, cubic field extensions of K, $K \times \mathrm{Mat}_{2 \times 2}(K)$, and $\mathrm{Mat}_{3 \times 3}(K)$.

A *triply Hermitian* hypercube for the cubic algebra J over K is one of the form

(20)
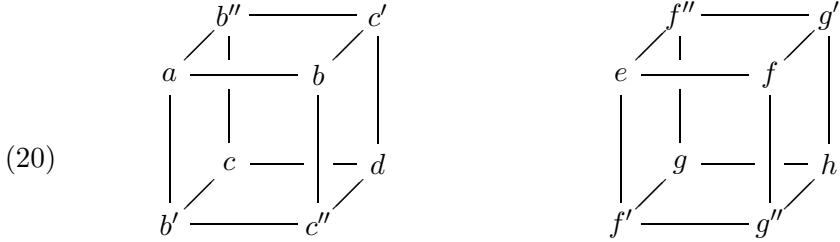
where $a, d, e, h \in K$ and $b, c, f, g \in J$, and b', b'' and c', c'' are formal conjugates of b and c, respectively. We denote the space of all triply Hermitian hypercubes for such a cubic Jordan algebra J/K by $\mathscr{C}_2(J)$.

For each such J, there is a natural group $\mathrm{SL}_2(J)$ acting by linear transformations but preserving a certain discriminant quartic form on the space $\mathscr{C}_2(J)$. Then we obtain a parametrization for the orbits of $\mathrm{GL}_2(K) \times \mathrm{SL}_2(J)$ on $\mathscr{C}_2(J)$ (a full version of the theorem may be found in §6.5):

Theorem 2.8. *For any field K with* $\mathrm{char}(K) \nmid 6$, *and a cubic Jordan algebra J over K, there is a canonical bijection between nondegenerate $\mathrm{GL}_2(K) \times \mathrm{SL}_2(J)$-orbits on the space $\mathscr{C}_2(J)$ of triply Hermitian hypercubes for J over K and isomorphism classes of triples $(C, L, \mathcal{F})$, where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and $\mathcal{F}$ is a flag of vector bundles on C with additional structure coming from J, subject to a relation between L and $\mathcal{F}$.*

In each case, one of the key components of the construction of the corresponding geometric data is a flag variety related to the representation of $\mathrm{SL}_2(J)$ on $\mathscr{C}_2(J)$. Each element of $\mathscr{C}_2(J)$ produces a map from a genus one curve C to this flag variety, thereby giving the flag $\mathcal{F}$ on C described in the theorem. See §6.5 for full details.

The cases $J = K^3$, $K \times K$, K, $K \times \mathrm{Mat}_{2 \times 2}(K)$, and $\mathrm{Mat}_{3 \times 3}(K)$ yield regular hypercubes, triply symmetric hypercubes, doubly symmetric hypercubes, doubly skew-symmetric hypercubes, and triply skew-symmetric hypercubes, respectively. From this perspective, one may also obtain moduli descriptions of some more exotic spaces, e.g., $\mathrm{GL}_2(K) \times \mathrm{Sp}_6(K)$-orbits on $K^2 \otimes \wedge_0^3(K^6)$, $\mathrm{GL}_2(K) \times \mathrm{Spin}_{12}(K)$-orbits on $K^2 \otimes K^{32}$, and $\mathrm{GL}_2(K) \times E_7(K)$-orbits on $K^2 \otimes K^{56}$.

3. Main results II: Genus one curves and $3 \times 3 \times 3$ Rubik's cubes

In this section, we discuss the space of $3 \times 3 \times 3$ cubical matrices ("Rubik's cubes") over K, and describe the various parametrizations of genus one curves with extra data that can be obtained from this perspective. Again, no proofs or details are given in this section. Further details, more basis-free constructions, and proofs may be found in Section 5.

3.1. On Rubik's cubes

Let K be a field of characteristic not dividing 6. Analogous to the space of $2 \times 2 \times 2$ cubes from §2.1, we may consider the space of $3 \times 3 \times 3$ cubes, which we call *Rubik's cubes*. Let $\mathcal{C}_3(K)$ denote the space $K^3 \otimes K^3 \otimes K^3$. Then each element of $\mathcal{C}_3(K)$ may be represented as a $3 \times 3 \times 3$ cubical matrix $B = (b_{ijk})_{1 \leq i,j,k \leq 3}$ with entries in K:

(21)

If we denote by $\{e_1, e_2, e_3\}$ the standard basis of K^3, then the element of $\mathcal{C}_3(K)$ described by the cubical matrix $B = (b_{ijk})_{1 \leq i,j,k \leq 3}$ above is

$$\sum_{1 \leq i,j,k \leq 3} b_{ijk}\, e_i \otimes e_j \otimes e_k.$$

Thus we may identify $\mathcal{C}_3(K)$ with the space of $3 \times 3 \times 3$ matrices with entries in K or, simply, the space of *Rubik's cubes over K*.

As in §2.1, a Rubik's cube can naturally be partitioned into three 3×3 matrices in three distinct ways. Namely, the cube $B = (b_{ijk})$ given by (21) can be sliced into the three $3 \times 3 \times 3$ matrices M_ℓ, N_ℓ, and P_ℓ, for $\ell = 1, 2, 3$, as follows:

1) $M_1 = (b_{1jk})$ is the front face, $N_1 = (b_{2jk})$ is the middle slice, and $P_1 = (b_{3jk})$ is the back face;

2) $M_2 = (b_{i1k})$ is the top face, $N_2 = (b_{i2k})$ is the middle slice, and $P_2 = (b_{i3k})$ is the bottom face;

3) $M_3 = (b_{ij1})$ is the left face, $N_3 = (b_{ij2})$ is the middle slice, and $P_3 = (b_{ij3})$ is the right face.

There is also a natural action of $\mathrm{SL}_3(K)^3$ on $\mathcal{C}_3(K)$, analogous to the action of $\mathrm{SL}_2(K)^3$ on the space $\mathcal{C}_2(K)$ of $2 \times 2 \times 2$ cubes. Namely, for any $i \in \{1, 2, 3\}$, the element $g = (g_{\ell m}) \in \mathrm{SL}_3(K)$ in the ith factor acts on the cube B by replacing (M_i, N_i, P_i) by $(g_{11}M_i + g_{12}N_i + g_{13}P_i,\ g_{21}M_i + g_{22}N_i + g_{23}P_i,\ g_{31}M_i + g_{32}N_i + g_{33}P_i)$. These three $\mathrm{SL}_3(K)$-actions commute, giving a well-defined action of $\mathrm{SL}_3(K)^3$ on $\mathcal{C}_3(K)$.

Recall that a $2 \times 2 \times 2$ cube naturally gave rise to three binary quadratic forms, by slicing the cube and taking determinants as in (2). In the analogous manner, a Rubik's cube $B = (b_{ijk})$ naturally gives rise to three ternary cubic forms

$$(22) \qquad\qquad f_i(x, y, z) = \det(M_i x + N_i y + P_i z)$$

for $1 \leq i \leq 3$. The ternary cubic form f_1 is invariant under the action of the subgroup $\mathrm{id} \times \mathrm{SL}_3(K)^2 \subset \mathrm{SL}_3(K)^3$ on $B \in \mathcal{C}_3(K)$. The remaining factor of $\mathrm{SL}_3(K)$ acts in the standard way on the ternary cubic form f_1, and it is well known that this action has two independent polynomial invariants, which are traditionally called $S(f_1)$ and $T(f_1)$ (see §4.2 for more details on ternary cubic forms). These invariants have degrees 4 and 6, respectively, in the coefficients of f_1. Analogous to the situation with $2 \times 2 \times 2 \times 2$ hypercubes, one checks that f_2 and f_3 also have the same invariants as f_1, and so we have produced well-defined $\mathrm{SL}_3(K)^3$-invariants $S(B)$ and $T(B)$ for Rubik's cubes B, having degrees 12 and 18, respectively. Again, this construction does *not* produce all the invariants; in §3.2.3, we will again construct a certain noncommutative diagram in order to produce the remaining generators of the $\mathrm{SL}_3(K)^3$-invariant ring.

The *discriminant* $\mathrm{disc}(f)$ of a ternary cubic form f is defined by

$$(23) \qquad\qquad \mathrm{disc}(f) = \frac{1}{1728}(S(f)^3 - T(f)^2),$$

and the discriminant of the ternary cubic form f is nonzero precisely when it cuts out a smooth curve in $\mathbb{P}^2$; such a ternary cubic form is called *nondegenerate*. Since the S and T invariants are common to all the f_i, their

discriminants are also all the same, and thus we may naturally define the *discriminant* of a Rubik's cube B to be

$$(24) \qquad \operatorname{disc}(B) := \frac{1}{1728}(S(B)^3 - T(B)^2),$$

which is nonzero precisely when any of the ternary cubic forms f_i associated to B cut out a smooth curve in $\mathbb{P}^2$. We say then that the Rubik's cube B is *nondegenerate* if its discriminant is nonzero.

We give a conceptual explanation as to why $S(f_i) = S(f_j)$ and $T(f_i) = T(f_j)$ (and thus $\operatorname{disc}(f_i) = \operatorname{disc}(f_j)$) for all i and j in the next subsection.

3.2. Genus one curves from Rubik's cubes

We now explain how a nondegenerate Rubik's cube B naturally gives rise to a number of genus one curves C_i ($1 \le i \le 3$) and C_{ij} ($1 \le i < j \le 3$). We also discuss how these genus one curves are related to each other, and the resulting description of the nondegenerate orbits of $\mathrm{SL}_3(K)^3$ on the space $K^3 \otimes K^3 \otimes K^3$ of Rubik's cubes over K.

3.2.1. Genus one curves in $\mathbb{P}^2$. Given a nondegenerate ternary cubic form f over K, we may attach to f a genus one curve $C(f)$ over K, namely the zero locus of the polynomial f in $\mathbb{P}^2$. It is known (see, e.g., [ARVT05, AKM+01]) that the Jacobian of the curve $C(f)$ may be written as a Weierstrass elliptic curve with coefficients expressed in terms of the invariants $S(f)$ and $T(f)$, namely as

$$E(f) : y^2 = x^3 - 27S(f)x - 54T(f).$$

We always take $E(f)$ as our model for the Jacobian of $C(f)$.

Now given a nondegenerate Rubik's cube $B \in \mathcal{C}_3(K)$, we have seen that we naturally obtain three ternary cubic forms f_1, f_2, f_3, over K from B. Thus each Rubik's cube $B \in \mathcal{C}_3(K)$ yields three corresponding genus one curves C_1, C_2, C_3 over K, where $C_i = C(f_i)$.

3.2.2. Genus one curves in $\mathbb{P}^2 \times \mathbb{P}^2$. The genus one curves we have obtained from a nondegenerate Rubik's cube $B \in \mathcal{C}_3(K)$ may also be embedded naturally in $\mathbb{P}^2 \times \mathbb{P}^2$. Let us first identify $\mathcal{C}_3(K)$ with the space of trilinear forms on $W_1 \times W_2 \times W_3$, where each W_i ($i \in \{1, 2, 3\}$) is a 3-dimensional K-vector space. (In this identification, when we write $\mathcal{C}_3(K) = K^3 \otimes K^3 \otimes K^3$,

then the ith factor of K^3 is the K-vector space dual to W_i.) Then for any $B \in \mathcal{C}_3(K)$, viewed as a trilinear form, we consider the set

$$C_{12}(K) := \{(w_1, w_2) \in \mathbb{P}(W_1) \times \mathbb{P}(W_2) : B(w_1, w_2, \cdot) \equiv 0\}$$
$$\subset \mathbb{P}(W_1) \times \mathbb{P}(W_2) \cong \mathbb{P}^2 \times \mathbb{P}^2.$$

If B is nondegenerate, then C_{12} in fact yields the graph of an isomorphism between C_1 and C_2. Indeed, for any point $w_1 \in C_1$, the form $B(w_1, \cdot, \cdot)$ is singular with a one-dimensional kernel in W_2; this gives a point of $\mathbb{P}(W_2)$ that then must lie on C_2!

As this process is reversible, it follows that C_{12} is isomorphic to both C_1 and C_2 via projection, and hence all the curves C_i are isomorphic to each other: for $1 \le i < j \le 3$, if we define $C_{ij} \subset \mathbb{P}^2 \times \mathbb{P}^2$ in the analogous manner, then we have natural isomorphisms

$$C_i \cong C_{ij} \cong C_j.$$

It also follows (by the same argument as given at the end of §2.3.2) that all three ternary cubic forms f_i have the same values for the invariants S and T, as was claimed at the end of §3.1.

3.2.3. The fundamental triangle of isomorphisms. From a nondegenerate Rubik's cube B, we have thus constructed three genus one curves C_{12}, C_{23}, and C_{13}, which are all isomorphic. In fact, we may construct explicit and natural isomorphisms between them, e.g.,

$$\tau_{12}^{23} : C_{12} \to C_2 \to C_{23},$$

given by projection and un-projection. More explicitly, for a given point $(w_1, w_2) \in C_{12}$, the bilinear form $B(\cdot, w_2, \cdot)$ is singular and has rank 2, so there exists a unique $w_3 \in \mathbb{P}(W_3)$ such that $B(\cdot, w_2, w_3) \equiv 0$. Then (w_2, w_3) is a point on C_{23}, giving the map τ_{12}^{23}. Clearly, all such maps are invertible, e.g., $\tau_{23}^{12} = (\tau_{12}^{23})^{-1}$.

We thus obtain a triangle of maps

(25)

$$
\begin{array}{ccc}
 & C_{12} & \\
 \nearrow & & \searrow \\
 \swarrow & & \searrow \\
C_{23} & \longleftrightarrow & C_{13}
\end{array}
$$

.

However, this triangle does not commute! Composing the three maps of this triangle in a clockwise direction, starting from say $C = C_{12}$, yields an automorphism of C given by translation by a point P on the Jacobian $E = \mathrm{Jac}(C)$ of C. Composing the three maps in the counterclockwise direction then yields the automorphism of C given by translation by $P' = -P$. As before, these points P, P' are in fact in $\mathrm{Pic}^0(C)(K)$. Indeed, if D_1 and D_2 are the degree 3 divisors on C corresponding to the embeddings into $\mathbb{P}(W_1)$ and $\mathbb{P}(W_2)$, respectively, then we find that the difference $D_2 - D_1$ corresponds to the point P on the Jacobian of C.

In summary, from a nondegenerate Rubik's cube $B \in \mathcal{C}_3(K)$, we obtain an elliptic curve

$$E(B) : y^2 = x^3 - 27S(B)x - 54T(B),$$

with

$$S(B) = S(f_i) \qquad \text{and} \qquad T(B) = T(f_i)$$

for $1 \leq i \leq 3$, where f_1, f_2, and f_3 are the ternary cubic forms naturally arising from B. Furthermore, the elliptic curve $E := E(B)$ is canonically the Jacobian of each of the genus one curves C_i ($1 \leq i \leq 3$) and C_{ij} ($1 \leq i \leq j \leq 3$) arising from B. Finally, there is a natural triangle (25) of isomorphisms among the C_{ij}, which does not commute. We thus obtain, in addition to a degree 3 divisor D_1 on the curve C_{12}, a pair of points P, P' in $\mathrm{Pic}^0(C_{12})(K)$ that sum to zero.

3.3. Orbit classification of Rubik's cubes

We will show in §5.1 that the data of a genus one curve $C = C_{12}$, the equivalence class of a degree 3 rational divisor $D = D_1$ on C, and a pair P, P' of nonzero points summing to zero in $\mathrm{Pic}^0(C)(K)$ is in fact sufficient to recover the orbit of a Rubik's cube B. We have:

Theorem 3.1. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a canonical bijection between nondegenerate $\mathrm{GL}_3(K)^3$-orbits on the space $K^3 \otimes K^3 \otimes K^3$ of Rubik's cubes over K and isomorphism classes of triples $(C, L, (P, P'))$, where C is a smooth genus one curve over K, L is a degree 3 line bundle on C, and P and P' are nonzero points in $\mathrm{Pic}^0(C)(K)$ that sum to zero.*

It is known (see, e.g., [Vin76]) that the ring of polynomial invariants for the action of $\mathrm{SL}_3(K)^3$ on the space $K^3 \otimes K^3 \otimes K^3$ is freely generated by three polynomials d_6, d_9, and $d_{12} = -27S$, having degrees 6, 9, and 12, respectively, in the entries of the Rubik's cube. In terms of the geometric

data in Theorem 3.1, these three invariants have geometric meaning. We may write the Jacobian of the curve C in Weierstrass form as

$$E : y^2 = x^3 + d_{12}x + d_{18},$$

where $d_{18} = -54T$ is a degree 18 polynomial in the entries of the Rubik's cube, and where the points P and P' are given by $(x, y) = (d_6, \pm d_9)$ on the model E. It is clear then that d_{18} may be expressed in terms of the generators d_6, d_9, and d_{12}. In conclusion, d_6, d_9, d_{12} and d_{18} are all fundamental and important polynomial invariants for the action of $\mathrm{SL}_3(K)^3$ on $K^3 \otimes K^3 \otimes K^3$; they all have key geometric interpretations and can be expressed as simple polynomials in the three basic invariants d_6, d_9, and d_{12}.

3.4. Triple symmetrization

Analogous to the case of symmetric hypercubes discussed in §2.5, we may consider symmetric Rubik's cubes. If we ask for complete symmetry under the action of S_3, the Rubik's cubes in question will be of the form

$$(26) \qquad \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \qquad \begin{pmatrix} b & d & e \\ d & g & h \\ e & h & i \end{pmatrix} \qquad \begin{pmatrix} c & e & f \\ e & h & i \\ f & i & j \end{pmatrix}$$

where each 3×3 matrix represents one "slice." Just as quadruply-symmetric hypercubes (14) could be identified with binary quartic forms (13), in the same way the triply-symmetric Rubik's cube (26) may be identified with the ternary cubic form

$$(27) \quad ax^3 + 3bx^2y + 3cx^2z + 3dxy^2 + 6exyz + 3fxz^2 + gy^3 + 3hy^2z + 3iyz^2 + jz^3.$$

This identification corresponds to the natural inclusion

$$\mathrm{Sym}_3(K^3) \hookrightarrow K^3 \otimes K^3 \otimes K^3$$

of the space of triply-symmetric Rubik's cubes into the space of all Rubik's cubes.

Such Rubik's cubes lead to geometric data $(C, L, (P, P'))$ as in Theorem 3.1, but due to the symmetry we also have $P = P'$. Since $P + P' = 0$, we see that P is a 2-torsion point on the Jacobian of C. Conversely, we will show in §5.2.2 that this is the only constraint on P; thus we obtain the following theorem classifying the orbits of $\mathrm{GL}_3(K)$ on $\mathrm{Sym}_3 K^3$:

Theorem 3.2. *For any field K with $\operatorname{char}(K) \nmid 6$, there is a natural bijection between nondegenerate $\operatorname{GL}_3(K)$-orbits on the space $\operatorname{Sym}_3 K^3$ of ternary cubic forms over K and isomorphism classes of triples (C, L, P), where C is a smooth genus one curve over K, L is a degree 3 line bundle on C, and P is a nonzero 2-torsion point on the Jacobian of C defined over K.*

We have already noted in (see §4.2 for further details) that certain $\operatorname{GL}_3(K)$-orbits on $\operatorname{Sym}^3 K^3$ correspond to pairs (X, L), where X is a genus one curve and L is a degree 3 line bundle on X. When $\operatorname{char}(K) \nmid 6$, these two spaces $\operatorname{Sym}_3 K^3$ and $\operatorname{Sym}^3 K^3$ are naturally identified, so we obtain two "dual" moduli interpretations of the space of ternary cubics in terms of genus one curves. However, as in the case of symmetric hypercubes viewed as binary quartics in §2.5, these two genus one curves arising from a ternary cubic are *not* the same; they are related by the classical Hessian construction (see §5.2.2).

3.5. Double symmetrization

The orbit description for ternary cubic forms in §3.4 was obtained by imposing a symmetry condition on the orbit description for Rubik's cubes. Rather than imposing a threefold symmetry, we can impose only a double symmetry to obtain Rubik's cubes of the form

$$(28) \qquad \begin{pmatrix} a_1 & b_1 & c_1 \\ b_1 & d_1 & e_1 \\ c_1 & e_1 & f_1 \end{pmatrix} \qquad \begin{pmatrix} a_2 & b_2 & c_2 \\ b_2 & d_2 & e_2 \\ c_2 & e_2 & f_2 \end{pmatrix} \qquad \begin{pmatrix} a_3 & b_3 & c_3 \\ b_3 & d_3 & e_3 \\ c_3 & e_3 & f_3 \end{pmatrix},$$

where again, each 3×3 matrix represents a slice of the Rubik's cube. Since a symmetric 3×3 matrix represents a ternary quadratic form, a doubly symmetric Rubik's cube may be viewed as a triple of ternary quadratic forms

$$(29) \qquad \begin{aligned} (a_1 x^2 + 2b_1 xy + 2c_1 xz + d_1 y^2 + e_1 yz + f_1 z^2, \\ a_2 x^2 + 2b_2 xy + 2c_2 xz + d_2 y^2 + e_2 yz + f_2 z^2, \\ a_3 x^2 + 2b_3 xy + 2c_3 xz + d_3 y^2 + e_3 yz + f_3 z^2). \end{aligned}$$

The above association of the triple (29) of ternary quadratic forms with the doubly symmetric Rubik's cube (28) corresponds to the natural inclusion

$$K^3 \otimes \operatorname{Sym}_2 K^3 \hookrightarrow K^3 \otimes K^3 \otimes K^3.$$

To such nondegenerate doubly symmetric Rubik's cubes, we can associate the usual geometric data $(C, L, (P, P'))$ as in Theorem 3.1, and as in the fully symmetric case, the symmetry implies that P is a 2-torsion point. We will show in §5.2.2 that this is again the only constraint on P, and so we obtain the following theorem classifying the orbits of $\mathrm{GL}_3(K)^2$ on $K^3 \otimes \mathrm{Sym}_2 K^3$:

Theorem 3.3. *For any field K with $\mathrm{char}(K) \nmid 6$, there is a natural bijection between nondegenerate $\mathrm{GL}_3(K)^2$-orbits on the space $K^3 \otimes \mathrm{Sym}_2 K^3$ of triples of ternary quadratic forms over K and isomorphism classes of triples (C, L, P), where C is a smooth genus one curved over K, L is a degree 3 line bundle on C, and P is a nonzero 2-torsion point on the Jacobian of C defined over K.*

Note that the data parametrized by triply symmetric and doubly symmetric Rubik's cubes is the same! The two orbit parametrizations in fact allow us to construct an explicit linear transformation taking any given nondegenerate element of the space $K^3 \otimes \mathrm{Sym}_2 K^3$ to an element of $\mathrm{Sym}_3 K^3$.

3.6. Double skew-symmetrization

Instead of imposing conditions of symmetry, one may impose conditions of skew-symmetry on Rubik's cubes. Let us view again our Rubik's cube space $K^3 \otimes K^3 \otimes K^3$ as the space of K-trilinear map $W_1 \times W_2 \times W_3 \to K$, where W_1, W_2, and W_3 are 3-dimensional K-vector spaces. Then given such a K-trilinear map ϕ, one may construct another K-trilinear map

$$\bar{\phi} : W_1 \times (W_2 \oplus W_3) \times (W_2 \oplus W_3)$$

that is skew-symmetric in the last two variables and is given by

$$\bar{\phi}(r, (s, t), (u, v)) = \phi(r, s, v) - \phi(r, u, t).$$

This gives a natural K-linear injection

$$\mathrm{id} \otimes \wedge_{3,3} : K^3 \otimes K^3 \otimes K^3 \to K^3 \otimes \wedge^2(K^6)$$

taking Rubik's cubes to triples of alternating 2-forms in six variables.

In analyzing the $\mathrm{GL}_3(K) \times \mathrm{GL}_6(K)$-orbits of this larger space, one finds that the degree 3 line bundles L_2 and L_3 coming from C_2 and C_3 are now replaced by a single rank 2 vector bundle (which splits into the direct sum of these line bundles for elements in the image of $\mathrm{id} \otimes \wedge_{3,3}$). We thus obtain the following (see §5.5 for details):

Theorem 3.4. *For any field K with $\operatorname{char}(K) \nmid 6$, there is a natural bijection between nondegenerate $\operatorname{GL}_3(K) \times \operatorname{GL}_6(K)$-orbits on the space $K^3 \otimes \wedge^2 K^6$ of triples of alternating senary 2-forms over K and isomorphism classes of nondegenerate triples (C, L, M), where C is a smooth genus one curved over K, L is a degree 3 line bundle on C, and M is a rank 2 degree 6 vector bundle on C with $L^{\otimes 2} \cong \det M$.*

The nondegeneracy condition on the geometric data is a mild open condition and will be discussed in §5.4.

3.7. A simultaneous generalization: doubly Hermitian Rubik's cubes

Many of the orbit parametrizations we have discussed in this section can be unified and generalized, by a Hermitianiziation process that is analogous to the one introduced in §2.11. Recall that a Rubik's cube may be seen as a triple of 3×3 matrices. To define a *doubly Hermitian Rubik's cube*, we replace the triple of standard 3×3 matrices by a triple of 3×3 matrices that are Hermitian with respect to some composition algebra A over K. By a composition algebra A, we mean a unital (not necessarily associative) algebra A over K with a nondegenerate quadratic norm form $\mathrm{n}_A(\cdot)$ such that $\mathrm{n}_A(xy) = \mathrm{n}_A(x)\,\mathrm{n}_A(y)$ for all $x, y \in A$. This implies that A is alternative (i.e., $x(xy) = (xx)y$ and $(yx)x = y(xx)$ for all $x, y \in A$) and is equipped with a K-algebra involution $\iota : A \to A$, sending $x \in A$ to its conjugate $\bar{x}$, such that all $\operatorname{tr}_A(x) := x + \bar{x}$ and $\mathrm{n}_A(x) = x\bar{x}$ lie in the image of K in A and all $x \in A$ satisfy the quadratic relation $a^2 - (\operatorname{tr}_A(x))x + \mathrm{n}_A(x) = 0$. (We also allow the 0 algebra as a composition algebra.) A Hermitian 3×3 matrix M for the composition algebra A over K is one of the form

$$\begin{pmatrix} a & d & e \\ \bar{d} & b & f \\ \bar{e} & \bar{f} & c \end{pmatrix}$$

where $a, b, c \in K$ and $d, e, f \in A$. We denote the space of all doubly Hermitian Rubik's cubes for such a composition algebra A by $\mathscr{C}_3(A)$. Examples of suitable composition algebras A include K itself, K^2, $\operatorname{Mat}_{2\times2}(K)$, or general quaternion or octonion algebras over K. Details about the composition algebras A used in this paper are discussed in §5.3.

For each such composition algebra A, there is a natural group $\operatorname{SL}_3(A)$ that acts on 3×3 Hermitian matrices by linear transformations that preserve the determinant. Then we may classify the orbits of the action of $\operatorname{GL}_3(K) \times$

$\mathrm{SL}_3(A)$ on $\mathscr{C}_3(A)$ as follows (a full version of this theorem may be found in §5.4):

Theorem 3.5. *For any field K with $\mathrm{char}(K) \nmid 6$, and a composition algebra A over K, there is a canonical bijection between nondegenerate $\mathrm{GL}_3(K) \times \mathrm{SL}_3(A)$-orbits on the space $\mathscr{C}_3(A)$ of doubly Hermitian Rubik's cubes for A over K and isomorphism classes of triples (C, L, M), where C is a smooth genus one curve over K, L is a degree 3 line bundle on C, and M is a vector bundle of rank equal to the dimension of A over K, with a global faithful A-action and other structure coming from A, subject to a relation between L and M.*

In each case, the vector bundle M arises via a natural map from the curve C to the variety of rank one 3×3 Hermitian matrices up to scaling. The rank one Hermitian matrices form a flag variety in the space of all Hermitian matrices, and the vector bundle M on C is part of the flag on C coming from the pullback of the universal flag. See §5.4 for details.

The cases $A = K \times K$, K, $\mathrm{Mat}_{2 \times 2}(K)$ yield regular Rubik's cubes, doubly symmetric Rubik's cubes, and doubly skew-symmetric Rubik's cubes, respectively. Other examples include twists of these spaces, as well as the space $K^3 \otimes K^{27}$ under the action of $\mathrm{GL}_3(K) \times \mathrm{E}_6(K)$, which arises when A is an octonion algebra.

Preliminaries and notation

Let K be a field not of characteristic 2 or 3. We will work over the field K throughout this paper (unless specified otherwise); many of the results have analogues over a $\mathbb{Z}[\frac{1}{6}]$-scheme as well.

We use the convention that the projectivization of a vector space parametrizes lines, not hyperplanes. For example, a basepoint-free line bundle L on a variety X induces a natural map $\phi_L : X \to \mathbb{P}(H^0(X, L)^\vee)$.

A *genus one curve* means a proper, smooth, geometrically connected curve with arithmetic genus 1, and an *elliptic curve* is such a genus one curve equipped with a base point.

An isomorphism of sets of data D_1 and D_2, where D_i consists of a genus one curve C_i and vector bundles for $i = 1$ or 2, is an isomorphism $C_1 \to C_2$, along with isomorphisms between the pullbacks of the vector bundles on C_2 and the respective bundles on C_1.

If A is an element in a tensor product of vector spaces, we use the notation $A(\cdot, \ldots, \cdot)$ to denote the multilinear form, where the dots may be replaced by substituting elements of the respective dual vector spaces. For

example, for vector spaces V_1, V_2, and V_3, if $A \in V_1 \otimes V_2 \otimes V_3$ and $v \in V_1^\vee$, the notation $A(v, \cdot, \cdot)$ will refer to the evaluation $A \lrcorner v$ of the trilinear form A on v, which gives an element of $V_2 \otimes V_3$. By a slight abuse of notation, we will also use this notation to specify whether $A(v, \cdot, \cdot)$ vanishes for $v \in \mathbb{P}(V_1^\vee)$, for example.

If V is a m-dimensional vector space, then the notation $\operatorname{Sym}^n V$ refers to the nth symmetric power of V, typically constructed as a quotient of the n-fold tensor product $V \otimes \cdots \otimes V$. For a fixed basis $v_1, \ldots, v_m$ of V, elements of $\operatorname{Sym}^n V$ may be thought of as degree n homogeneous polynomials in $v_1, \ldots, v_m$. In contrast, we use $\operatorname{Sym}_n V$ to denote the space of the n-fold symmetric tensors, which is usually constructed as the subspace of $V \otimes \cdots \otimes V$ fixed under the natural action of the symmetric group S_n. Note that $\operatorname{Sym}^n V$ and $\operatorname{Sym}_n V$, over a field of characteristic not dividing $n!$, are isomorphic. In this paper, we take care to use either the quotient or subspace as needed, even though they will be isomorphic in each case here (since we have char $K \neq 2, 3$ and only consider cases where $n = 2$ or 3), for the purposes of future applications.

4. Genus one curves with degree 2, 3, 4, or 5 line bundles

In this section, we describe representations V of algebraic groups G whose orbits correspond to genus one curves with degree d line bundles for $2 \leq d \leq 5$. For any field K not of characteristic 2, 3, or 5, there is a natural bijection between nondegenerate orbits in $V(K)/G(K)$ and isomorphism classes of genus one curves defined over K equipped with degree d line bundles.

Most of these quotient descriptions are classical (or at least fairly well known) over an algebraically closed field. For example, for $d = 2$, the space under consideration is that of binary quartic forms, and for $d = 3$, ternary cubic forms. What is new here is that, for each case, we also show that with the right forms of the group G acting on the representation V, the stabilizer of a generic element of the representation agrees with the automorphism group of the curve and the line bundle. Thus we obtain an equivalence of moduli stacks, which is important in the arithmetic applications (e.g., in [BS15a, BS15b]). We suspect that some of this section is known to the experts, but has not previously been stated explicitly; see also the related work of Cremona, Fisher, and Stoll [CF09, Fis06, CFS10, Fis10].

4.1. Binary quartic forms

A *binary quartic form* over K is a two-dimensional vector space V over K equipped with an element q of $\operatorname{Sym}^4 V$. With a choice of basis $\{w_1, w_2\}$

for V, a binary quartic form over K may be represented as a homogeneous degree 4 polynomial

$$(30) \qquad q(w_1, w_2) = aw_1^4 + bw_1^3 w_2 + cw_1^2 w_2^2 + dw_1 w_2^3 + ew_2^4,$$

where $a, b, c, d, e \in K$. The group $\mathrm{GL}(V)$ acts on $\mathrm{Sym}^4 V$ by acting on V in the standard way. The ring of $\mathrm{SL}(V)$-invariants of a binary quartic form q as in equation (30) is a polynomial ring, generated by the two invariants

$$I(q) = 12ae - 3bd + c^2 \qquad \text{and} \qquad J(q) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

The categorical quotient $\mathrm{Sym}^4 V /\!/ \mathrm{SL}_2(V)$ is thus birational to the affine plane, with coordinates given by the invariants I and J. There is also a natural notion of the discriminant $\Delta(q) = 4I(q)^3 - J(q)^2$ of a binary quartic form. The nonvanishing of the discriminant $\Delta(q)$ corresponds to q having four distinct roots over the separable closure of K; we call such binary quartic forms *nondegenerate*.

We may also consider the following twisted action of $g \in \mathrm{GL}(V)$ on $q \in \mathrm{Sym}^4 V$:

$$(31) \qquad g \cdot q(w_1, w_2) = (\det g)^{-2} q((w_1, w_2)g)$$

for which the $\mathrm{SL}(V)$-invariants described above are preserved as well. This representation is $\mathrm{GL}(V)$ acting on $\mathrm{Sym}^4 V \otimes (\wedge^2 V)^{-2}$; we will sometimes denote it by the action of $\mathrm{GL}(V)^{(-2)}$ on binary quartic forms. Note that the stabilizer of this twisted action contains the diagonal $\mathbb{G}_m$ of $\mathrm{GL}(V)$ (i.e., scalar matrices), thereby inducing an action of $\mathrm{PGL}(V)$ on the space of binary quartic forms.

There is one more action we will consider, which is scaling by squares, i.e., $\gamma \in \mathbb{G}_m$ sends $q \in \mathrm{Sym}^4 V \otimes (\wedge^2 V)^{-2}$ to $\gamma^2 q$. We will denote this as the action of $2\mathbb{G}_m$ on binary quartics.

A nondegenerate binary quartic form q may be associated to a genus one curve C in the weighted projective space $\mathbb{P}(1, 1, 2)$ by the equation

$$(32) \qquad y^2 = q(w_1, w_2) = aw_1^4 + bw_1^3 w_2 + cw_1^2 w_2^2 + dw_1 w_2^3 + ew_2^4,$$

where w_1 and w_2 each have degree 1 and y has degree 2. Over the algebraic closure, the four roots of the binary quartic correspond to the four points of $\mathbb{P}(V^\vee)$ over which C ramifies; in other words, the subscheme of $\mathbb{P}(V^\vee) = \mathbb{P}^1$ cut out by q is the ramification locus of the two-to-one map $C \to \mathbb{P}(V^\vee)$. Nondegeneracy is clearly preserved by all of the group actions above.

From a nondegenerate binary quartic q, we thus obtain a smooth irreducible genus one curve C, as well as a degree 2 line bundle L on C, which is the pullback of $\mathcal{O}_{\mathbb{P}(V^\vee)}(1)$ to C. Then the space of sections $H^0(C, L)$ may be identified with the vector space V. The $\mathrm{GL}(V)^{(-2)} \times 2\mathbb{G}_m$-action on a binary quartic does not change the isomorphism class of the curve C obtained in this way. The Jacobian of the curve C associated to q has Weierstrass form

$$y^2 = x^3 - 27I(q)x - 27J(q)$$

(see, e.g., [AKM$^+$01, CF09]).

Conversely, given a smooth irreducible genus one curve C over K and a degree 2 line bundle L, the hyperelliptic map $\eta : C \to \mathbb{P}(H^0(C, L)^\vee)$ given by the complete linear series $|L|$ has a ramification divisor of degree 4 by the Riemann–Hurwitz Theorem. The branch divisor is a degree 4 subscheme of $\mathbb{P}(H^0(C, L)^\vee)$ defined over K, which recovers a binary quartic form over K, up to scaling. We next compute this scaling factor more precisely, in order to keep track of the group actions for Theorem 4.1 below.

Given the genus one curve $\pi : C \to \mathrm{Spec}\ K$ and a degree 2 line bundle L on C, we have the exact sequence

$$0 \longrightarrow \eta^* \Omega^1_{\mathbb{P}(H^0(C,L)^\vee)} \longrightarrow \Omega^1_C \longrightarrow \Omega^1_{C/\mathbb{P}(H^0(C,L)^\vee)} \longrightarrow 0,$$

and taking the pushforward under η gives the exact sequence

$$(33) \quad 0 \longrightarrow \Omega^1_{\mathbb{P}(H^0(C,L)^\vee)} \otimes \eta_* \mathcal{O}_C \longrightarrow \eta_* \Omega^1_C \longrightarrow \eta_* \Omega^1_{C/\mathbb{P}(H^0(C,L)^\vee)} \longrightarrow 0.$$

The first two terms of the sequence (33) are rank two bundles whose determinants have degrees -6 and -2, respectively. Taking determinants and twisting gives the map

$$\mathcal{O} \to (\Omega^1_{\mathbb{P}(H^0(C,L)^\vee)})^{\otimes -2} \otimes \omega_C^{\otimes 2}$$

where $\omega_C := \pi_* \Omega^1_C$ is the Hodge bundle for C. The induced map on cohomology is

$$(34) \qquad K \longrightarrow \mathrm{Sym}^4(H^0(C, L)) \otimes (\wedge^2(H^0(C, L)))^{\otimes(-2)} \otimes \omega_C^{\otimes 2}$$

and the image of $1 \in K$ is the desired binary quartic form. If we were not allowing the action of $2\mathbb{G}_m$ on binary quartics as well, then we would need to specify a differential to pin down the scaling of the binary quartic form.

In other words, there is an isomorphism between the open subset of $\mathrm{Sym}^4 V$ of nondegenerate binary quartic forms and the moduli problem for (C, L, ϕ, δ), where C is a smooth irreducible genus one curve, L is a degree 2 line bundle on C, $\phi : H^0(C, L) \to V$ is an isomorphism, and δ is a nonzero differential on C. By the computation (34), this isomorphism is $\mathrm{GL}(V) \times \mathbb{G}_m$-equivariant: the group acts on binary quartic forms as described above (namely, as $\mathrm{GL}(V)^{(-2)} \times 2\mathbb{G}_m$), while on the geometric data, $\mathrm{GL}(V)$ goes through the isomorphism ϕ to act on $H^0(C, L)$, and $\mathbb{G}_m$ acts by scaling on δ.

Thus, by descending to the quotient by these group actions, we obtain the correspondence of Theorem 4.1 below. The stabilizer of a binary quartic form here is exactly the automorphism group of the geometric data corresponding to the form. In order to describe the stabilizer, we first recall that there is a projective representation $E[2] \to \mathrm{PGL}(H^0(E, \mathcal{O}(2O)) = \mathrm{PGL}_2$ since translating by the 2-torsion points of E stabilizes the line bundle $\mathcal{O}(2O)$. We recall the definition of the Heisenberg group $\Theta_{E,2}$ for an elliptic curve E as the pullback of $\mathbb{G}_m \to \mathrm{GL}_2 \to \mathrm{PGL}_2$ along the map $E[2] \to \mathrm{PGL}_2$; it satisfies the following commutative diagram:

$$
(35) \qquad
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta_{E,2} & \longrightarrow & E[2] & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_2 & \longrightarrow & \mathrm{PGL}_2 & \longrightarrow & 0.
\end{array}
$$

More generally, for any n, we may define $\Theta_{E,n}$ analogously as an extension of $E[n]$ by $\mathbb{G}_m$. (See [Mum66] for more details on Heisenberg groups.)

Theorem 4.1. *Let V be a 2-dimensional vector space over K. Then nondegenerate $\mathrm{GL}(V)^{(-2)} \times 2\mathbb{G}_m$-orbits on $\mathrm{Sym}^4 V$ are in bijection with isomorphism classes of pairs (C, L), where C is a smooth irreducible genus one curve over K and L is a degree 2 line bundle on C. The stabilizer group (as a K-scheme) of a nondegenerate element of $\mathrm{Sym}^4 V$ corresponding to (C, L) is an extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\Theta_{\mathrm{Jac}(C),2}$, where $\mathrm{Jac}(C)$ is the Jacobian of the curve C, $\mathrm{Aut}(\mathrm{Jac}(C))$ is its automorphism group as an elliptic curve, and $\Theta_{\mathrm{Jac}(C),2}$ is the Heisenberg group as defined in (35).*

Remark 4.2. When the Jacobian of C does not have j-invariant 0 or 1728, the automorphism group of (C, L) is in fact just the direct product $\Theta_{\mathrm{Jac}(C),2} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{GL}(V) \times \mathbb{G}_m$. More generally, the automorphism group scheme described in Theorem 4.1 is not necessarily a split extension.

The set of isomorphism classes of pairs (C, L), where C is an E-torsor and L is a degree 2 line bundle on C, may be identified with the set $H^1(K, \Theta_{E,2})$, which may also be identified with the kernel of the *obstruction map* in the language of [O'N02, CFO$^+$08]. Therefore, given an elliptic curve

(36) $$E : y^2 = x^3 - 27Ix - 27J,$$

the set $H^1(K, \Theta_{E,2})$ is in bijective correspondence with the set of $\mathrm{GL}(V)^{(-2)}$-orbits of binary quartic forms q having invariants $I(q) = I$ and $J(q) = J$.

Remark 4.3. Theorem 4.1 may also be rephrased in terms of *divisors* on the genus one curves instead of *line bundles*; we also replace the group $\mathrm{GL}(V)^{(-2)} \times 2\mathbb{G}_m$ with $\mathrm{PGL}(V) \times 2\mathbb{G}_m$. In this case, the stabilizer of a binary quartic corresponding to a pair $(C, [D])$ for a genus one curve C with a degree 2 K-rational divisor D (of equivalence class $[D]$) is the group of K-points of the corresponding extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\mathrm{Jac}(C)[2]$. For example, if the j-invariant of $\mathrm{Jac}(C)$ is not 0 or 1728, then the stabilizer is just $\mathbb{Z}/2\mathbb{Z} \times \mathrm{Jac}(C)(K)[2]$. While the nondegenerate orbits of $\mathrm{Sym}^4 V$ under our original group $\mathrm{GL}(V)^{(-2)} \times 2\mathbb{G}_m$ and the group $\mathrm{PGL}(V) \times 2\mathbb{G}_m$ are identical, with the latter group action the stabilizer of an element matches the naturally defined automorphism group of the corresponding pair $(C, [D])$.

Furthermore, by considering only the $\mathrm{PGL}(V)$-action, the invariants of the binary quartic form are fixed, and so is a differential on the Jacobian. This revision of Theorem 4.1—i.e., the bijection between $\mathrm{PGL}(V)$-orbits of binary quartic forms and isomorphism classes of triples $(E, C, [D])$, where E is a fixed elliptic curve of the form (36)—is used in [BS15a] to prove that the average size of 2-Selmer groups for elliptic curves over $\mathbb{Q}$, ordered by height, is 3, which in turn implies that the average rank of elliptic curves (ordered in the same way) is bounded by 1.5.

Remark 4.4. By generalizing the above constructions to base schemes over $\mathbb{Z}[1/6]$ and letting V be a rank 2 free module over $\mathbb{Z}[1/6]$, we obtain an isomorphism between the nondegenerate substack of the double quotient stack $[2\mathbb{G}_m \setminus \mathrm{Sym}^4 V \otimes (\wedge^2 V)^{-2}/\mathrm{GL}(V)]$ and the quotient stack $[\mathscr{M}_{1,1}/\Theta_{E^{\mathrm{univ}},2}]$, where $\mathscr{M}_{1,1}$ is the moduli space of elliptic curves and $\Theta_{E^{\mathrm{univ}},2}$ is the theta group scheme for the universal elliptic curve E^{univ} over $\mathscr{M}_{1,1}$. Here, the T-points of the double quotient stack are triples $(\mathcal{V}, L_T, s)$, where $p : \mathcal{V} \to T$ is a rank 2 vector bundle over T, L_T is a line bundle on T, and s is a map $L_T^{\otimes 2} \to \mathrm{Sym}^4(\mathcal{V}) \otimes (\wedge^2 \mathcal{V})^{-2}$.

Analogous statements will be true for all of the other cases discussed in this section; we discuss this further in §4.5.

4.2. Ternary cubic forms

A *ternary cubic form* over K is a three-dimensional vector space V and an element f of $\mathrm{Sym}^3 V$; with a choice of basis $\mathfrak{B} = \{w_1, w_2, w_3\}$ for $V^\vee$, such a form may be represented as a homogeneous degree 3 polynomial

(37)
$$
\begin{aligned}
f(w_1, w_2, w_3) = {}& aw_1^3 + bw_2^3 + cw_3^3 + a_2 w_1^2 w_2 + a_3 w_1^2 w_3 \\
& + b_1 w_1 w_2^2 + b_3 w_2^2 w_3 + c_1 w_1 w_3^2 + c_2 w_2 w_3^2 + m w_1 w_2 w_3
\end{aligned}
$$

with coefficients in K. There is a natural action of $\mathrm{GL}(V)$ on the space of all ternary cubic forms by the standard action of $\mathrm{GL}(V)$ on V. The ring of $\mathrm{SL}(V)$-invariants of the space of ternary cubic forms is a polynomial ring generated by a degree 4 invariant $d_4 = S$ and a degree 6 invariant $d_6 = T$, and they may be computed by classical formulas (see [Fis06], for our choice of scaling). Thus, the coarse moduli space $\mathrm{Sym}^3 V /\!\!/ \mathrm{SL}(V)$ is birational to the affine plane $\mathbb{A}^2$ with coordinates d_4 and d_6.

For the twisted action of $\mathrm{GL}(V)$ on $\mathrm{Sym}^3 V$ where $g \in \mathrm{GL}(V)$ sends $f(X, Y, Z) \in \mathrm{Sym}^3 V$ to $(\det g)^{-1} f((X, Y, Z)g)$, the $\mathrm{SL}(V)$-invariants described above are also preserved. This representation is described more accurately as the action of $\mathrm{GL}(V)$ on $\mathrm{Sym}^3 V \otimes (\wedge^3 V)^{-1}$, and we will also sometimes denote it by the action of $\mathrm{GL}(V)^{(-1)}$ on $\mathrm{Sym}^3 V$ to indicate the -1-twist of the determinant. Note that this representation has a nontrivial kernel, namely the diagonal $\mathbb{G}_m$ of $\mathrm{GL}(V)$ (i.e., scalar matrices), so it induces a natural $\mathrm{PGL}(V)$-action on the space of ternary cubic forms.

We will also consider the action of $\mathbb{G}_m$ on $\mathrm{Sym}^3 V$ (or on $\mathrm{Sym}^3 V \otimes (\wedge^3 V)^{-1}$) by scaling. Scaling the form f by $\gamma \in \mathbb{G}_m$ scales each $\mathrm{GL}(V)^{(-1)}$-invariant by γ^d, where d is the degree of the invariant.

We claim that the nondegenerate subset of ternary cubic forms, up to the $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$-action, parametrizes genus one curves equipped with degree 3 line bundles, up to isomorphisms. In particular, a ternary cubic form f defines a curve $\iota : C := \{f = 0\} \hookrightarrow \mathbb{P}(V^\vee)$. We say that f a *nondegenerate* ternary cubic form if C is smooth, which occurs if and only if the degree 12 discriminant $\Delta(f) := (d_4^3 - d_6^2)/1728$ of f is nonzero. In this case, the curve C has genus one, and the pullback $\iota^* \mathcal{O}_{\mathbb{P}(V^\vee)}(1)$ is a degree 3 line bundle on C.

On the other hand, given a (smooth irreducible) genus one curve $\pi : C \to \mathrm{Spec}\, K$ and a degree 3 line bundle L on C, the embedding of C into $\mathbb{P}(H^0(C, L)^\vee) \cong \mathbb{P}^2$ gives rise to the exact sequence of sheaves

$$
0 \longrightarrow \mathcal{I}_C \longrightarrow \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)} \longrightarrow \mathcal{O}_C \longrightarrow 0
$$

on $\mathbb{P}(H^0(C,L)^\vee)$, where $\mathcal{I}_C$ is the ideal defining the curve C. Tensoring with the sheaf $\mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(3)$, taking cohomology, and then tensoring with $H^0(\mathbb{P}(H^0(C,L)^\vee), \mathcal{I}_C(3))^\vee$ gives the map

$$K \longrightarrow H^0(\mathbb{P}(H^0(C,L)^\vee), \mathcal{O}(3)) \otimes (\wedge^3(H^0(C,L)))^{-1} \otimes \omega_C,$$

where $\omega_C := \pi_* \Omega^1_C$ is the Hodge bundle for the curve C. The image of $1 \in K$ is an element of $\mathrm{Sym}^3(H^0(C,L)) \otimes (\wedge^3(H^0(C,L)))^{-1}$, i.e., a ternary cubic form with $V := H^0(C,L)$. Although the Hodge bundle ω_C is trivial over a field, if we did not include the $\mathbb{G}_m$-action here, we would need to specify a differential to pin down the scaling of the ternary cubic form.

These two functors between ternary cubic forms and pairs (C,L) are inverse to one another.

As in the binary quartic case, there is in fact an isomorphism between the nondegenerate subset of $\mathrm{Sym}^3 V$ and the moduli problem for (C,L,ϕ,δ), where C is a genus one curve, L is a degree 3 line bundle, $\phi : H^0(C,L) \to V$ is an isomorphism, and δ is a differential on C. This isomorphism is $\mathrm{GL}(V) \times \mathbb{G}_m$-equivariant, and so we obtain the following:

Theorem 4.5. *Let V be a 3-dimensional K-vector space. Then nondegenerate $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$-orbits of $\mathrm{Sym}^3 V$ are in bijection with isomorphism classes of pairs (C,L), where C is a smooth irreducible genus one curve over K and L is a degree 3 line bundle on C. The stabilizer group (as a K-scheme) of a nondegenerate element of $\mathrm{Sym}^3 V$ corresponding to (C,L) is an extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\Theta_{\mathrm{Jac}(C),3}$, where $\mathrm{Jac}(C)$ is the Jacobian of C, $\mathrm{Aut}(\mathrm{Jac}(C))$ is its automorphism group as an elliptic curve, and $\Theta_{\mathrm{Jac}(C),3}$ is the degree 3 Heisenberg group of $\mathrm{Jac}(C)$.*

Remark 4.6. More precisely, the stabilizer group of a nondegenerate element of $\mathrm{Sym}^3 V$ coincides with the automorphism group of the corresponding pair (C,L). Here, the automorphism group of the pair (C,L) consists of the K-points of the group scheme given by a possibly non-split extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\Theta_{\mathrm{Jac}(C),3}$.

For example, if C has a point O, and L is the line bundle $\mathcal{O}(3O)$, then the extension is indeed split, since for all automorphisms of C fixing O, the pullback of L is isomorphic to L. However, in general this extension will not split. For example, if C is a nontrivial torsor of its Jacobian, then the automorphism group of (C,L) is just $\Theta_{\mathrm{Jac}(C),3}$.

Note that the automorphism group of (C,L) as a *torsor* for $(\mathrm{Jac}(C), \mathcal{O}(3O))$ is always $\Theta_{\mathrm{Jac}(C),3}$.

Given a ternary cubic form f, the associated genus one curve C has Jacobian $E := \mathrm{Jac}(C)$ which is determined by the $\mathrm{SL}(V)$-invariants $d_4 = d_4(f)$ and $d_6 = d_6(f)$ (see [AKM$^+$01] for details). In Weierstrass form, the elliptic curve E may be expressed as

$$(38) \qquad E : y^2 = x^3 - 27d_4x - 54d_6.$$

The discriminant $\Delta(E)$ is then given by the formula

$$1728\Delta(E) = d_4^3 - d_6^2.$$

Note that d_4 and d_6 are scaled by the usual action of $\mathbb{G}_m$ on f, so they are only relative invariants for the action of the group $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$ on the orbit of f; however, all elliptic curves in this orbit are isomorphic, as E is isomorphic to the elliptic curve given by $y^2 = x^3 - 27\lambda^4 d_4 x - 54\lambda^6 d_6$ for any $\lambda \in K^*$.

Conversely, given two numbers $d_4, d_6 \in K$ such that $d_4^3 - d_6^2 \neq 0$, the $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$-orbits of $\mathrm{Sym}^3 V$ having *relative* invariants d_4 and d_6 are made up of ternary cubic forms having invariants $\gamma^4 d_4$ and $\gamma^6 d_6$ for $\gamma \in K^*$. Over an algebraically closed field, these ternary cubic forms comprise exactly one orbit, but over a general field they may break up into many K-orbits.

Given invariants $d_4, d_6 \in K$, one may specify an elliptic curve E, say in the form of (38). Then the $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$-orbits of ternary cubic forms over K having associated Jacobian E correspond to pairs (C, L) with Jacobian isomorphic to E. Such pairs (C, L) are twists of the elliptic curve E and the standard degree 3 line bundle $\mathcal{O}(3O)$ where O is the identity point on E. The K-rational pairs (C, L) with a choice of isomorphism $\mathrm{Jac}^0(C) \xrightarrow{\cong} E$ are exactly parametrized up to isomorphism by $H^1(K, \Theta_{E,3})$. Thus, the $\mathrm{GL}(V)^{(-1)}$-orbits of $\mathrm{Sym}^3 V$ with invariants d_4 and d_6 are in bijection with the pointed set $H^1(K, \Theta_{E,3})$, where E is the elliptic curve in (38). We recover the following proposition, which is Theorem 2.5 of [Fis06]:

Proposition 4.7. *Let E be an elliptic curve over K with Weierstrass form*

$$y^2 = x^3 - 27d_4x - 54d_6.$$

Then the set $H^1(K, \Theta_{E,3})$ parametrizes $\mathrm{GL}(V)^{(-1)}$-equivalence classes of $\mathrm{Sym}^3 V$ with invariants d_4 and d_6.

Remark 4.8. The difference between the $\mathrm{GL}(V)^{(-1)}$-orbits of $\mathrm{Sym}^3 V$ with invariants d_4 and d_6 and the $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$-orbits with the same relative invariants is subtle. For example, under the first action, a ternary cubic

form f and its negative $-f$ are not generally in the same orbit (but they are in the same $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$-orbit). While f and $-f$ cut out the same genus one curve C in the plane, they correspond to inverse elements in $H^1(K, \Theta_{\mathrm{Jac}(C),3})$; this exactly reflects the $\mathbb{Z}/2\mathbb{Z}$ in the automorphism group of any elliptic curve.

Remark 4.9. Analogously to Remark 4.3, we may replace line bundles with equivalence classes of divisors in the statement of Theorem 4.5 and the group $\mathrm{GL}(V)^{(-1)} \times \mathbb{G}_m$ with $\mathrm{PGL}(V) \times \mathbb{G}_m$. We may further only consider the action of $\mathrm{PGL}(V)$ to obtain a bijection between $\mathrm{PGL}(V)$-orbits of $\mathrm{Sym}^3 V$ and isomorphism classes of triples $(E, C, [D])$, where E is a fixed elliptic curve of the form (38) and C is an E-torsor with a rational degree 3 divisor D. The stabilizer of a nondegenerate element of $\mathrm{Sym}^3 V$ corresponding to $(E, C, [D])$ is the automorphism group of $(E, C, [D])$, namely $E[3](K)$.

In [BS15b], this bijection is used to prove that the average size of 3-Selmer groups for elliptic curves over $\mathbb{Q}$, ordered by height, is 4, implying an improved upper bound of 7/6 for the average rank of elliptic curves over $\mathbb{Q}$.

Remark 4.10. As in Remark 4.4, we actually have an isomorphism between the nondegenerate substack of the quotient stack

$$[\mathrm{Sym}^3 V \otimes (\wedge^3 V)^{-1}/\mathrm{GL}(V) \times \mathbb{G}_m]$$

and the quotient stack $[\mathscr{M}_{1,1}/\Theta_{E^{\mathrm{univ}},3}]$, where $\Theta_{E^{\mathrm{univ}},3}$ is the theta group scheme for the universal elliptic curve E^{univ} over $\mathscr{M}_{1,1}$. See §4.5 for more details.

4.3. Pairs of quaternary quadratic forms

Next, let V and W be vector spaces of dimensions 4 and 2, respectively, over K. We study the space $W \otimes \mathrm{Sym}^2 V$. With a choice of bases for both V and W, any element of $W \otimes \mathrm{Sym}^2 V$ may be represented as a pair of symmetric 4×4 matrices, say A and B. There is a natural action of $\mathrm{GL}(W) \times \mathrm{GL}(V)$ on this space, and the $\mathrm{SL}(W) \times \mathrm{SL}(V)$-invariants for this space form a polynomial ring generated by two invariants d_8 and d_{12} of degrees 8 and 12, respectively [AKM+01]. In particular, the $\mathrm{SL}(V)$-invariants of the element represented by the pair (A, B) of symmetric matrices are the coefficients of the binary quartic form $q(x, y) = \det(Ax + By)$ (see, e.g., [AKM+01, MSS96]), and the $\mathrm{SL}(W)$-invariants of this binary quartic form $q(x, y)$ are the polynomials $I(q)$ and $J(q)$ from §4.1.

We describe briefly how nondegenerate elements of this space naturally give genus one curves with degree 4 line bundles (see [MSS96] for an excellent exposition of the details). An element of $W \otimes \mathrm{Sym}^2 V$ represents a pencil (parametrized by $\mathbb{P}(W^\vee)$) of quadrics in $\mathbb{P}(V^\vee)$. If this pencil is nontrivial, its base locus is a curve C, which is of genus one if smooth, by adjunction. The curve C is smooth exactly when the discriminant $\Delta(q) = 4I(q)^3 - J(q)^2$ is nonzero, just as for binary quartic forms, and elements of $W \otimes \mathrm{Sym}^2 V$ giving smooth curves are called *nondegenerate*. Pulling back $\mathcal{O}_{\mathbb{P}(V^\vee)}(1)$ to the genus one curve C gives a degree 4 line bundle. Furthermore, the rulings on these quadrics parametrize a double cover D of $\mathbb{P}(W^\vee)$ ramified at the degree 4 subscheme given by the binary quartic form $q(x,y)$. This curve D is also a genus one curve, and in fact, as elements of $H^1(K, E)$, the class of D is double that of C.

On the other hand, starting with a genus one curve C and a degree 4 line bundle L, the embedding of C into $\mathbb{P}(H^0(C,L)^\vee) \cong \mathbb{P}^3$ gives rise to the exact sequence of sheaves

$$0 \longrightarrow \mathcal{I}_C \longrightarrow \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)} \longrightarrow \mathcal{O}_C \longrightarrow 0,$$

and twisting by $\mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(2)$ shows that $H^0(\mathbb{P}(H^0(C,L)^\vee), \mathcal{I}_C(2))$ is at least 2-dimensional. It is easy to check that for C to be a smooth irreducible genus one curve, this space is exactly 2-dimensional (e.g., by computing the free resolution for $\mathcal{O}_C$ over $\mathbb{P}(H^0(C,L)^\vee) \cong \mathbb{P}^3$). We thus obtain a 2-dimensional subspace of $\mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(2)$ (the space of quadratic forms on $\mathbb{P}^3$) as desired.

Therefore, we have an isomorphism between nondegenerate elements of $W \otimes \mathrm{Sym}^2 V$ and the moduli problem for triples (C, L, ϕ, ψ), where C is a genus one curve, L is a degree 4 line bundle, and $\phi : H^0(C,L) \to V$ and $\psi : H^0(\mathbb{P}(H^0(C,L)^\vee), \mathcal{I}_C) \to W^\vee$ are isomorphisms. The group $\mathrm{GL}(W) \times \mathrm{GL}(V)$ acts on $W \otimes \mathrm{Sym}^2 V$ in the standard way, and it acts on ϕ and ψ by the actions on V and $W^\vee$, respectively. Therefore, taking the quotients of both sides of this isomorphism by $\mathrm{GL}(W) \times \mathrm{GL}(V)$ gives a correspondence between the orbits and the isomorphism class of pairs (C, L).

Theorem 4.11. *Let W and V be K-vector spaces of dimensions 2 and 4, respectively. There exists a bijection from nondegenerate $\mathrm{GL}(W) \times \mathrm{GL}(V)$-orbits of $W \otimes \mathrm{Sym}^2 V$ and isomorphism classes of pairs (C, L), where C is a smooth irreducible genus one curve and L is a degree 4 line bundle on C. The stabilizer group (as a K-scheme) of a nondegenerate element of $W \otimes \mathrm{Sym}^2 V$ corresponding to (C, L) is an extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\Theta_{\mathrm{Jac}(C),4}$, where $\mathrm{Jac}(C)$ is the Jacobian of C, $\mathrm{Aut}(\mathrm{Jac}(C))$ is its automorphism group as an elliptic curve and $\Theta_{\mathrm{Jac}(C),4}$ is the degree 4 Heisenberg group of $\mathrm{Jac}(C)$.*

Remark 4.12. As in the ternary cubic case, the automorphism group of a pair (C, L) is made up of the K-points of the group scheme given by a possibly non-split extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\Theta_{\mathrm{Jac}(C),4}$. In this case, part of the extension splits more often, e.g., if the curve C has a degree 2 line bundle M, then the pair $(C, M^{\otimes 2})$ has automorphism group $\Theta_{\mathrm{Jac}(C),4} \rtimes \mathbb{Z}/2\mathbb{Z}$ if $\mathrm{Jac}(C)$ does not have j-invariant 0 or 1728.

Remark 4.13. Again, in Theorem 4.11, we may replace the line bundle L with the equivalence class of a rational degree 4 divisor D, and the group $\mathrm{GL}(W) \times \mathrm{GL}(V)$ with a subquotient (restricting to pairs (g_1, g_2) with $(\det g_1)(\det g_2)^2 = 1$ and quotienting by the remaining elements in the kernel of the multiplication map $\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ sending (γ_1, γ_2) to $\gamma_1 \gamma_2^2$). Then the stabilizer of a nondegenerate element of $W \otimes \mathrm{Sym}^2 V$ corresponding to $(E, C, [D])$ is $E[4](K)$. This correspondence is used in [BS13a] to compute the average size of the 4-Selmer group of elliptic curves over $\mathbb{Q}$.

As in the previous cases, the Jacobian of the curve C corresponding to an element of $W \otimes \mathrm{Sym}^2 V$ is given by its $\mathrm{SL}(W) \times \mathrm{SL}(V)$-invariants d_8 and d_{12}:

$$\mathrm{Jac}(C) : y^2 = x^3 - 27 d_8 x - 27 d_{12}.$$

This follows easily from the fact that d_8 and d_{12} are the $\mathrm{SL}(W)$-invariants $I(q)$ and $J(q)$ of the binary quartic form q.

4.4. Quintuples of 5×5 skew-symmetric matrices

The degree 5 problem was studied extensively by Fisher in [Fis, Fis08] and much of the following can be deduced from the work of Buchsbaum-Eisenbud in [BE82]. For completeness, we very briefly remind the reader of the constructions involved. In this section, let K be a field not of characteristic 2, 3, or 5.

Let V and W be 5-dimensional K-vector spaces. We consider the space $V \otimes \wedge^2 W$, which has $\mathrm{SL}(V) \times \mathrm{SL}(W)$-invariant ring generated by two generators d_{20} and d_{30} of degrees 20 and 30, respectively. An element of $V \otimes \wedge^2 W$, with a choice of bases for V and W, may be thought of as five 5×5 skew-symmetric matrices, or a single 5×5 skew-symmetric matrix of linear forms on $V^\vee$. Then generically the 4×4 Pfaffians intersect in a genus one curve in $\mathbb{P}(V^\vee) = \mathbb{P}^4$, and pulling back $\mathcal{O}_{\mathbb{P}(V^\vee)}(1)$ to this curve gives a degree 5 line bundle on the curve. The isomorphism class of the curve and the degree 5 line bundle are clearly $\mathrm{GL}(V) \times \mathrm{GL}(W)$-equivariant. The nondegeneracy required here is the nonvanishing of the degree 60 discriminant formed in the usual way from the generators of the invariant ring.

To construct an element of $V \otimes \wedge^2 W$ from a smooth irreducible genus one curve C and a degree 5 line bundle L, one identifies $V = H^0(C, L)$ and $W = H^0(\mathbb{P}(V^\vee), \mathcal{I}_C(2))$, where $\mathcal{I}_C$ is the ideal sheaf for C. Then one immediately obtains a section of $\mathcal{O}_{\mathbb{P}(V^\vee)}(1) \otimes \wedge^2 W$ from the free resolution

$$0 \to \mathcal{O}(5) \to \mathcal{O}(-3) \otimes W^\vee \to \mathcal{O}(-2) \otimes W \to \mathcal{O} \to \mathcal{O}_C$$

of $\mathcal{O}_C$ over $\mathbb{P}(H^0(C, L)^\vee)$.

Therefore, there is an isomorphism between elements of $V \otimes \wedge^2 W$ and the moduli problem parametrizing (C, L, ϕ, ψ), where C is a genus one curve, L is a degree 5 line bundle, and $\phi : H^0(C, L) \to V$ and $\psi : H^0(\mathbb{P}(H^0(C, L)^\vee), \mathcal{I}_C(2)) \to W$ are isomorphisms. Quotienting both sides by the natural actions of $\mathrm{GL}(V) \times \mathrm{GL}(W)$ gives

Theorem 4.14. *Let V and W be 5-dimensional K-vector spaces. Then there is a canonical bijection between nondegenerate $\mathrm{GL}(V) \times \mathrm{GL}(W)$-orbits of $V \otimes \wedge^2 W$ and isomorphism classes of pairs (C, L), where C is a genus one curve and L is a degree 5 line bundle on C. The stabilizer group (as a K-scheme) of a nondegenerate element of $V \otimes \wedge^2 W$ corresponding to (C, L) is an extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by $\Theta_{\mathrm{Jac}(C),5}$, where $\mathrm{Jac}(C)$ is the Jacobian of C, $\mathrm{Aut}(\mathrm{Jac}(C))$ is its automorphism group as an elliptic curve, and $\Theta_{\mathrm{Jac}(C),5}$ is the degree 5 Heisenberg group of $\mathrm{Jac}(C)$.*

Remark 4.15. As in the previous three cases, Theorem 4.14 may be rephrased using isomorphism classes of pairs $(E, C, [D])$, where now D is a degree 5 rational divisor on C, by replacing the group $\mathrm{GL}(V) \times \mathrm{GL}(W)$ with a subquotient (again, restricting to pairs (g_1, g_2) with $(\det g_1)(\det g_2)^2 = 1$ and quotienting by the remaining elements in the kernel of the multiplication map $\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ sending (γ_1, γ_2) to $\gamma_1 \gamma_2^2$). This correspondence is used in [BS13b] to determine the average size of the 5-Selmer group of elliptic curves over $\mathbb{Q}$.

Again, the Jacobian of the curve C associated to a nondegenerate element of $V \otimes \wedge^2 W$ is given by the $\mathrm{SL}(V) \times \mathrm{SL}(W)$-invariants d_{20} and d_{30}:

$$\mathrm{Jac}(C) : y^2 = x^3 + d_{20}x + d_{30}.$$

See [Fis08] for details and methods for computing these invariants.

4.5. Some remarks on different bases

This short section may be safely skipped for readers interested in the main theorems of this paper over fields K (as opposed to more general base rings

or schemes). Here, we simply comment on how one can vary the base schemes to study the moduli problems in Section 4.

All of the constructions discussed in this section may be made precise over arbitrary $\mathbb{Z}[1/30]$-schemes S. In particular, let $\mathcal{M}_d$ denote the moduli stack of genus one curves with degree d line bundles. Then for $2 \le d \le 5$, we claim that $\mathcal{M}_d$ is isomorphic to an open substack of a certain quotient stack $[V/G]$ for a group G and representation V of G. The constructions are straightforward generalizations of those over fields in §4.1 through §4.4, e.g., as in Remark 4.4.

For example, the case of ternary cubics is discussed in detail in [Ho09, §2.A.2]: the idea is that the T-points of the double quotient $[\mathbb{G}_m \setminus \mathrm{Sym}^3 V \otimes (\wedge^3 V)^{-1}/\mathrm{GL}(V)]$ are triples $(\mathcal{V}, L_T, f)$, where $\mathcal{V}$ is a rank 3 vector bundle over T, L_T is a line bundle on T, and f is a section of $\mathrm{Sym}^3 \mathcal{V} \otimes (\wedge^3 \mathcal{V})^{-1} \otimes L_T$, and nondegenerate triples correspond to genus one curves over T with degree 3 line bundles. The curve C is the zero set of the section of f in $\mathbb{P}(\mathcal{V}^\vee)$, and the line bundle L is the pullback of $\mathcal{O}_{\mathbb{P}(\mathcal{V}^\vee)}(1)$ via $C \to \mathbb{P}(\mathcal{V}^\vee)$; conversely, given the curve $\pi : C \to T$ and L, the construction gives the vector bundle $\pi_* L$ with $L_T := \pi_* \Omega^1_{C/T}$ and an appropriate section.

In each of these cases $2 \le d \le 5$, because the groups G appearing have vanishing Galois cohomology group $H^1(K, G)$, this description of $\mathcal{M}_d$ as an open substack of $[V/G]$ immediately implies that isomorphism classes of objects parametrized by $\mathcal{M}_d(K)$ are in bijection with the nondegenerate elements of $V(K)/G(K)$.

In the remainder of this paper, even though we restrict our attention to working over a base field K not of characteristic 2 or 3, most of the constructions we describe may be generalized to other base schemes. Just as for $\mathcal{M}_d$ here, one may show that the moduli spaces we encounter, of genus one curves with extra data, may be given as open substacks of quotient stacks.

5. Representations associated to degree 3 line bundles

In this section, we study a class of representations whose orbits are related to genus one curves with degree 3 line bundles. The main results in this section are summarized in Section 3.

We begin by studying the space of Rubik's cubes, which is one of the fundamental examples of this paper, and some of its simpler variants. The orbit space for Rubik's cubes (also called $3 \times 3 \times 3$ boxes) is related to the moduli space of genus one curves with two non-isomorphic degree 3 line bundles. This may also be identified with the moduli space of genus one

curves with a single degree 3 line bundle and one nonzero point on the Jacobian (lying in the appropriate subgroup).

In §5.3, we then recall the theory of cubic Jordan algebras, in preparation for the general case. The main general theorem is in §5.4, where we describe how the orbit spaces of these representations, built from cubic Jordan algebras, are moduli spaces for genus one curves with degree 3 line bundles and additional vector bundles. In later subsections, we then explain how to recover the earlier cases from the general theorem, and we also describe another special case that gives rank 2 vector bundles on genus one curves.

Many of the orbit problems described in this section are used in [BH12] to determine average sizes of 3-Selmer groups in certain families of elliptic curves over $\mathbb{Q}$.

5.1. Rubik's cubes, or $3 \times 3 \times 3$ boxes

We study an important example of a representation whose orbits naturally produce genus one curves with degree 3 line bundles. This representation was studied by K. Ng in [Ng95] over $\mathbb{C}$, and we extend his results to more general fields K. The main theorems of this section (Theorem 5.1 and Corollary 5.4) are joint with C. O'Neil.

Let V_1, V_2, and V_3 be three-dimensional K-vector spaces, so the group $G := \mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$ acts on the representation $V := V_1 \otimes V_2 \otimes V_3$. The following theorem, which is proved for $K = \mathbb{C}$ in [Ng95], describes the orbits of these "Rubik's cubes" over more general fields K. Here, nondegeneracy is equivalent to the nonvanishing of a degree 36 invariant, which we will describe in more detail below.

Theorem 5.1. *Let V_1, V_2, and V_3 be 3-dimensional vector spaces over K. Then nondegenerate G-orbits of $V_1 \otimes V_2 \otimes V_3$ are in bijection with isomorphism classes of quadruples (C, L_1, L_2, L_3), where C is a genus one curve over K and L_1, L_2, and L_3 are degree 3 line bundles on C with L_1 not isomorphic to L_2 or L_3 and satisfying $L_1^{\otimes 2} \cong L_2 \otimes L_3$.*

Note that the action of the group G on V is clearly not faithful: the kernel of the multiplication map

$$\mathbb{G}_m(V_1) \times \mathbb{G}_m(V_2) \times \mathbb{G}_m(V_3) \to \mathbb{G}_m \subset \mathrm{GL}(V),$$

where each $\mathbb{G}_m(V_i)$ is the group of scalar transformations of V_i for $i = 1, 2, 3$, fixes every element in $V_1 \otimes V_2 \otimes V_3$. For the sole purpose of classifying the orbits, this does not matter, since the orbits of G and of the quotient by this

kernel on the representation V are identical. However, this kernel, isomorphic to $\mathbb{G}_m^2$, shows up as part of the automorphism group of the geometric data; in particular, the stabilizer in G of a generic nondegenerate element of $V_1 \otimes V_2 \otimes V_3$ giving the curve C corresponds to the K-points of an extension H of the group scheme $\mathrm{Jac}(C)[3]$ by this $\mathbb{G}_m^2$. More generally, the stabilizer of a nondegenerate element consists of the K-points of a possibly non-split extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by the group scheme H. For each nondegenerate element, the stabilizer group coincides exactly with the group of automorphisms of the geometric data (if we also record the isomorphism $L_1^{\otimes 2} \cong L_2 \otimes L_3$ in Theorem 5.1).

The rest of this section is devoted to describing the construction of the genus one curve and its line bundles from an orbit. In particular, we prove Theorem 5.1.

5.1.1. Geometric construction.

We first describe the construction of the genus one curve and the line bundles from a G-orbit. Let $\mathcal{A} \in V = V_1 \otimes V_2 \otimes V_3$, so $\mathcal{A}$ induces a linear map from $V_1^\vee$ to $V_2 \otimes V_3$. There is a natural *determinantal* cubic hypersurface Y in $\mathbb{P}(V_2 \otimes V_3)$; with the choice of bases for V_2 and V_3, it can be described as the vanishing of the determinant of the 3×3 matrices that comprise $V_2 \otimes V_3$. Then the intersection of Y with the image of $\mathbb{P}(V_1^\vee) \to \mathbb{P}(V_2 \otimes V_3)$ is generically a cubic curve C_1 on the image of $\mathbb{P}(V_1^\vee)$, given as the vanishing of a covariant ternary cubic form in $\mathrm{Sym}^3 V_1$.

In other words, the curve C_1 is a determinantal variety, given by the determinant of a matrix of linear forms on $\mathbb{P}(V_1^\vee)$. Explicitly, with a choice of bases for V_1, V_2, and V_3, one can denote $\mathcal{A}$ as a $3 \times 3 \times 3$ cube $(a_{rst})_{1 \leq r,s,t \leq 3}$ of elements $a_{rst} \in K$. Then this ternary cubic form in $\mathrm{Sym}^3 V_1$ may be written simply as

$$f_1(v) := \det(\mathcal{A}(v, \cdot, \cdot)),$$

for $v \in V_1^\vee$. One may similarly define cubic curves $C_2 \subset \mathbb{P}(V_2^\vee)$ and $C_3 \subset \mathbb{P}(V_3^\vee)$, cut out by ternary cubic forms $f_2 \in \mathrm{Sym}^3 V_2$ and $f_3 \in \mathrm{Sym}^3 V_3$.

We call a Rubik's cube $\mathcal{A}$ *nondegenerate* if the variety C_1 (equivalently, C_2 or C_3) thus defined is smooth and one-dimensional, which corresponds to the nonvanishing of a degree 36 polynomial in a_{rst}. This polynomial is called the *discriminant* of the Rubik's cube $\mathcal{A}$, and it coincides with the usual degree 12 discriminant $\Delta(f_1)$ of the ternary cubic form f_1 (which is equal to $\Delta(f_2)$ and $\Delta(f_3)$).

If $\mathcal{A}$ is nondegenerate, then the degree 3 plane curve C_1 is smooth of genus one. For all points $w^\dagger \in C_1$, we claim that the singular matrix

$\mathcal{A}(w^\dagger, \cdot, \cdot)$ has exactly rank 2. If not, then the 2×2 minors of $\mathcal{A}(w, \cdot, \cdot)$ would vanish on $w^\dagger$, and so would all the partial derivatives

$$\frac{\partial f}{\partial w_i}\bigg|_{w=w^\dagger} = \sum_{s,t=1}^{3} a_{ist} A_{st}^*(w^\dagger)$$

where $A_{st}^*(w^\dagger)$ is the (s,t)th 2×2 minor of $\mathcal{A}(w^\dagger, \cdot, \cdot)$. Thus, since C_1 was assumed to be smooth, we see that the rank of the matrix $\mathcal{A}(w^\dagger, \cdot, \cdot)$ cannot drop by two.

In other words, the nondegeneracy condition is equivalent to the condition that the image of $\mathbb{P}(V_1^\vee)$ in $\mathbb{P}(V_2 \otimes V_3)$ not intersect the image of the Segre variety $\mathbb{P}(V_2) \times \mathbb{P}(V_3) \hookrightarrow \mathbb{P}(V_2 \otimes V_3)$. In the sequel, we assume that $\mathcal{A}$ is nondegenerate. (Note that nondegeneracy is preserved by the group action.)

Given a nondegenerate Rubik's cube $\mathcal{A}$, define the variety

$$C_{12} := \{(w,x) \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) : \mathcal{A}(w,x,\cdot) = 0\} \subset \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee).$$

Because $\mathcal{A}$ is a trilinear form and the locus on which it vanishes in $V_1 \times V_2$ is invariant under scaling, this is a well-defined locus in $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$. Since $\mathcal{A}$ is nondegenerate, the projection

$$C_{12} \longrightarrow \mathbb{P}(V_1^\vee)$$

is an isomorphism onto C_1. The inverse map takes a point $w \in C_1 \subset \mathbb{P}(V_1^\vee)$ to the pair $(w,x) \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$, where x corresponds to the exactly one-dimensional kernel of the linear map $\mathcal{A}(w, \cdot, \cdot) \in V_2 \otimes V_3 \cong \mathrm{Hom}(V_2^\vee, V_3)$. This map $C_1 \to C_{12}$ is algebraic, as this kernel is given as a regular map by the 2×2 minors of the matrix $\mathcal{A} \lrcorner w$. Therefore, by dimension considerations, the curve C_{12} is the complete intersection of three bidegree $(1,1)$ forms on $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) = \mathbb{P}^2 \times \mathbb{P}^2$. Similarly, the projection from C_{12} to $\mathbb{P}(V_2^\vee)$ is an isomorphism onto C_2, which shows that C_1 and C_2 are isomorphic.

We may also consider the curves

$$C_{13} := \{(w,y) \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_3^\vee) : \mathcal{A}(w,\cdot,y) = 0\}$$
$$C_{23} := \{(x,y) \in \mathbb{P}(V_2^\vee) \times \mathbb{P}(V_3^\vee) : \mathcal{A}(\cdot,x,y) = 0\}$$

and the analogous maps between C_i, C_3, and C_{i3} for $i = 1$ or 2 are also isomorphisms. Thus, all the curves C_1, C_2, C_3, C_{12}, C_{13}, and C_{23} are isomorphic, and the nondegeneracy condition is equivalent to the smoothness

of any or all of these curves. The diagram

(39)

summarizes the relationships between these curves. By construction, the maps τ_i^j and τ_j^i are inverses to one another. These maps from the curve C_1 to each projective space give the degree 3 line bundles

$$L_1 := \iota_1^* \mathcal{O}_{\mathbb{P}(V_1^\vee)}(1)$$
$$L_2 := (\iota_2 \circ \tau_1^2)^* \mathcal{O}_{\mathbb{P}(V_2^\vee)}(1)$$
$$L_3 := (\iota_3 \circ \tau_1^3)^* \mathcal{O}_{\mathbb{P}(V_3^\vee)}(1)$$

on C_1. For $1 \leq i \leq 3$, all three dimensions of sections of the degree 3 bundle L_i arise from pulling back sections from $\mathcal{O}_{\mathbb{P}(V_i^\vee)}(1)$.

Lemma 5.2. *The degree 3 line bundle L_1 on C_1 is not isomorphic to either of the line bundles L_2 or L_3.*

Proof. It suffices, by symmetry, to show that L_1 and L_2 are not isomorphic line bundles. If $L_1 \cong L_2$, then the curve C_{12} would lie on a diagonal of $\mathbb{P}^2 \times \mathbb{P}^2 = \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$, and with an identification of the bases for V_1 and V_2, we have $\mathcal{A}(w, w, \cdot) = 0$ for all $w \in C_1$. Because C_1 spans $\mathbb{P}(V_1^\vee)$, we must have that $\mathcal{A}(\cdot, \cdot, y)$ is a skew-symmetric 3×3 matrix for any $y \in \mathbb{P}(V_3^\vee)$. Since odd-dimensional skew-symmetric matrices have determinant zero, we would have $C_3 = \mathbb{P}(V_3^\vee)$, which is a contradiction. $\square$

Lemma 5.3. *The line bundles L_1, L_2, L_3 on C_1 defined above satisfy the relation*

(40) $$L_1 \otimes L_1 \cong L_2 \otimes L_3.$$

Proof. For $w \in C_1 \subset \mathbb{P}(V_1^\vee)$, each coordinate of $\tau_1^2(w) \in \mathbb{P}(V_2^\vee)$ is given by the 2×2 minors $A_{ij}^*(w)$ of $\mathcal{A}(w, \cdot, \cdot)$ for some fixed j where not all $A_{ij}^*(w)$ vanish. Let D_2 be an effective degree 3 divisor on C_1 such that $\mathcal{O}(D_2) \cong L_2$. Then the points of D_2 (defined over an appropriate extension of K) are the preimage on C_1 of the intersection of a hyperplane with the image of the curve C_{12} in $\mathbb{P}(V_2^\vee)$; in particular, we may choose D_2, without loss of generality, to be the divisor defined by the locus where a particular minor, say $A_{11}^*(w)$, vanishes on the curve C_1 but at least one $A_{i1}^*(w)$ is nonzero. Similarly, we may choose a divisor D_3 such that $\mathcal{O}(D_3) \cong L_3$ to be the points $w \in C_1$ where $A_{11}^*(w) = 0$ but not all other $A_{j1}^*(w)$ vanish. Then the points of the degree 6 effective divisor $D_2 + D_3$ are exactly the intersection of the curve C_1 and $A_{11}^*(w) = 0$, and the line bundle $\mathcal{O}(D_2 + D_3)$ is isomorphic to the pullback of $\mathcal{O}_{\mathbb{P}(V_1^\vee)}(2)$ to C_1.   □

The composition maps arising from traversing the inner triangle in (39), such as

$$\alpha_{123} := \tau_3^1 \circ \tau_2^3 \circ \tau_1^2 : C_1 \longrightarrow C_1,$$

are not the identity map. A calculation using Lemma 5.3 and its symmetric analogues shows that the automorphism α_{123} of C_1 is given by translation by the point P_{123} in $\mathrm{Jac}(C_1)$ corresponding to the degree 0 line bundle $L_2 \otimes L_1^{-1} \in \mathrm{Pic}^0(C_1)$. In particular, Lemma 5.3 and its symmetric analogues imply that each of the maps τ_1^2, τ_2^3, and τ_3^1 is an isomorphism where the pullback of the appropriate $\mathcal{O}_{\mathbb{P}^2}(1)$ between the target embedding and the source differs by the same degree 0 line bundle $L_2 \otimes L_1^{-1}$. Thus, the pullback of $L_1 = \iota_1^* \mathcal{O}_{\mathbb{P}(V_1^\vee)}$ along the composition α_{123} differs from L_1 itself by $(L_2 \otimes L_1^{-1})^{\otimes 3}$ (equivalently, by $3P_{123}$ if written additively in $\mathrm{Jac}(C_1)$), so the map α_{123} corresponds to translation by the point $P_{123} \in \mathrm{Jac}(C_1)$.

More generally, the analogous three-cycle α_{ijk} is the automorphism of C_i given by translation by a point $P_{ijk} \in \mathrm{Pic}^0(C_i)$, where P_{ijk} is the image of the point $\mathrm{sgn}(ijk)P_{123} = \pm P_{123} \in \mathrm{Jac}(C_1)$ under the canonical isomorphism $\mathrm{Jac}(C_1) \to \mathrm{Jac}(C_i)$.

5.1.2. Bijections. Because the geometric constructions in the previous section are G-invariant, we have shown that a G-orbit of V produces a genus one curve C with three degree 3 line bundles L_1, L_2, L_3, such that $L_1^2 \cong L_2 \otimes L_3$ and L_1 is not isomorphic to L_2 or L_3. We show that this data exactly determines a G-orbit of V.

Proof of Theorem 5.1. We have already shown that there is a well-defined map Φ from G-orbits of nondegenerate elements of V to the listed geometric data. In the other direction, given such a quadruple (C, L_1, L_2, L_3), we

consider the multiplication map (i.e., the cup product on cohomology)

$$(41) \qquad \mu_{12} : H^0(C, L_1) \otimes H^0(C, L_2) \longrightarrow H^0(C, L_1 \otimes L_2).$$

A simple case of [Mum70, Theorem 6] shows that μ is surjective. Thus, by Riemann-Roch, the kernel of μ_{12} has dimension $9 - 6 = 3$. Now let $V_1 := H^0(C, L_1)$, $V_2 := H^0(C, L_2)$, and $V_3 := (\ker(\mu_{12}))^\vee$, so the injection

$$\ker(\mu_{12}) \hookrightarrow H^0(C, L_1) \otimes H^0(C, L_2)$$

gives an element of $\mathrm{Hom}(\ker(\mu_{12}), H^0(C, L_1) \otimes H^0(C, L_2)) \cong V_1 \otimes V_2 \otimes V_3$.

If quadruples (C, L_1, L_2, L_3) and (C', L_1', L_2', L_3') are equivalent, then there is an isomorphism $\sigma : C \to C'$ such that $\sigma^* L_i' \cong L_i$ for $1 \leq i \leq 3$. The isomorphisms induced on the spaces of sections, e.g., $H^0(C, L_1) \xrightarrow{\cong} H^0(C', L_1')$, commute with the multiplication maps, so the Rubik's cubes constructed by their kernels differ only by choices of bases.

We check that the two functors between G-orbits of V and the equivalence classes of quadruples are inverse to one another. Given a quadruple (C, L_1, L_2, L_3) of the appropriate type, let the images of the natural embeddings be $C_1 \subset \mathbb{P}(H^0(C, L_1)^\vee)$, $C_2 \subset \mathbb{P}(H^0(C, L_2)^\vee)$, and $C_{12} \subset \mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee)$. We construct the desired trilinear form $\mathcal{A} \in H^0(C, L_1) \otimes H^0(C, L_2) \otimes (\ker \mu_{12})^\vee$ as above. Now let

$$C_1' := \{w \in \mathbb{P}(H^0(C, L_1)^\vee) : \det \mathcal{A}(w, \cdot, \cdot) = 0\} \subset \mathbb{P}(H^0(C, L_1)^\vee)$$
$$C_2' := \{x \in \mathbb{P}(H^0(C, L_2)^\vee) : \det \mathcal{A}(\cdot, x, \cdot) = 0\} \subset \mathbb{P}(H^0(C, L_2)^\vee)$$
$$C_{12}' := \{(w, x) \in \mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee) : \mathcal{A}(w, x, \cdot) = 0\}$$
$$\subset \mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee)$$

be the varieties cut out by the trilinear form $\mathcal{A}(\cdot, \cdot, \cdot)$.

We claim that $C_1 = C_1'$, $C_2 = C_2'$, and $C_{12} = C_{12}'$ as sets and thus as varieties, which implies that the curve C_1' is isomorphic to C and that the line bundles on C_1' defined as pullbacks of $\mathcal{O}(1)$ on $\mathbb{P}(H^0(C, L_1)^\vee)$ and $\mathbb{P}(H^0(C, L_2)^\vee)$ are isomorphic to the pullbacks of L_1 and L_2, respectively, via the isomorphism $C \xrightarrow{\cong} C_1'$. For all $(w, x) \in C_{12}$, the construction of $\mathcal{A}$ as the kernel of μ_{12} implies that $\mathcal{A}(w, x, \cdot) = 0$, so C_{12}' contains C_{12} and also $C_1' \supset C_1$ and $C_2' \supset C_2$.

Now either the polynomial $\det \mathcal{A}(w, \cdot, \cdot)$ or $\det \mathcal{A}(\cdot, x, \cdot)$ is not identically 0. If they both were identically 0, then $\mathcal{A}(w, x, \cdot) = 0$ for all $(w, x) \in \mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee)$, which is a contradiction. Without loss of

generality, assume $\det \mathcal{A}(w, \cdot, \cdot)$ is not identically zero. Then both C_1' and C_1 are given by nonzero degree 3 polynomials and thus define the same variety, so C_1' is a smooth irreducible genus one curve in $\mathbb{P}^2 = \mathbb{P}(H^0(C, L_1)^\vee)$. Because C_1' is smooth, the trilinear form $\mathcal{A}$ is nondegenerate, and C_{12}' is also smooth and irreducible, hence exactly the same variety as C_{12}.

It remains to show that the geometric data coming from a Rubik's cube produces the G-orbit of the same cube again. Given nondegenerate $\mathcal{A} \in V_1 \otimes V_2 \otimes V_3$, where V_i are 3-dimensional vector spaces for $1 \leq i \leq 3$, we have described the associated quadruple (C, L_1, L_2, L_3) as the image of Φ. Then the vector spaces V_i and $H^0(C, L_i)$ are naturally isomorphic for $i = 1$, 2, and $V_3^\vee$ can be identified with the kernel of μ_{12}. With these identifications, the Rubik's cube constructed from this quadruple is well-defined and G-equivalent to the original $\mathcal{A}$. $\qquad\square$

We may also rewrite the geometric data in Theorem 5.1 in terms of K-points on the Jacobian of C. Indeed, instead of keeping track of the line bundles L_2 and L_3, it suffices to record the difference of the line bundles as a degree 0 line bundle, which corresponds to a point in the Jacobian. This yields another version of Theorem 3.1:

Corollary 5.4. *Let V_1, V_2, and V_3 be 3-dimensional vector spaces over K. Then nondegenerate G-orbits of $V_1 \otimes V_2 \otimes V_3$ are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve over K, L is a degree 3 line bundle on C, and $0 \neq P \in \mathrm{Pic}^0(C)(K) \subset \mathrm{Jac}(C)(K)$.*

5.1.3. Invariant theory. The ring of $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2) \times \mathrm{SL}(V_3)$-invariants of the representation $V_1 \otimes V_2 \otimes V_3$ for three-dimensional vector spaces V_1, V_2, V_3 is generated freely by polynomial invariants of degrees 6, 9, and 12, respectively. These have interpretations in terms of the geometric data described in the bijection of Corollary 5.4.

Proposition 5.5. *There exists a choice of normalization for the relative invariants c_6, c_9, c_{12} such that given a nondegenerate tensor in $V_1 \otimes V_2 \otimes V_3$ corresponding to (C, L, P) as in Corollary 5.4, the Jacobian of C may be expressed in generalized Weierstrass form as*

$$(42) \qquad E : y^2 + c_9 y = x^3 + c_6 x^2 + c_{12} x$$

and the point P on E is given by $(0,0)$.

The $\mathrm{SL}(V_1)$-invariants of the ternary cubic $f = f_1$ given by (C, L) are also clearly invariants for the whole space $V_1 \otimes V_2 \otimes V_3$, since f is fixed

under the action of $\mathrm{SL}(V_2) \times \mathrm{SL}(V_3)$. The polynomials $d_4(f)$ and $d_6(f)$ have degrees 12 and 18 as invariants of $V_1 \otimes V_2 \otimes V_3$. One may check that with the normalizations above, we have

$$d_4(f) = 16c_6^2 - 48c_{12} \quad \text{and} \quad d_6(f) = -64c_6^3 - 216c_9^2 + 288c_6c_{12}$$

so that (E, P) may be taken by linear changes of variables to the elliptic curve

$$E' : y^2 = x^3 - 27d_4(f)x - 54d_6(f)$$

with the point P becoming $(12c_6, 108c_9)$ on E'. This recovers the interpretation of the invariants described in §3.3.

One proof of the above proposition is obtained by computing the expression for the point P in terms of the orbit. We omit these computations, as all the invariants have a very large number of terms![2] A more abstract argument is simple: any elliptic curve with a non-identity rational point P may be written in the form (42), for some c_6, c_9, $c_{12} \in K$, where $(0, 0)$ is the point P. Then the numbers c_6, c_9, c_{12} are algebraic invariants of the geometric data (C, L_1, L_2, L_3) coming from a Rubik's cube, up to scaling by λ^6, λ^9, λ^{12}, respectively, for some $\lambda \in K^*$. Thus, these must be relative G-invariants of the representation V.

Given this interpretation of the invariants, we may specialize the correspondence for a particular elliptic curve E over K. We think of c_6, c_9, and c_{12} as polynomial functions of the corresponding degree from $V_1 \otimes V_2 \otimes V_3 \to K$ (which are, of course, $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2) \times \mathrm{SL}(V_3)$-invariant). Let $d_{12} = 16c_6^2 - 48c_{12}$ and $d_{18} = -64c_6^3 - 216c_9^2 + 288c_6c_{12}$.

Corollary 5.6. *Let E be an elliptic curve over K, given in Weierstrass form as*

$$y^2 = x^3 - 27a_4x - 54a_6.$$

Then the subset of triples $(\alpha_1, \alpha_2, \alpha_3) \in H^1(K, \Theta_{E,3})^3$ such that

(i) *the sum of the images of α_i under the natural map $H^1(K, \Theta_{E,3}) \to H^1(K, E[3])$ is zero,*

(ii) *α_1 is not equal to α_2 or α_3, and*

(iii) *the images of α_i under $H^1(K, \Theta_{E,3}) \to H^1(K, E[3]) \to H^1(K, E)$ all coincide*

---

[2]The degree 9 invariant is also known as the Strassen invariant and has a simple closed form expression [Stu09]. If ϕ is represented by three 3×3 matrices M_1, M_2, and M_3 by "slicing" in any of the three directions with $\det M_2 \neq 0$, then $c_9(\phi)$ may be given by the expression $(\det M_2^2(M_1M_2^{-1}M_3 - M_3M_2^{-1}M_1))$.

are in bijection with the $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$*-orbits of* $V_1 \otimes V_2 \otimes V_3$ *that have representatives* $\mathcal{A}$ *with* $d_{12}(\mathcal{A}) = \lambda^{12} a_4$ *and* $d_{18}(\mathcal{A}) = \lambda^{18} a_6$, *for some nonzero* $\lambda \in K^*$.

The condition on the invariants merely ensures that both sides of the bijection are restricted to exactly those Rubik's cubes corresponding to curves with Jacobian E.

Given any elliptic curve over K, there may be no such $(\alpha_1, \alpha_2, \alpha_3)$, for example, if the elliptic curve does not have any non-identity rational points. However, given an elliptic curve E over K of the form (42), there always exists a G-orbit of V where E is the Jacobian of the associated genus one curve. In particular, taking C to simply be the trivial torsor E with the degree 3 line bundles $\mathcal{O}(3O)$ and $\mathcal{O}(2O + P)$, where P is the point $(0,0)$ on E, constructs such an orbit.

Corollary 5.7. *The map from nondegenerate orbits* $V(K)/G(K)$ *to elliptic curves of the form*

$$y^2 + c_9 y = x^3 + c_6 x^2 + c_{12} x$$

with c_6, c_9, $c_{12} \in K$, *obtained by taking the Jacobian of the genus one curve associated to the orbit, is surjective.*

For a global number or function field K, if we restrict to orbits where the curve C is everywhere locally soluble (meaning that C has a K_ν-point for every place ν of K), Corollary 5.6 simplifies significantly and yields a bijection between certain orbits and elements of the 3-Selmer group of elliptic curves of the form (42). See [BH12] for details and applications.

5.2. Symmetric Rubik's cubes

In this subsection, we study "symmetrized" Rubik's cubes. There is a natural S_3-action on each Rubik's cube, obtained by permuting the factors V_i for $i = 1$, 2, 3, and we study the subset of Rubik's cubes that are invariant under the subgroup $S_2 \subset S_3$, or under all of S_3.

5.2.1. Doubly symmetric Rubik's cubes. The simplest case is that of doubly symmetric Rubik's cubes, i.e., triples of 3×3 symmetric matrices. This is the subrepresentation $V_1 \otimes \mathrm{Sym}_2 V_2 \subset V_1 \otimes V_2 \otimes V_2$ of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$, for three-dimensional K-vector spaces V_1 and V_2. Away from characteristic 2, this is the same as the quotient $V_1 \otimes \mathrm{Sym}^2 V_2$. We give the orbit parametrization for this space in the following basis-free version of Theorem 3.3:

Theorem 5.8. *Let V_1 and V_2 be 3-dimensional vector spaces over K. Then the nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$-orbits of $V_1 \otimes \mathrm{Sym}_2 V_2$ are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve over K, L is a degree 3 line bundle on C, and P is a nonzero 2-torsion point of $\mathrm{Jac}(C)(K)$.*

Proof. Given an element $\mathcal{A}$ of $V_1 \otimes \mathrm{Sym}_2 V_2 \subset V_1 \otimes V_2 \otimes V_2$, we construct the genus one curve C and line bundles L_1, L_2, L_3 as before. Because of the symmetry, the line bundles L_2 and L_3 coincide. The relation $L_1^{\otimes 2} \cong L_2 \otimes L_3$ and the fact that $L_1 \not\cong L_2$ shows that the point $P := L_1 \otimes L_2^{-1}$ is a nonzero 2-torsion point of $\mathrm{Jac}(C)$. As all 2-torsion points of $E(K)$ are contained in $\mathrm{Pic}^0(C)(K)$, requiring P to be in $\mathrm{Pic}^0(C)(K)$ is not an extra condition.

On the other hand, given such (C, L, P) and setting $L' = L \otimes P$, the proof of Theorem 5.1 shows that the quadruple $(C, L_1, L_2, L_3) = (C, L, L', L')$ recovers a $\mathrm{GL}(U_1) \times \mathrm{GL}(U_2) \times \mathrm{GL}(U_3)$-orbit of $U_1 \otimes U_2 \otimes U_3$, where $U_1 = H^0(C, L_1)$, $U_2 = H^0(C, L_2)$, and U_3 is the dual of the three-dimensional kernel of the multiplication map $\mu_{12} : U_1 \otimes U_2 \to H^0(C, L_1 \otimes L_2)$. It remains to show that there exists a natural identification of U_2 and U_3 such that a representative $\mathcal{A}$ of this orbit is doubly symmetric.

The proof of Theorem 5.1 implies that $\mathcal{A}$ in turn produces a genus one curve and line bundles isomorphic to those with which we started. In other words, we find that there is an isomorphism $\phi : U_2 \to U_3$. Let C_1 be the image of C under the embedding given by L_1. For any point $x \in C_1$, we have $\det(\mathcal{A}(x, \cdot, \cdot)) = 0$ and the kernel of $\mathcal{A}(x, \cdot, \cdot)$ in $U_2^\vee$ and in $U_3^\vee$ is the same (after applying ϕ). Because C_1 spans $\mathbb{P}(U_1^\vee)$, the image of $U_1^\vee$ in $U_2 \otimes U_2$ given by $(\mathrm{id} \otimes \phi) \circ \mathcal{A}$ is a three-dimensional subspace W of $U_2 \otimes U_2$ such that the "left" and the "right" kernels of each element in $U_2^\vee$ are the same (usually empty).

We will make use of the following lemma, whose proof is postponed:

Lemma 5.9. *Let M_1 and M_2 be two $n \times n$ matrices over K with M_2 invertible. Assume $M_1 M_2^{-1}$ has distinct eigenvalues over $\overline{K}$ and that for all $y, z \in \overline{K}$, the transpose of the left kernel of $M_1 y - M_2 z$ is equal to its right kernel. Then M_1 and M_2 are symmetric matrices.*

To apply Lemma 5.9, note that for two nonsingular elements M_1 and M_2 of $U_2 \otimes U_2$, the matrix $M_1 M_2^{-1}$ will have distinct eigenvalues over $\overline{K}$ if the binary cubic form $\det(M_1 y - M_2 z)$ has distinct roots, in which case $M_1 y - M_2 z$ has rank at least 2 for any values of y and z. Recall that because the curve C is nonsingular, the space W does not contain any matrices of rank less than 2 and any two elements of W will satisfy the conditions of

the lemma. We thus may find a basis for W consisting only of symmetric elements, thus giving an element of $U_1 \otimes \mathrm{Sym}_2 U_2$ as desired. $\qquad\square$

Proof of Lemma 5.9. Because $\det(M_1 M_2^{-1} - \lambda I)$ has distinct roots, the binary n-ic form $\det(M_1 y - M_2 z) = \det(M_2)(\det M_1 M_2^{-1} y - \lambda z)$ has distinct roots $[y_i : z_i]$ in $\mathbb{P}^1(\overline{K})$ for $i = 1, \ldots, n$. For each i, let v_i be a nonzero vector in the right kernel of $M_1 y_i - M_2 z_i$, implying that v_i^t is a nonzero vector in the left kernel. The vectors v_i are linearly independent because they are eignevectors corresponding to distinct eigenvalues.

Now consider the bilinear forms $M_1(\cdot, \cdot)$ and $M_2(\cdot, \cdot)$ defined by $M_k(a, b) = a^t M_k b$ for $k = 1$ and 2. Now $v_i^t(M_1 y_i - M_2 z_i)v_j = v_i^t(M_1 y_j - M_2 z_j)v_j = 0$ for any $i \neq j$. Since (y_i, z_i) and (y_j, z_j) are linearly independent, we must have $v_i^t M_k v_j = 0$ for any $i \neq j$ and for $k = 1$ and 2. Therefore, M_1 and M_2 give diagonal bilinear forms with respect to the basis $v_1, \ldots, v_n$, and thus are symmetric matrices with respect to any basis. $\qquad\square$

The representation $V_1 \otimes \mathrm{Sym}_2 V_2$ has $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariant ring generated by the two previously defined polynomials c_6 and c_{12} of degrees 6 and 12, respectively. These have the same interpretation as in §5.1.3. That is, the Jacobian of C may be written in normal form as

$$E : y^2 = x^3 + c_6 x^2 + c_{12} x$$

with nonzero 2-torsion point P having coordinates $(x, y) = (0, 0)$. In other words, the symmetric tensors are simply the elements of $V_1 \otimes V_2 \otimes V_2$ where the degree 9 invariant vanishes. Nondegeneracy is again given by the same degree 36 discriminant, which now factors:

$$\Delta = 16 c_{12}^2 (-4 c_{12} + c_6^2).$$

The reduced discriminant has degree 24, and nondegeneracy is determined by the nonvanishing of c_{12} and of $-4c_{12} + c_6^2$.

5.2.2. Triply symmetric Rubik's cubes, or ternary cubic forms again. We now consider triply symmetric Rubik's cubes, i.e., orbits of $\mathrm{GL}(V) \times \mathbb{G}_m$ on $\mathrm{Sym}_3 V$ for a three-dimensional vector space V over K. Although this space, away from characteristic 3, is isomorphic to the space of ternary cubic forms $\mathrm{Sym}^3 V$ discussed in §4.2,[3] we treat this space as a subspace of $V \otimes V \otimes V$, instead of a quotient, to obtain a different moduli interpretation.

---

[3]More precisely, these representations are dual to one another if V is self-dual.

Because $\mathrm{Sym}_3 V \hookrightarrow V \otimes \mathrm{Sym}_2 V$, for each tensor $\mathcal{A} \in \mathrm{Sym}_3 V$ we may construct the associated genus one curve C and line bundles on C. We then find that the orbit spaces of these two representations in fact correspond to the same moduli problem! The following is a basis-free version of Theorem 3.2:

Theorem 5.10. *Let V be a three-dimensional vector space over K. Then nondegenerate $\mathrm{GL}(V) \times \mathbb{G}_m$-orbits of $\mathrm{Sym}_3 V$ are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve over K, L is a degree 3 line bundle on C, and P is a nonzero 2-torsion point of $\mathrm{Jac}(C)(K)$.*

Proof. We simply strengthen the proof of Theorem 5.8 with the observation that all the vector spaces in question may be naturally identified. As in the proof of Theorem 5.8, given a triple (C, L, P), we let $U_1 = H^0(C, L)$ and $U_2 = U_3 = H^0(C, L \otimes P)$ and obtain an element $\mathcal{A}$ of $U_1 \otimes \mathrm{Sym}^2 U_2$. We may also use the same proof to show that there is an identification between, e.g., U_1 and U_3 such that $\mathcal{A}$ is symmetric between those two directions; thus, by taking corresponding identified bases for U_1, U_2, and U_3, we obtain an element of $\mathrm{Sym}^3 U_1$ in $U_1^{\otimes 3} \cong U_1 \otimes U_2 \otimes U_3$. $\qquad\square$

This curve C is not the same as the curve Z associated to the ternary cubic via §4.2. The curve C has a degree 36 discriminant, while Z has a discriminant of degree 12. In fact, it is easy to check that the curve C is the zero locus of the Hessian of the ternary cubic form defining Z! (Recall that the Hessian of a ternary cubic form is given by the determinant of the matrix of second partial derivatives, which yields another ternary cubic form.) Therefore, we have another proof of the following:

Proposition 5.11. *Given a ternary cubic form f over K, let $H(f)$ denote the Hessian ternary cubic form. If the discriminant of $H(f)$ is nonzero, then the Jacobian of the genus one curve cut out by $H(f)$ is an elliptic curve with a nonzero rational 2-torsion point.*

This fact is classically shown by constructing a fixed-point free involution on the curve cut out by $H(f)$; see [Dol12, Chapter 3].

To describe the invariant theory and the relationship with this curve Z, let $\mathcal{A}$ be a nondegenerate element of $\mathrm{Sym}_3 V$. Recall that the generators d_4 and d_6 of the $\mathrm{SL}(V)$-invariant ring of this representation are of degrees 4 and 6; we maintain the normalization from §4.2. Then $\mathcal{A}$, viewed as a ternary cubic form as in §4.2, gives rise to a genus one curve Z in $\mathbb{P}(V^\vee)$ whose Jacobian is given by (38).

On the other hand, let C denote the genus one curve obtained from viewing $\mathcal{A}$ as a (symmetric) Rubik's cube. Then an easy computation shows that the Jacobian of C may be given in Weierstrass form as

$$(43) \qquad E : y^2 = x^3 - 72d_6x^2 + 1296d_4^3x,$$

where the point $(0, 0)$ is the nonzero 2-torsion point on E. The discriminant of E factors as a rational multiple of

$$d_4^6(d_4^3 - d_6^2),$$

so the reduced discriminant has degree $4 + 12 = 16$. Note that the factor $d_4^3 - d_6^2$ is a scalar multiple of the discriminant of the elliptic curve $\mathrm{Jac}(Z)$. Thus, requiring nondegeneracy of $\mathcal{A}$ as a Rubik's cube implies that both the genus one curve Z and the curve C are smooth. Also, observe that even without the parametrization of Theorem 5.10, we know that all elliptic curves over K with a rational 2-torsion point may be written in the form (43), since such an elliptic curve may clearly be written as

$$y^2 = x^3 + ax^2 + bx$$

for any $a, b \in K$ with nonzero discriminant (i.e., $b(a^2 - 4b) \neq 0$). Taking $d_4 = 1296/b$ and $d_6 = -23328a/b^2$ gives (43).

5.3. Cubic Jordan algebras

A *Jordan algebra* over K is a K-algebra with a commutative bilinear product $\bullet$ satisfying the Jordan identity $(x^2 \bullet y) \bullet x = x^2 \bullet (y \bullet x)$. In this section, we introduce the "cubic Jordan algebras" that will be relevant for the more general degree 3 moduli problem. Some of their connections with geometry and representation theory will prove vital for describing and proving the related orbit parametrizations in §5.4.

5.3.1. Jordan cubic forms and Springer's construction. Following [McC04] and [KMRT98, Chapter IX], we first briefly describe Springer's construction of Jordan algebras from nondegenerate cubic forms; the algebras thus constructed are known as *cubic Jordan algebras*. Let U be a finite-dimensional vector space over our field K (recall that char $K \neq 2, 3$), and let N be a cubic form on U such that $N(e) = 1$ for some basepoint e. Then there

are naturally associated spur and trace forms, and their (bi)linearizations[4], denoted by

$$(44) \quad S(x) := N(x, x, e) \quad\quad S(x, y) := N(x, y, e) = S(x + y) - S(x) - S(y)$$
$$\quad\quad\quad Tr(x) := N(e, e, x) \quad\quad Tr(x, y) := Tr(x) Tr(y) - S(x, y).$$

In general, an *adjoint map* $\sharp$ for the cubic form (N, e) is a quadratic map $\sharp : U \to U$ satisfying

$$(45) \quad\quad\quad\quad\quad\quad Tr(x^\sharp, y) = N(x, x, y)$$

$$(46) \quad\quad\quad\quad\quad\quad (x^\sharp)^\sharp = N(x)x$$

$$(47) \quad\quad\quad\quad\quad\quad e \times x = Tr(x)e - x$$

where $\times$ denotes the bilinearization

$$(48) \quad\quad\quad\quad x \times y := (x + y)^\sharp - x^\sharp - y^\sharp.$$

An *admissible* cubic form is a cubic form N with basepoint e and an associated adjoint map $\sharp$. Such a form gives rise to a natural Jordan algebra structure on U with unit element e and product given by

$$(49) \quad\quad\quad x \bullet y := \frac{1}{2} \left(x \times y + Tr(x)y + Tr(y)x - S(x, y)e \right).$$

We also have the identity

$$x^3 - Tr(x)x^2 + S(x)x - N(x)e = 0,$$

i.e., the "characteristic polynomial of x", evaluated at x, vanishes for all $x \in U$ (Cayley–Hamilton Theorem).

For cubic forms, there is often a natural choice of an adjoint map. In particular, a cubic form is called *nondegenerate* if its associated bilinear trace form $Tr(\cdot, \cdot)$ is nondegenerate, in which case U and its dual $U^\vee$ may

---

[4]The linearization of a homogeneous degree n polynomial is a symmetric multilinear polynomial in n (not necessarily commuting) variables such that the original polynomial may be recovered by specializing all n variables to the same variable. For example, the linearization of x^2 is $\frac{1}{2}(x_1x_2 + x_2x_1)$ and of x^3 is $\frac{1}{6}(x_1x_2x_3 + x_1x_3x_2 + x_2x_1x_3 + x_2x_3x_1 + x_3x_1x_2 + x_3x_2x_1)$. See [McC04, §1.4] for more details on linearization.

be canonically identified. In other words, for fixed x, the linear functional $y \mapsto \mathrm{N}(x, x, y)$ corresponds to an element $x^\sharp \in U$, giving a quadratic map

$$(50) \qquad \sharp : \quad U \longrightarrow U^\vee \overset{\cong}{\longrightarrow} U$$
$$x \longmapsto \mathrm{N}(x, x, \cdot) \longmapsto x^\sharp.$$

This map $\sharp$ by definition satisfies (45); if $\sharp$ also satisfies (46), then it is easy to check that (47) holds as well and thus $\sharp$ is an adjoint map [McC04, §4.3]. Therefore, a nondegenerate cubic form N on U with basepoint e has a natural Jordan algebra structure on U with product defined as in (49).

By an abuse of notation, sometimes the map $\sharp$ will refer to just the first map in (50), that is, the map from $x \in U$ to the linear functional $y \mapsto \mathrm{N}(x, x, y)$ in $U^\vee$, since U and $U^\vee$ are naturally identified.

5.3.2. Composition algebras and Hermitian matrices. We now describe a class of cubic Jordan algebras that will play a crucial role in the representations we study. We begin with some remarks about composition algebras, which are used to construct these Jordan algebras.

A *composition algebra* A over a field K is a K-algebra A with identity element e and a nondegenerate quadratic norm form q on A that satisfies

$$q(e) = 1 \quad \text{and} \quad q(ab) = q(a)q(b)$$

for any elements $a, b \in A$. By a theorem of Hurwitz, such an algebra A is either K itself, a quadratic étale K-algebras, a quaternion algebra over K, or a Cayley algebra over K.

Example 5.12. If $K = \overline{K}$ is algebraically closed, then the only composition algebras are the four *split* composition algebras of dimensions 1, 2, 4, and 8, namely the split unarions $\mathscr{U}(K) := K$, the split binarions $\mathscr{B}(K) \cong K \times K$, the split quaternions $\mathscr{Q}(K) \cong \mathrm{Mat}_{2 \times 2}(K)$, and the split octonions $\mathscr{O}(K)$ with the natural norm forms.

Example 5.13. Over $K = \mathbb{R}$, in addition to the split composition algebras, there exist the usual division algebras of dimensions 2, 4, and 8: the complex numbers $\mathbb{C}$, the Hamiltonian quaternions $\mathbb{H}$, and the Cayley octonions $\mathbb{O}$, respectively.

If the quadratic form q on the composition algebra A is nondegenerate, then A is alternative separable of degree 2 and has an anti-involution $\star$

sending $a \in A$ to $a^\star = \overline{a}$ [KMRT98, Prop. 33.9]. Any element $a \in A$ hence satisfies the equation

$$a^2 - \mathrm{tr}_A(a)a + \mathrm{n}_A(a)e = 0,$$

where the trace and norm are defined in terms of the quadratic norm form q as

$$\mathrm{tr}_A(a) := q(a + e) - q(a) - q(e) \quad \text{and} \quad \mathrm{n}_A(a) := q(a).$$

For a composition algebra A over K as above, the Hermitian matrix algebra $\mathscr{H}_n(A)$ consists of the $n \times n$ matrices $M = (m_{ij}) \in \mathrm{Mat}_{n \times n}(A)$ with $M = \overline{M}^t$, or equivalently, $m_{ji} = m_{ij}^\star$ for $1 \leq i, j \leq n$. The multiplicative structure of the algebra $\mathscr{H}_n(A)$ is commutative but not associative, given by

(51)
$$M \bullet M' := \frac{1}{2}(M \cdot M' + M' \cdot M)$$

where $\cdot$ denotes usual matrix multiplication. Under this algebra structure, the Hermitian matrices $\mathscr{H}_n(A)$ form a Jordan algebra.

We now consider the case of cubic Jordan algebras given as a Hermitian matrix algebra for a composition algebra A. There is one Jordan algebra structure on $\mathscr{H}_3(A)$ inherited from the composition law (51). Also, on $\mathscr{H}_3(A)$, we may define a natural admissible cubic form $(\mathrm{N}, e, \sharp)$:

(52)
$$\mathrm{N}\begin{pmatrix} c_1 & a_3 & a_2^\star \\ a_3^\star & c_2 & a_1 \\ a_2 & a_1^\star & c_3 \end{pmatrix} := c_1 c_2 c_3 - c_1\, \mathrm{n}_A(a_1) - c_2\, \mathrm{n}_A(a_2) - c_3\, \mathrm{n}_A(a_3) + \mathrm{tr}_A(a_1 a_2 a_3)$$

$$e := \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

(53)
$$\sharp : \begin{pmatrix} c_1 & a_3 & a_2^\star \\ a_3^\star & c_2 & a_1 \\ a_2 & a_1^\star & c_3 \end{pmatrix} \mapsto \begin{pmatrix} c_2 c_3 - \mathrm{n}_A(a_1) & a_2^\star a_1^\star - c_3 a_3 & a_3 a_1 - c_2 a_2^\star \\ a_1 a_2 - c_3 a_3^\star & c_1 c_3 - \mathrm{n}_A(a_2) & a_3^\star a_2^\star - c_1 a_1 \\ a_1^\star a_3^\star - c_2 a_2 & a_2 a_3 - c_1 a_1^\star & c_1 c_2 - \mathrm{n}_A(a_3) \end{pmatrix}$$

for $c_1, c_2, c_3 \in K$ and $a_1, a_2, a_3 \in A$. For example, if A were commutative, then the norm form N is the usual determinant of the matrix and the map $\sharp$ coincides with the usual adjoint map for 3×3 matrices. Springer's construction then gives a Jordan algebra structure on $\mathscr{H}_3(A)$ using this admissible cubic form.

Proposition 5.14 ([McC04, §4.4])**.** *The two Jordan algebra structures on $\mathscr{H}_3(A)$, as defined above, are the same.*

5.3.3. Hermitian tensor spaces. In this section, we describe in a basis-free manner the algebra $\mathscr{H}_n(A)$ for *associative* composition algebras A over K, i.e., composition algebras of dimensions 1, 2, or 4 over K. For such A, we introduce the notion of a *Hermitian tensor space* of an A-bimodule $\mathfrak{M}$. Just as for symmetric and alternating tensor products, the idea is to construct a subspace (or a quotient space) of a tensor space that corresponds to Hermitian matrices.

If $\mathfrak{M}$ is an A-bimodule, then we define $\mathfrak{M}^\star$ to be its twist by the involution $\star$ on A. In other words, there is K-vector space (but not A-module) isomorphism

$$\mathfrak{M} \longrightarrow \mathfrak{M}^\star$$
$$m \longmapsto m^\star$$

but the left and right A-actions on $\mathfrak{M}^\star$ are given by

$$a(m^\star) = ((m)a^\star)^\star \qquad \text{and} \qquad (m^\star)a = (a^\star(m))^\star$$

for all $a \in A$ and $m \in \mathfrak{M}$. For any two A-bimodules, the tensor product is again an A-bimodule; in our case, we have that $\mathfrak{M} \otimes_A \mathfrak{M}^\star$ is an A-bimodule with left and right A-actions described by

$$a(m_1 \otimes m_2^\star) = a(m_1) \otimes m_2^\star \quad \text{and}$$
$$(m_1 \otimes m_2^\star)a = m_1 \otimes (m_2^\star)a = m_1 \otimes (a^\star(m_2))^\star$$

for all $a \in A$ and $m_1, m_2 \in \mathfrak{M}$. Note that elements of A can "pass through" the tensor product, i.e., the relation $(m_1)a \otimes m_2^\star = m_1 \otimes a(m_2^\star)$ holds for all $a \in A$ and $m_1, m_2 \in \mathfrak{M}$. There is a natural involution τ on elements of $\mathfrak{M} \otimes_A \mathfrak{M}^\star$ sending

$$m_1 \otimes m_2^\star \mapsto m_2 \otimes m_1^\star.$$

Definition 5.15. The *Hermitian tensor space* $\mathrm{Herm}^2(\mathfrak{M})$ of $\mathfrak{M}$ is the sub-bimodule of $\mathfrak{M} \otimes_A \mathfrak{M}^\star$ consisting of elements M satisfying $\tau(M) = M$.

Remark 5.16. One could also define a similar Hermitian tensor space as a quotient

$$\mathfrak{M} \otimes_A \mathfrak{M}^\star / \mathfrak{I}$$

where $\mathfrak{I}$ is the submodule generated by all tensors of the form $m_1 \otimes m_2^\star - m_2 \otimes m_1^\star$ for $m, m' \in \mathfrak{M}$. Over a field of characteristic not 2, these notions are the same (just like for symmetric tensors). For our purposes, the subspace defined in Definition 5.15 is more useful.

For any $\mathfrak{M}$, there is a Segre-like map

$$(54) \qquad \mathrm{Seg} : \mathfrak{M} \longrightarrow \mathrm{Herm}^2(\mathfrak{M}) \subset \mathfrak{M} \otimes_A \mathfrak{M}^\star$$
$$m \longmapsto m \otimes m^\star$$

whose image consists precisely of the "rank one" tensors in $\mathfrak{M} \otimes_A \mathfrak{M}^\star$. This is, of course, not a linear map. In fact, the right A-action on $\mathfrak{M}$ scales the image of Seg by elements of the field K; in particular,

$$(55) \quad \mathrm{Seg}((m)a) = (m)a \otimes ((m)a)^\star = (m)a \otimes a^\star(m^\star) = \mathrm{n}_A(a)(m \otimes m^\star).$$

If $\mathfrak{M}$ is a free rank r A-bimodule with a choice of basis, then the Hermitian tensor space $\mathrm{Herm}^2(\mathfrak{M})$ is visibly just the space $\mathscr{H}_r(A)$ of $r \times r$ Hermitian matrices over A, as the involution τ corresponds to taking the conjugate transpose of a matrix.

In the sequel, let $\mathfrak{M}$ denote a free self-dual rank 3 A-bimodule, and let $J(A) := \mathrm{Herm}^2(\mathfrak{M})$. Then $J(A)$ also has the structure of a cubic Jordan algebra as in §5.3.2. When we refer to $J(A)$ for associative A, the module $\mathfrak{M}$ will be assumed. For an octonion algebra A over K, the notation $J(A)$ will refer to the exceptional Jordan algebra $\mathscr{H}_3(A)$.

Remark 5.17. Because $\mathfrak{M}$ is assumed to be self-dual, we may view elements of the tensor space $\mathfrak{M} \otimes_A \mathfrak{M}^\star$ as maps from $\mathfrak{M}^\vee \cong \mathfrak{M}$ to $\mathfrak{M}^\star$. So there are also basis-free definitions of the norm, trace, and spur forms, as well as the adjoint map $\sharp$ in (50), for $J(A)$.

5.3.4. Rank. Elements of $J(A)$ inherit the notion of *rank* from the ambient tensor space $\mathfrak{M} \otimes_K \mathfrak{M}^\star$. In this section, we discuss the stratification of $J(A)$ by rank, which is closely related to Severi varieties and their tangent and secant varieties.

By forgetting the Jordan algebra and the A-module structure on $J(A)$, it makes sense to think of $J(A)$ as a K-vector space of dimension $3\dim(A)+3$. The projective space $\mathbb{P}(J(A))$ will denote the space of K-lines in $J(A)$ as a K-vector space and thus has dimension $3\dim A + 2$ over K.

Let $X_A \in \mathbb{P}(J(A))$ correspond to the rank one elements of $J(A)$, so X_A is cut out by quadrics in $\mathbb{P}(J(A))$. Let $Y_A \in \mathbb{P}(J(A))$ consist of the elements of $J(A)$ having rank at most two. Then Y_A is visibly the secant variety of X_A in $\mathbb{P}(J(A))$. On the other hand, the variety Y_A is defined by the cubic norm form N on $J(A)$, so it is a cubic hypersurface in $\mathbb{P}(J(A))$.

If the composition algebra A has dimension d over K, then X_A, Y_A, and $\mathbb{P}(J(A))$ have dimensions $2d$, $3d + 1$, and $3d + 2$, respectively. Since $d = 1$,

2, 4, or 8, in all these cases, the secant variety Y_A of X_A is defective, and by a theorem of Zak [Zak93], the secant variety is also the tangent variety.

Example 5.18. Over an algebraically closed field of characteristic 0, the varieties $X_A \subset \mathbb{P}(J(A))$ for the four composition algebras A (see Example 5.12) are exactly the four Severi varieties [Zak85]:

  (i) the Veronese surface $\mathbb{P}^2 \subset \mathbb{P}^5$,
 (ii) the Segre fourfold $\mathbb{P}^2 \times \mathbb{P}^2 \subset \mathbb{P}^8$,
(iii) the Grassmannian $\mathrm{Gr}(2,6) \subset \mathbb{P}^{14}$, and
 (iv) the 16-dimensional variety $E^{16} \subset \mathbb{P}^{26}$ discovered by Lazarsfeld [LVdV84].

Over a general field K, the varieties that arise are twisted forms of these.

From the geometric perspective, the adjoint map $\sharp : J(A) \to J(A)^\vee$ is essentially (up to scaling) the birational map

$$(56) \qquad\qquad \beta_A : \mathbb{P}(J(A)) \dashrightarrow \mathbb{P}(J(A)^\vee)$$

given by the linear system of quadrics passing through X_A, or in other words, the partial derivatives of the norm form N on $J(A)$ (see [ESB89] or [Zak85]). By definition, the map β_A blows down Y_A to X_A, and the inverse blows up X_A to Y_A, so X_A is naturally isomorphic to the dual variety of Y_A and vice versa.

These varieties X_A have a simple moduli interpretation, based on their definition as rank one elements of $J(A)$ up to K-scaling.

Lemma 5.19. *For any composition algebra A of dimension $1, 2$, or 4 over K, the variety X_A parametrizes elements of $\mathfrak{M}$ up to right A-scaling.*

Proof. The map Seg defined in (54) descends to a well-defined map

$$(\mathfrak{M} \setminus \{0\})/A \longrightarrow \mathbb{P}(J(A))$$

by the computation in (55). (Here $(\mathfrak{M} \setminus \{0\})/A$ denotes nonzero elements of the module $\mathfrak{M}$ up to right A-scaling.) The image of this map is by definition X_A, and it is easy to check that this map is injective. $\qquad\square$

In fact, the variety X_A for all composition algebras A (including those of dimension 8) over an algebraically closed field of characteristic 0 is often considered an embedding of the projective plane $\mathbb{P}^2(A)$ over A into $\mathbb{P}(J(A))$ [Zak85]. Here, we work over a more general base field K, but the above argument only holds for associative composition algebras. For octonion algebras A over K, an explicit computation shows that the variety X_A here shares

the same points as the usual definition of an octonionic projective plane [CS03, Chapter 12], which can also be described as right (or left) A-lines in A^3.

5.3.5. Linear transformations of Jordan algebras. Let $\mathrm{SL}(J)$ be the group of norm-preserving K-linear automorphisms of a Jordan algebra J. In this way, the Jordan algebra J may be thought of as a representation of the group $\mathrm{SL}(J)$. In the case $J = \mathcal{H}_3(A)$, we also denote $\mathrm{SL}(J)$ by $\mathrm{SL}_3(A)$.

Over an algebraically closed field $K = \overline{K}$, the cubic Jordan algebras $J(A)$ built from the four split composition algebras A correspond to the following groups and representations (see, e.g., [Jac68, §VI.7-VI.9] or [Kru07, Remark 10] for more details):

A	semisimple simply connected form of $\mathrm{SL}(J(A))$	$J(A)$
$\mathscr{U}(K) = K$	$\mathrm{SL}_3(K)$	$\mathrm{Sym}^2(3)$
$\mathscr{B}(K) \cong K \times K$	$\mathrm{SL}_3(K) \times \mathrm{SL}_3(K)$	$3 \otimes 3$
$\mathscr{Q}(K) \cong \mathrm{Mat}_{2 \times 2}(K)$	$\mathrm{SL}_6(K)$	$\wedge^2(6)$
$\mathscr{O}(K)$	$E_6(K)$	27

Over a general field, we may consider various forms of these groups and the corresponding representations.

For the cubic Jordan algebras $J(A)$ described in §5.3.4, the cone on X_A — that is, the set of rank one tensors — in $J(A)$ is exactly the orbit of the highest weight vector of the representation $J(A)$ of $\mathrm{SL}(J(A))$ (see [Zak93, Chapter 3] for an explanation over an algebraically closed field). Over the algebraic closure, it is the unique closed orbit of the action of $\mathrm{SL}(J(A))$ on $\mathbb{P}(J(A))$. Thus, the variety $X_A \subset \mathbb{P}(J(A))$ is isomorphic to the flag variety $\mathrm{SL}(J(A))/P$, where P is the parabolic subgroup of $J(A)$ that stabilizes the highest weight vector.

More generally, over the algebraic closure, the orbits of the action of $\mathrm{SL}(J(A))$ on $J(A)$ give a stratification of $J(A)$ by rank. We obtain another description of the rank two tensors of the representation $J(A)$, which together form another orbit of $\mathrm{SL}(J(A))$ on $\mathbb{P}(J(A))$.

Note that this description of X_A automatically gives a moduli interpretation of X_A, since it is a generalized flag variety; the moduli interpretation given in Lemma 5.19 is slightly stronger, since it also includes the action of the composition algebra A on the vector bundle.

5.4. Doubly Hermitian Rubik's cubes

Our goal in this section is to study, in a uniform way, the orbits of the representations $V \otimes J(A)$ of the group $G_{J(A)} := \mathrm{GL}(V) \times \mathrm{SL}(J(A))$, where

V is a three-dimensional vector space over the field K and $J(A)$ is the cubic Jordan algebra obtained from a composition algebra A as defined in §5.3. We will restrict ourselves to nondegenerate elements of the tensor space, as these will correspond exactly to nonsingular curves.

Definition 5.20. An element $\phi \in V \otimes J(A)$ is called *nondegenerate* if the induced composition map

$$\sharp \circ \phi : V^\vee \to J(A) \to J(A)^\vee$$

is injective.

We will show that nondegenerate elements of $V \otimes J(A)$ correspond to genus one curves with extra data, including what we call an A-line on the curve. Intuitively, an A-line on a variety Z is like a rank one (left or right) A-module, if the notion of rank were well defined for noncommutative rings.

Definition 5.21. Let A be a dimension d composition algebra over K and let Z be a variety defined over K. Then an A-*line* over Z is a rank d vector bundle E over Z with a global faithful right A-action.

Fix a trivial rank ds bundle B over Z. We say that an A-line E on Z has *size s* if E is isomorphic to a subbundle of B, such that B has a global faithful right A-action that restricts on E to the given A-action on E. A size 3 A-line E on Z is *very ample* if there is an immersion $\kappa : Z \to X_A$ such that the pullback of the universal A-line on X_A is isomorphic to E. Finally, for a very ample size 3 A-line E on Z, we denote by $\operatorname{lin} E$ the line bundle on Z given by pulling back $\mathcal{O}_{\mathbb{P}(J(A))}(1)$ to Z via the composition $Z \xrightarrow{\kappa} X_A \hookrightarrow \mathbb{P}(J(A))$. We will show that $\operatorname{lin} E$ is closely related to the determinant bundle $\det E$ (of E as a vector bundle), in each case.

From an element of $V \otimes J(A)$, we will construct a genus one curve with a degree 3 line bundle and an A-line. This construction will be automatically invariant under the action of $G_{J(A)}$. In fact, this is exactly the data that determines a $G_{J(A)}$-orbit!

Theorem 5.22. *The nondegenerate $G_{J(A)}$-orbits of $V \otimes J(A)$ are in bijection with isomorphism classes of nondegenerate triples (C, L, E), where C is a smooth genus one curve over K, L is a degree 3 line bundle on C, and E is a very ample size 3 A-line over C satisfying $\operatorname{lin} E \cong L^{\otimes 2}$.*

The nondegeneracy condition for a triple (C, L, E) will be discussed more in the proof; it is an open condition, so the theorem may be rephrased as a bijection between the orbits of $V \otimes J(A)$ and the K-points of an open

substack of the moduli space of such triples (with the isomorphism between $\lim E$ and $L^{\otimes 2}$). For some choices of A, we will work out a relatively simple interpretation of this condition.

5.4.1. Geometric construction. We now show that a nondegenerate element ϕ of $V \otimes J(A)$ naturally gives rise to the geometric data of a genus one curve C, a degree 3 line bundle on C, and an A-bundle E. Let d be the dimension of the composition algebra A over K.

Given $\phi \in V \otimes J(A)$, we may instead think of ϕ as a linear map in $\mathrm{Hom}(V^\vee, J(A))$. Nondegeneracy of ϕ immediately implies that this map is injective, so we obtain a linear map

$$\mathbb{P}(\phi) : \mathbb{P}(V^\vee) \longrightarrow \mathbb{P}(J(A)).$$

Let W be the image of $\mathbb{P}(\phi)$ in $\mathbb{P}(J(A))$. Then the secant variety Y_A of X_A cuts out a cubic plane curve C on W. In other words, the curve $\iota : C \hookrightarrow \mathbb{P}(J(A))$ is defined by the vanishing of the cubic norm form N on the plane W. Let L be the pullback of $\mathcal{O}(1)$ from the projective plane W to C, so L is a degree 3 line bundle on C.

We claim that for ϕ nondegenerate, this curve C is smooth and irreducible, and thus of genus one. Nondegeneracy of ϕ implies that W does not intersect the variety X_A, which is the base locus for the rational map β_A in (56), or equivalently, that the partials of the norm form N do not simultaneously vanish. In this case, the curve C is nonsingular.

Lemma 5.23. *The image $C^\sharp$ of the curve $C \subset Y_A$ under the adjoint map β_A is isomorphic to C, and hence is a smooth irreducible genus one curve in $X_A \subset \mathbb{P}(J(A)^\vee)$.*

Proof. Recall that $J(A)$ and its dual may be naturally identified, and from §5.3.4, the adjoint map β_A is a birational map from $\mathbb{P}(J(A))$ to $\mathbb{P}(J(A)^\vee)$, which blows down $Y_A \setminus X_A$ to X_A. The image of the plane W under β_A is birational on $W \setminus C$. In other words, the generic fiber of β_A restricted to W is connected, so by Zariski's connectedness theorem, all the special fibers are connected; since there are no contractible curves in $W \cong \mathbb{P}^2$, each fiber is a single point. Thus, the image $C^\sharp$ of C is also a smooth irreducible genus one curve, and it is contained in X_A. $\qquad\square$

By the moduli interpretation of the variety X_A, the closed immersion $C^\sharp \hookrightarrow X_A$ is equivalent to the data of a very ample size 3 A-line on $C^\sharp$, which pulls back to a very ample size 3 A-line E on C. In other words, we have produced the triple (C, L, E) as desired.

It is clear that the isomorphism class of the triple (C, L, E) is preserved under the action of $G_{J(A)}$, where two such triples (C, L, E) and (C', L', E') are isomorphic if there is an isomorphism $\sigma : C \to C'$ such that $\sigma^* L' = L$ and $\sigma^* E' = E$ and the A-actions on E and E' are related by σ. The groups $\mathrm{GL}(V)$ and $\mathrm{SL}(J(A))$ act by linear transformations on V and on $J(A)$, respectively, and the action of $\mathrm{SL}(J(A))$ fixes the varieties X_A and Y_A. Thus, both actions do not affect the geometric data, up to isomorphism.

Now we show that the triple (C, L, E) satisfies the last condition of the theorem.

Lemma 5.24. *There is an isomorphism*

$$\lin E \cong L^{\otimes 2}$$

of line bundles on the curve C.

Proof. This relation follows from the fact that the map β_A is given by quadratic polynomials. The line bundle $\lin E$ on the curve C is the pullback of $\mathcal{O}_{\mathbb{P}(J(A))}(1)$ via

$$C \xrightarrow{\beta_A} C^\sharp \hookrightarrow X_A \hookrightarrow \mathbb{P}(J(A)^\vee) \cong \mathbb{P}(J(A)),$$

which is isomorphic to $\iota^* \mathcal{O}_{\mathbb{P}(J(A))}(2)$. On the other hand, the line bundle L is defined as the pullback of $\mathcal{O}_W(1)$ to C, and since W lies linearly in $\mathbb{P}(J(A))$, in fact L is isomorphic to $\iota^* \mathcal{O}_{\mathbb{P}(J(A))}(1)$. $\qquad\square$

This line bundle $\lin E$ on C is closely related to the determinant bundle of E.

Lemma 5.25. *For a very ample size 3 A-line E on a projective variety Z, where A is a composition algebra over K of dimension d, if $\dim A = 1$, then*

$$(\det E)^{\otimes 2} \cong \lin E$$

and if $\dim A = 2$, 4, or 8, then

$$\det E \cong (\lin E)^{\otimes (d/2)}.$$

Proof. It suffices to prove this lemma for the variety X_A itself. Recall that X_A is a homogeneous variety in $\mathbb{P}(J(A))$ given as the projectivization of the orbit of the highest weight vector of the representation $J(A)$ of $\mathrm{SL}(J(A))$. It is well known that the pullback of $\mathcal{O}_{\mathbb{P}(J(A))}(1)$ to X_A is the product of the determinants of the vector bundles in the universal flag on X_A [Ful97,

Chapter 9]. Comparing the universal A-line E on X_A to the vector bundles in the universal flag under the typical moduli interpretation gives the lemma. (For example, when A is the split quaternions over K, our A-line E is a rank 4-vector bundle on $X_A = \mathrm{Gr}(2,6)$ and is the second tensor power of the typical universal rank 2 bundle defined on the Grassmannian.) $\square$

5.4.2. Bijection. The geometric construction described above gives one direction of the bijection. We now prove Theorem 5.22 (and its weaker version, Theorem 3.5).

Proof of Theorem 5.22. Suppose (C, L, E) is a triple satisfying the conditions of the theorem. We wish to recover a plane W in $\mathbb{P}(J(A))$ such that C is isomorphic to the curve cut out by W and the cubic hypersurface Y_A.

The degree 3 line bundle L on C gives a closed immersion $\eta : C \hookrightarrow \mathbb{P}(H^0(C, L)^\vee) \cong \mathbb{P}^2$. The A-line E on C implies that there is a closed immersion

$$(57) \qquad\qquad \kappa : C \to X_A \hookrightarrow \mathbb{P}(J(A)) \cong \mathbb{P}(J(A)^\vee)$$

given by the sections of $\mathrm{lin}\, E$. More precisely, since $\mathrm{lin}\, E \cong \kappa^* \mathcal{O}_{\mathbb{P}(J(A))}(1)$ and $\deg(\mathrm{lin}\, E) = 6$ by assumption, the image of κ lies in a $\mathbb{P}^5$ lying linearly in $\mathbb{P}(J(A))$, namely the image of the map $\lambda : \mathbb{P}(H^0(C, \mathrm{lin}\, E)^\vee) \hookrightarrow \mathbb{P}(J(A))$.

Recall that we have an isomorphism $L^{\otimes 2} \cong \mathrm{lin}\, E$. The multiplication map

$$H^0(C, L) \otimes H^0(C, L) \longrightarrow H^0(C, L^{\otimes 2}) \cong H^0(C, \mathrm{lin}\, E)$$

is surjective and factors through $\mathrm{Sym}^2 H^0(C, L)$, so a dimension count shows that the spaces $H^0(C, \mathrm{lin}\, E)$ and $\mathrm{Sym}^2 H^0(C, L)$ are naturally isomorphic. Thus, we have a natural quadratic map

$$(58) \qquad \rho : \mathbb{P}(H^0(C, L)^\vee) \longrightarrow \mathbb{P}(\mathrm{Sym}^2 H^0(C, L)^\vee) \xrightarrow{\ \cong\ } \mathbb{P}(H^0(C, \mathrm{lin}\, E)^\vee).$$

Pulling back the line bundle $\mathcal{O}_{\mathbb{P}(J(A))}(1)$ to the curve C via the composition $\lambda \circ \rho \circ \eta$ and via κ give isomorphic line bundles on C, so under an appropriate change of basis, the images of C in $\mathbb{P}(J(A))$ via these two maps coincide. In other words, the following diagram commutes:

$$
\begin{array}{ccc}
C & \longrightarrow & X_A \\
\downarrow{\scriptstyle \eta} & & \downarrow \\
\mathbb{P}(H^0(C, L)^\vee) & \xrightarrow[\text{quadratic}]{\lambda \circ \rho} & \mathbb{P}(J(A))
\end{array} \quad .
$$

The image of $\mathbb{P}(H^0(C, L)^\vee)$ under ρ is a Veronese surface $\mathscr{V}$ in the space $\mathbb{P}(H^0(C, \lin E)^\vee) \subset \mathbb{P}(J(A))$. The nondegeneracy condition we require is that this Veronese $\mathscr{V}$ is not contained in Y_A. Under the inverse of the adjoint map β_A, we claim that $\mathscr{V}$ gives a $\mathbb{P}^2$ lying linearly in $\mathbb{P}(J(A))$. Recall that $\beta_A \circ \beta_A$ is the identity on $\mathbb{P}(J(A)) \setminus Y_A$. By assumption, outside of the image of C on $\mathscr{V}$, the map β_A is birational, so by the valuative criterion of properness, there is a well-defined map from all of the surface $\mathscr{V}$ to $\mathbb{P}(J(A))$, whose image is a linear subspace of $\mathbb{P}(J(A))$. This plane may be identified with $\mathbb{P}(H^0(C, L)^\vee)$ under some choice of basis.

Note that the nondegeneracy condition on the triple (C, L, E) is satisfied when constructed from an element of $V \otimes J(A)$. Finally, the constructions in each direction are inverse to one another, since $\beta_A \circ \beta_A$ is the identity on an open set of $\mathbb{P}(J(A))$.   □

5.5. Specializations

For particular choices of A, Theorem 5.22 recovers some of the spaces considered earlier, while some other choices of A give new parametrization theorems. In this section, we describe some of the cases where A is split.

For example, the case where $A = K \times K$ and $d = 2$ recovers the space of Rubik's cubes studied in §5.1. For $A = K \times K$, it is easy to check that the Jordan algebra $J(A)$ is isomorphic to the Jordan algebra $\mathrm{Mat}_{3 \times 3}(K)$ of 3×3 matrices over K, where the norm, spur, and trace forms coming from the characteristic polynomial in the standard way. The variety X_A is isomorphic to the Segre fourfold $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$, and its secant variety Y_A is the cubic hypersurface given by the vanishing of the determinant. Then the curve obtained as a intersection of a plane and Y_A in $\mathbb{P}(J(A))$ may be thought of as a determinantal variety, just as before.

The specialization of Theorem 5.22 to $A = K$ and $d = 1$ gives the space of doubly symmetric Rubik's cubes, which we studied in §5.2.1. Here, the variety X_A is the Veronese surface $\mathbb{P}^2 \hookrightarrow \mathbb{P}^5$. The A-line E is another degree 3 line bundle, given as the pullback of $\mathcal{O}(1)$ from the Veronese surface to the curve. The squares of the line bundles L and E are isomorphic, and thus their difference is a 2-torsion point on the Jacobian of the curve, as described in Theorem 5.8.

We next study Theorem 5.22 in the case where $d = 4$ and the composition algebra A is the algebra of split quaternions over K, i.e., the algebra $\mathrm{Mat}_{2 \times 2}(K)$ of 2×2 matrices over K, in order to recover Theorem 3.4. In this case, the algebra $J(A)$ is isomorphic to the algebra of 6×6 skew-symmetric matrices over K, where the cubic form is the degree 3 Pfaffian of such a

matrix. The moduli problem becomes one of determining so-called *Pfaffian representations*, which have been studied over an algebraically closed field in [BK11].

Theorem 5.26. *Let V and W be K-vector spaces of dimensions 3 and 6, respectively. Then nondegenerate $\mathrm{GL}(V) \times \mathrm{SL}(W)$-orbits of $V \otimes \wedge^2 W$ are in bijection with isomorphism classes of nondegenerate triples (C, L, F), where C is a genus one curve over K, L is a degree 3 line bundle on C, and F is a rank 2 vector bundle on C, with $\det F \cong L^{\otimes 2}$.*

The interpretation of X_A as a moduli space of rank 2 vector bundles is straightforward. Here $X_A \hookrightarrow \mathbb{P}(J(A))$ is the Plücker embedding of the Grassmannian $\mathrm{Gr}(2, W)$ in $\mathbb{P}(\wedge^2(W)) \cong \mathbb{P}^{14}$. The A-line E coming from Theorem 5.22 is a rank 4 — not rank 2! — vector bundle over C, but there is an equivalence of categories between modules E over rank 4 Azumaya algebras and rank 2 vector bundles F. This phenomenon is special to the case of the split quaternion algebra; for nonsplit quaternion algebras, the minimal rank vector bundle recovered from this data will have rank 4.

We may also set A to be the split octonion algebra $\mathscr{O}$ over K, although the data is certainly less familiar to most people! Then the algebra $J(A)$ is the exceptional Jordan algebra, and the variety X_A is the fourth Severi variety found by Lazarsfeld [LVdV84, Zak85]. The variety X_A is 16-dimensional, and it is often interpreted as a projective plane $\mathbb{P}^2(\mathscr{O})$ over $\mathscr{O}$ [SBG+95]. This interpretation is exactly how we recover a $\mathscr{O}$-line on a curve C from a map $C \to \mathbb{P}^2(\mathscr{O})$.

Theorem 5.27. *Let V and W be K-vector spaces of dimensions 3 and 27, respectively, with the split algebraic group E_6 acting on W. Then nondegenerate $\mathrm{GL}(V) \times E_6$-orbits of $V \otimes W$ are in bijection with isomorphism classes of nondegenerate quadruples (C, L, ξ, E), where C is a genus one curve over K, L is a degree 3 line bundle on C, $\xi : C \to \mathbb{P}^2(\mathscr{O}) \subset \mathbb{P}(W)$ is a map, and E is the rank 8 vector bundle on C obtained from pulling back the universal bundle on $\mathbb{P}^2(\mathscr{O})$, and $\det E \cong L^{\otimes 8}$.*

One may also take A to be a nonsplit composition algebra over K. We plan to discuss some applications of these cases in future work.

6. Representations associated to degree 2 line bundles

In this section, analogously to Section 5, we study a class of representations whose orbits are related to genus one curves with degree 2 line bundles. The main theorems in this section are summarized in Section 2.

We begin in §6.1 by considering the space of bidegree $(2, 2)$ forms on $\mathbb{P}^1 \times \mathbb{P}^1$. We show that the orbits here correspond to genus one curves equipped with a degree 2 line bundle and a nonzero point on the Jacobian. (This is analogous to the interpretation of orbits for the space of Rubik's cubes!) In §6.2–6.3, we then examine the space of hypercubes ($2 \times 2 \times 2 \times 2$ matrices) and some of its simpler variants; this space of hypercubes is the fundamental space for many degree 2 moduli problems, just as the space of Rubik's cubes, considered in the previous section, was the fundamental space for many degree 3 moduli problems.

In preparation for the general case, in §6.4 we then introduce the notion of "triply Hermitian cubes" with respect to a cubic Jordan algebra J, which form a vector space $\mathscr{C} = \mathscr{C}(J)$, and we describe a flag variety inside this space up to scaling. In §6.5, given an element of the space $V \otimes \mathscr{C}$ where V is a two-dimensional vector space, we then construct genus one curves with a projection to that flag variety. This yields bijections between orbits on $V \otimes \mathscr{C}$ (i.e., the space of "triply Hermitian hypercubes") and isomorphism classes of genus one curves equipped with degree 2 line bundles and additional vector bundles. After uniformly treating the bijections for such spaces, we then specialize to several of the split cases, for which the geometric data becomes easier to describe; many of these are related to interesting arithmetic structures.

Many of the orbit problems described in this section are used in [BH12] to determine average sizes of 2-Selmer groups for certain families of elliptic curves over $\mathbb{Q}$.

6.1. Bidegree $(2, 2)$ forms

Let V_1 and V_2 be two-dimensional vector spaces over K. A $(2, 2)$ *form f* over K is an element of $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$. With a choice of bases $\{w_1, w_2\}$ and $\{x_1, x_2\}$ of V_1 and V_2, respectively, such a form f may be represented as a polynomial

$$(59) \quad f(w_1, w_2, x_1, x_2) = a_{22}w_1^2 x_1^2 + a_{32}w_1 w_2 x_1^2 + a_{42}w_2^2 x_1^2 + a_{23}w_1^2 x_1 x_2$$
$$+ a_{33}w_1 w_2 x_1 x_2 + a_{43}w_2^2 x_1 x_2 + a_{24}w_1^2 x_2^2$$
$$+ a_{34}w_1 w_2 x_2^2 + a_{44}w_2^2 x_2^2.$$

The group $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$ acts on the space of $(2, 2)$ forms by the standard action on each factor. We will also consider a twisted action of $(g_1, g_2) \in \mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$:

$$(g_1, g_2)f(w, x) = \det(g_1)^{-1} \det(g_2)^{-1} f(g_1(w), g_2(x)).$$

This is the representation $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2 \otimes (\wedge^2 V_1 \otimes \wedge^2 V_2)^{-1}$ of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$; by abuse of notation, we will refer to this as the twisted action on $(2,2)$ forms. This twisted action is not faithful; for example, the scalars $\mathbb{G}_m(V_i)$ of $\mathrm{GL}(V_i)$ act trivially on all $(2,2)$ forms. Finally, the standard scaling action of $\mathbb{G}_m$ on such bidegree $(2,2)$ forms f will be relevant in the sequel. The group G for the moduli problem here will be the product of the scaling $\mathbb{G}_m$ and $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$ acting by the twisted action.

6.1.1. Geometric construction and bijection. The $(2,2)$ form f cuts out a bidegree $(2,2)$ curve C in $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$. If the curve C is smooth, then a standard computation shows that C has genus $(2-1)(2-1) = 1$. Pulling back line bundles via the embedding $\iota : C \hookrightarrow \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$ gives two degree 2 line bundles on C, namely

$$L_1 := \iota^* \mathcal{O}_{\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)}(1,0) \qquad \text{and} \qquad L_2 := \iota^* \mathcal{O}_{\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)}(0,1).$$

Each of the projection maps $\mathrm{pr}_i : C \to \mathbb{P}(V_i^\vee)$, for $i = 1$ or 2, is a degree 2 cover of $\mathbb{P}(V_i^\vee)$, ramified at four points over a separable closure of K. A binary quartic q_1 on V_1 associated to the ramification locus in $\mathbb{P}(V_1^\vee)$ may be computed by taking the discriminant of f as a quadratic polynomial on V_2:

$$
\begin{aligned}
q_1(w_1, w_2) : = {} & \mathrm{disc}(f(x_1, x_2)) \\
= {} & (a_{23} w_1^2 + a_{33} w_1 w_2 + a_{43} w_2^2)^2 \\
& - (a_{22} w_1^2 + a_{32} w_1 w_2 + a_{42} w_2^2)(a_{24} w_1^2 + a_{34} w_1 w_2 + a_{44} w_2^2),
\end{aligned}
$$

(60)

and similarly for $q_2(x_1, x_2)$ as a binary quartic form on V_2. The nonsingular genus one curve obtained from each of these binary quartics, as in §4.1, is isomorphic to the curve C. Via those isomorphisms, the line bundles L_1 and L_2 coincide with the natural degree 2 line bundles on the genus one curves coming from these binary quartics.

We call a $(2,2)$ form f or its associated curve C *nondegenerate* if both of the associated binary quartics are nondegenerate, i.e., have four distinct roots over a separable closure. For each of the binary quartics, this condition is given by the nonvanishing of the discriminant $\Delta(q_i)$. As the binary quartic q_i is invariant under the action of $\mathrm{SL}(V_j)$ on f, the discriminant $\Delta(q_i)$ is a degree 12 $\mathrm{SL}(V_i) \times \mathrm{SL}(V_j)$-invariant for f. Moreover, it is easy to check that $I(q_1) = I(q_2)$ and $J(q_1) = J(q_2)$, so $\Delta(q_1) = \Delta(q_2)$. Thus, the polynomials $I(f) := I(q_i)$ and $J(f) := J(q_i)$ for $i = 1$ or 2 are $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariants of f having degrees 4 and 6, respectively. The *discriminant* $\Delta(f) = \Delta(q_i)$ of

the $(2,2)$ form f is a degree 12 invariant, and a *nondegenerate* $(2,2)$ form is one with nonzero discriminant.[5] The nonvanishing of this discriminant is also equivalent to the condition that the curve C cut out by f is nonsingular.

Thus, from a nondegenerate $(2,2)$ form f, we have constructed a genus one curve in $\mathbb{P}^1 \times \mathbb{P}^1$, and the G-action preserves the isomorphism class of this curve and the line bundles. Conversely, given a genus one curve C and two degree 2 line bundles L_1 and L_2 on C, there are natural degree 2 maps $\eta_i : C \to \mathbb{P}(H^0(C, L_i)^\vee) = \mathbb{P}^1$ and the product map

$$(\eta_1, \eta_2) : C \longrightarrow \mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee) \ .$$

If $L_1 \cong L_2$, then (η_1, η_2) is a degree 2 cover of a diagonal in $\mathbb{P}^1 \times \mathbb{P}^1$, i.e., the image of this map is isomorphic to $\mathbb{P}^1$. Otherwise, we claim that this map is a closed immersion.

Lemma 6.1. *For a smooth irreducible genus one curve C and non-isomorphic degree 2 line bundles L_1 and L_2 on C, the composition*

$$C \xrightarrow{\ (\eta_1, \eta_2)\ } \mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee)$$

$$\Big\downarrow \text{Segre}$$

$$\mathbb{P}(H^0(C, L_1)^\vee \otimes H^0(C, L_2)^\vee)$$

is a closed immersion.

Proof. By Riemann-Roch, the spaces of sections $H^0(C, L_1), H^0(C, L_2)$, and $H^0(C, L_1 \otimes L_2)$ have dimensions 2, 2, and 4, respectively. The multiplication map

$$\mu_{12} : H^0(C, L_1) \otimes H^0(C, L_2) \longrightarrow H^0(C, L_1 \otimes L_2)$$

is an isomorphism, by Castelnuovo's basepoint-free pencil trick (see [ACGH85, p. 126]). Since $\deg(L_1 \otimes L_2) = 4$, the curve C is isomorphic to its image in $\mathbb{P}(H^0(C, L_1 \otimes L_2)^\vee) = \mathbb{P}^3$. Since the desired map is the composition of this map to $\mathbb{P}(H^0(C, L_1 \otimes L_2)^\vee)$ with the isomorphism $\mathbb{P}(\mu_{12}^\vee)$, it is a closed immersion. $\square$

---

[5]Neither $J(f)$ nor $\Delta(f)$ is a generator for the ring of $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariants of $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$. The invariant ring is a polynomial ring with generators in degrees 2, 3, and 4, and will be discussed more carefully in §6.1.2.

The image C_{12} of the curve C in $\mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee)$ is cut out by a $(2, 2)$ form, via the exact sequence

$$0 \to \mathcal{I}_C \to \mathcal{O}_{\mathbb{P}(H^0(C,L_1)^\vee) \times \mathbb{P}(H^0(C,L_2)^\vee)} \to \mathcal{O}_C \to 0$$

where $\mathcal{I}_C$ is the ideal defining C_{12}. Tensoring with $\mathcal{O}(2, 2)$, taking cohomology, and tensoring by the dual of $H^0(\mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee), \mathcal{I}_C(2, 2))$ gives a map from K to

$$
\begin{aligned}
H^0(\mathbb{P}(H^0(C, L_1)^\vee) &\times \mathbb{P}(H^0(C, L_2)^\vee), \mathcal{O}(2, 2)) \\
&\otimes (\wedge^2(H^0(C, L_1)))^{-1} \otimes (\wedge^2(H^0(C, L_2)))^{-1} \otimes \omega_C,
\end{aligned}
$$

where ω_C is the usual Hodge bundle for C. We thus obtain a bidegree $(2, 2)$ form, namely an element of $\mathrm{Sym}^2(H^0(C, L_1)) \otimes \mathrm{Sym}^2(H^0(C, L_2)) \otimes (\wedge^2(H^0(C, L_1)) \otimes \wedge^2(H^0(C, L_2)))^{-1}$. The factor ω_C fixes the scaling, just as in the cases in Section 4.

Thus, a genus one curve and two nonisomorphic degree 2 line bundles L_1 and L_2 give rise to a $(2, 2)$ form.

Theorem 6.2. *The nondegenerate G-orbits of $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$ for two-dimensional vector spaces V_1 and V_2 are in bijection with isomorphism classes of triples (C, L_1, L_2), where C is a genus one curve and L_1 and L_2 are non-isomorphic degree 2 line bundles on C.*

The stabilizer of the G-action corresponds to the automorphism group of the triple (C, L_1, L_2), which for a generic nondegenerate $(2, 2)$ form is the K-points of an extension of $\mathrm{Jac}(C)[2]$ by $\mathbb{G}_m^2$. In general, the stabilizer consists of the K-points of a possibly non-split extension of this group scheme by $\mathrm{Aut}(\mathrm{Jac}(C))$.

By the same argument as in Corollary 5.4, we may keep track of the difference $L_2 \otimes L_1^{-1}$ instead of L_2. The difference corresponds to a point on the Jacobian of C, and in fact, in $\mathrm{Pic}^0(C)(K)$.

Corollary 6.3. *The nondegenerate G-orbits of $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$ for two-dimensional vector spaces V_1 and V_2 are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve, L is a degree 2 line bundle on C, and $0 \neq P \in \mathrm{Pic}^0(C)(K)$.*

6.1.2. Invariant theory. The $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariants of the representation $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$ form a polynomial ring generated by invariants δ_2, δ_3, and δ_4 of degrees 2, 3, and 4 (see [Dem73, Vin76], for example). These same polynomials are relative invariants under the standard

action of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$, but are invariant under the twisted action of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$ described above. When f is a $(2,2)$ form given by (59), we may take the generators to be

$$\delta_2 = a_{33}^2 - 4a_{32}a_{34} + 8a_{24}a_{42} - 4a_{23}a_{43} + 8a_{22}a_{44}$$
$$\delta_3 = a_{24}a_{33}a_{42} - a_{23}a_{34}a_{42} - a_{24}a_{32}a_{43} + a_{22}a_{34}a_{43} + a_{23}a_{32}a_{44} - a_{22}a_{33}a_{44}$$
$$\delta_4 = I(f)$$

although any linear combination of $I(f)$ and δ_2^2 is a degree 4 generator of the invariant ring. Given a $(2,2)$ form f, these invariants are essentially described by the triple (C, L, P) of Corollary 6.3, or in particular, the Jacobian E of C and the coordinates of P on some form of E.

Recall that $I(f)$ and $J(f)$ are $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariants of degrees 4 and 6, obtained from the binary quartics q_i for $i = 1$ or 2. The Jacobian of the curve C given by $f = 0$ is the Jacobian of the genus one curve associated to q_i, and it can be written in Weierstrass form as

$$y^2 = x^3 - 27I(f)x - 27J(f).$$

The nonzero point P has coordinates $(x(f), y(f))$ satisfying E, which are $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariants of degrees 2 and 3, respectively, i.e., scalar multiples of the generators δ_2 and δ_3 of the invariant ring! The relation

$$(108\delta_3)^2 = (3\delta_2)^3 - 27I(f)(3\delta_2) - 27J(f)$$

shows that $(x(f), y(f)) = (3\delta_2, 108\delta_3)$.

We may also write the Jacobian of the genus one curve C in generalized Weierstrass form as

(61) $$y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x$$

where the coefficients satisfy

$$a_2 = 9\delta_2, \qquad a_3 = 216\delta_3, \qquad a_4 = 27\delta_2^2 - 27\delta_4,$$

and are different generators of the invariant ring (since we are working over a field K not of characteristic 2 or 3).

6.2. Hypercubes

We now consider $2 \times 2 \times 2 \times 2$ boxes, or hypercubes. This space is the fundamental representation for the degree 2 cases, and we will study a number of variants and generalizations in the subsections that follow.

The representation in question is $V := V_1 \otimes V_2 \otimes V_3 \otimes V_4$, where each V_i is a 2-dimensional K-vector space, with the natural action by $G := \mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3) \times \mathrm{GL}(V_4)$. We prove the following theorem, where nondegeneracy corresponds to the nonvanishing of a certain degree 24 invariant, described in more detail below.

Theorem 6.4. *Let V_1, V_2, V_3, V_4 be 2-dimensional vector spaces over K. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3) \times \mathrm{GL}(V_4)$-orbits of the space $V_1 \otimes V_2 \otimes V_3 \otimes V_4$ are in bijection with isomorphism classes of quintuples (C, L_1, L_2, L_3, L_4), where C is a genus one curve over K, and the L_i are degree 2 line bundles on C, satisfying $L_1 \otimes L_2 \cong L_3 \otimes L_4$ and $L_i \not\cong L_j$ for $i \neq j, 1 \leq i \leq 2, 1 \leq j \leq 4$.*

The stabilizer of a nondegenerate hypercube giving the genus one curve C is exactly the automorphism group of the quintuple, provided that we record the isomorphism $L_1 \otimes L_2 \cong L_3 \otimes L_4$. In particular, let H be the extension of $\mathrm{Jac}(C)[2]$ by the kernel of the multiplication map $\mathbb{G}_m(V_1) \times \mathbb{G}_m(V_2) \times \mathbb{G}_m(V_3) \times \mathbb{G}_m(V_4) \to \mathbb{G}_m$, where each $\mathbb{G}_m(V_i)$ is the set of scalar transformations of V_i for $1 \leq i \leq 4$. Then the stabilizer consists of the K-points of a possibly non-split extension of $\mathrm{Aut}(\mathrm{Jac}(C))$ by this group scheme H. For example, if the j-invariant of $\mathrm{Jac}(C)$ is not 0 or 1728, and C has a rational point O and full rational 2-torsion with respect to O, generated by P_1 and P_2, then the hypercube corresponding to the quintuple $(C, \mathcal{O}(2O), \mathcal{O}(O + P_1), \mathcal{O}(O + P_2), \mathcal{O}(O + P_1 + P_2))$ will have stabilizer group $H \times \mathbb{Z}/2\mathbb{Z}$, that is, an extension of $(\mathbb{Z}/2\mathbb{Z})^3$ by $\mathbb{G}_m^3$.

6.2.1. Geometric construction.
We describe how to construct the genus one curve and degree 2 line bundles from a hypercube; any G-equivalent hypercube will produce an isomorphic curve and line bundles.

Let $\mathcal{A} \in V_1 \otimes V_2 \otimes V_3 \otimes V_4$, so $\mathcal{A}$ induces a linear map from $V_1^\vee \otimes V_2^\vee$ to $V_3 \otimes V_4$ and thus a linear map

$$\mathbb{P}(V_1^\vee \otimes V_2^\vee) \to \mathbb{P}(V_3 \otimes V_4).$$

There is a natural determinantal quadric in $\mathbb{P}(V_3 \otimes V_4)$; with choices of bases for V_3 and V_4, it consists of nonzero 2×2 matrices, up to scaling, which have

determinant 0. Let C_{12} be the intersection of this quadric with the image of the Segre map $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) \to \mathbb{P}(V_1^\vee \otimes V_2^\vee)$, composed with the linear map given by $\mathcal{A}$. Then C_{12} is generically a curve.

More explicitly, the curve C_{12} is a determinantal variety, given by the vanishing of the determinant of a 2×2 matrix of bidegree $(1, 1)$ forms on $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) = \mathbb{P}^1 \times \mathbb{P}^1$. With choices of bases for all the vector spaces V_i, the hypercube may be written as a $2 \times 2 \times 2 \times 2$ array $(a_{rstu})_{1 \leq r,s,t,u \leq 2}$ with $a_{rstu} \in K$. Then the curve C_{12} is given as the vanishing of the determinant of $\mathcal{A}(w, x, \cdot, \cdot)$, which may be represented as the matrix

$$(a_{11tu}w_1x_1 + a_{12tu}w_1x_2 + a_{21tu}w_2x_1 + a_{22tu}w_2x_2)_{1 \leq t,u \leq 2}$$

where $\{w_1, w_2\}$ and $\{x_1, x_2\}$ are the bases for $V_1^\vee$ and $V_2^\vee$, respectively. This determinant $f_{12}(w, x)$ is a $(2, 2)$ form, i.e., an element of $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$, and it is invariant under the action $\mathrm{SL}(V_3) \times \mathrm{SL}(V_4)$. One may similarly define the varieties C_{ij} for any $1 \leq i \neq j \leq 4$. (We identify C_{ij} and C_{ji}.)

We call a hypercube *nondegenerate* if the variety C_{12} is smooth and one-dimensional, which by §6.1 is given by the nonvanishing of a $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$ invariant of degree 12 in the coefficients of f_{12} and thus degree 24 in the hypercube. This degree 24 polynomial is invariant under all $\mathrm{SL}(V_i)$ for $1 \leq i \leq 4$. By symmetry (or explicit computation), this polynomial is the discriminant for all the f_{ij}, and we call it the *discriminant* of the hypercube $\mathcal{A}$ itself. Nondegeneracy is preserved by the action of G. In the sequel, we will only work with nondegenerate hypercubes.

If $\mathcal{A}$ is nondegenerate, then for all points $(w, x) \in C_{12}$, the matrix $\mathcal{A}(w, x, \cdot, \cdot)$ is not the zero matrix and thus has rank exactly 1. (If it were the zero matrix, then all the partial derivatives would vanish at the point (w, x), so C_{12} would not be smooth.) So for all $(w, x) \in C_{12}$, there is exactly one dimension of vectors $y \in V_3$ such that $\mathcal{A}(w, x, y, \cdot) = 0$ (and similarly, one dimension of vectors $z \in V_4$ with $\mathcal{A}(w, x, \cdot, z) = 0$).

Given a nondegenerate hypercube $\mathcal{A}$, it turns out that all of the resulting curves C_{ij} are isomorphic! To see this, define the variety

$$C_{123} := \{(w, x, y) \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) \times \mathbb{P}(V_3^\vee) : \mathcal{A}(w, x, y, \cdot) = 0\}.$$

The projection π_{123}^{12} of this variety C_{123} onto C_{12} is an isomorphism, where the inverse map ρ_{12}^{123} is given by taking the point in $\mathbb{P}(V_3^\vee)$ corresponding to the exactly one-dimensional kernel of $\mathcal{A}(w, x, \cdot, \cdot)$. By symmetry, the curves C_{13} and C_{23} are also isomorphic to C_{123}. We may similarly define the curves $C_{ijk} \subset \mathbb{P}(V_i^\vee) \times \mathbb{P}(V_j^\vee) \times \mathbb{P}(V_k^\vee)$ for any $\{i, j, k\} \subset \{1, 2, 3, 4\}$, and they are

all isomorphic to their projections to any two factors. The C_{ij} are all smooth irreducible isomorphic genus one curves, related by natural isomorphisms

$$\tau_{ij}^{jk} : C_{ij} \xrightarrow{\rho_{ij}^{ijk}} C_{ijk} \xrightarrow{\pi_{ijk}^{ik}} C_{jk}$$

for $\{i, j, k\} \subset \{1, 2, 3, 4\}$, where each π is the projection and ρ is the natural inverse "un-projection" map (where each map has domain given by the subscript and target given by the superscript). We also obtain isomorphisms of the form

$$\tau_{ijk}^{jkl} : C_{ijk} \to C_{jk} \to C_{jkl}$$

for $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Finally, by the definition of these curves, we have natural projection maps

$$\pi_{ij}^i : C_{ij} \to \mathbb{P}(V_i^\vee) \qquad \text{and} \qquad \pi_{ijk}^i : C_{ijk} \to \mathbb{P}(V_i^\vee).$$

It is clear that τ_{ijk}^{jkl} and τ_{jkl}^{ijk} are inverse maps, as are τ_{ij}^{jk} and τ_{jk}^{ij}. However, composing more than two such maps in sequence will not always give identity maps on these curves. There are two types of interesting cycles we can obtain from composing the τ_{ijk}^{jkl} maps. These are best exemplified by arranging the curves C_{ijk} in a tetrahedron as in (8): there are four triangles (the faces of the tetrahedron) and three four-cycles.

Lemma 6.5. *The triangle of maps on each of the faces of the tetrahedron* (8) *is not the identity map, but composing it twice gives the identity map. In particular, the composition $C_{ijk} \to C_{ikl} \to C_{ijl} \to C_{ijk}$ is the hyperelliptic involution for $C_{ijk} \to \mathbb{P}(V_i^\vee)$, sending any point (w, x_1, y_1) to the point (w, x_2, y_2), where $\{x_1, x_2\}$ and $\{y_1, y_2\}$ are the (not necessarily distinct) solutions to $\mathcal{A}_\lrcorner (w \otimes x) = 0$ and $\mathcal{A}_\lrcorner (w \otimes y) = 0$, respectively.*

Proof. Given a point $w \in \mathbb{P}(V_1^\vee)$ not in the ramification locus of the projection from C_{12}, there are two distinct points $x_1, x_2 \in \mathbb{P}(V_2^\vee)$ such that $\det \mathcal{A}(w, x_i, \cdot, \cdot) = 0$. For $i = 1$ or 2, we have $\mathcal{A}(w, x_i, y_i, \cdot) = 0$ for exactly one point $y_i \in \mathbb{P}(V_3^\vee)$. Since $\mathcal{A}(w, x_2, y_1, z) = 0$ for some $z \in \mathbb{P}(V_4^\vee)$, the linear form $\mathcal{A}(w, \cdot, y_1, z)$ vanishes when evaluated at both x_1 and x_2, so it is identically 0; similarly, the linear form $\mathcal{A}(w, x_2, \cdot, z)$ is identically zero. Thus, we have the composition

$$C_{123} \xrightarrow{\tau_{123}^{134}} C_{134} \xrightarrow{\tau_{134}^{124}} C_{124} \xrightarrow{\tau_{124}^{123}} C_{123}$$
$$(w, x_1, y_1) \longmapsto (w, y_1, z) \longmapsto (w, x_2, z) \longmapsto (w, x_2, y_2). \qquad \square$$

Four-cycles of maps τ_{ijk}^{jkl} are also not the identity; we will show this by proving a relation among degree 2 line bundles defined on each of the curves. For simplicity of notation, choose one curve, say C_{12}, to be the primary curve under consideration. This choice matters in the definitions and constructions we will make in the sequel, but all choices are equivalent.

Define four line bundles L_i on C_{12} by pulling back the line bundle $\mathcal{O}(1)$ from each $\mathbb{P}(V_i^\vee)$. Of course, it is important through which maps we choose to pullback the bundle:

$$
\begin{aligned}
L_1 &:= (\pi_{12}^1)^* \mathcal{O}_{\mathbb{P}(V_1^\vee)}(1) \\
L_2 &:= (\pi_{12}^2)^* \mathcal{O}_{\mathbb{P}(V_2^\vee)}(1) \\
L_3 &:= (\pi_{123}^3 \circ \rho_{12}^{123})^* \mathcal{O}_{\mathbb{P}(V_3^\vee)}(1) \\
L_4 &:= (\pi_{124}^4 \circ \rho_{12}^{124})^* \mathcal{O}_{\mathbb{P}(V_4^\vee)}(1).
\end{aligned}
$$
(62)

That is, L_1 and L_2 come directly from the maps $C_{12} \to \mathbb{P}(V_1^\vee)$ and $C_{12} \to \mathbb{P}(V_2^\vee)$, and for $i = 3$ or 4, the line bundle L_i is pulled back via the simplest maps $C_{12} \to C_{12i} \to C_{2i} \to \mathbb{P}(V_i^\vee)$. Since all the curves C_{ij} are defined by bidegree $(2, 2)$ equations, each of these line bundles on C_{12} have degree 2.

By Lemma 6.1, the line bundles L_1 and L_2 are not isomorphic, since C_{12} is a smooth irreducible genus one curve given by a nondegenerate $(2, 2)$ form. Similarly, since C_{ij} is also a smooth irreducible genus one curve for $i = 1$ or 2 and $j = 3$ or 4, the line bundles $(\tau_{ij}^{12})^* L_i = (\pi_{ij}^i)^* \mathcal{O}_{\mathbb{P}(V_i^\vee)}(1)$ and $(\tau_{ij}^{12})^* L_j = (\pi_{ij}^j)^* \mathcal{O}_{\mathbb{P}(V_j^\vee)}(1)$ on C_{ij} are not isomorphic, so L_i and L_j are not isomorphic bundles on C_{12}. Thus, the four line bundles defined in (62) are all pairwise nonisomorphic, except possibly L_3 and L_4.

Lemma 6.6. *For the line bundles on C_{12} defined above, we have the relation*

$$L_1 \otimes L_2 \cong L_3 \otimes L_4.$$
(63)

Proof. With a choice of a basis for V_i, points of the projective spaces $\mathbb{P}(V_i^\vee)$ may be represented as $[a : b]$. Let $\mathcal{D}(L)$ be the linear equivalence class of divisors corresponding to a line bundle L. A representative D_3 of $\mathcal{D}(L_3)$ is (the formal sum of the points in) the preimage of a fixed point, say $[1 : 0]$, in $\mathbb{P}(V_3^\vee)$, and similarly, we may choose a divisor D_4 in the class of $\mathcal{D}(L_4)$ as the preimage of $[1 : 0] \in \mathbb{P}(V_4^\vee)$. Let $\mathcal{A}(w, x, \cdot, \cdot)$ be denoted by the matrix

$$
\begin{pmatrix}
\mathcal{A}_{11}(w, x) & \mathcal{A}_{12}(w, x) \\
\mathcal{A}_{21}(w, x) & \mathcal{A}_{22}(w, x)
\end{pmatrix} \in V_3 \otimes V_4.
$$

Then $D_3 + D_4$ is the sum of the four points that are solutions (counted up to multiplicity) of the system

$$\left\{ \begin{array}{c} \mathcal{A}_{11}(w, x) = 0 \\ \det \mathcal{A}(w, x, \cdot, \cdot) = 0 \end{array} \right\}.$$

Interpreted in another way, these four points of intersection are exactly the points of intersection of C_{12} and the bidegree $(1, 1)$ curve given by $\mathcal{A}_{11}$ in $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$. Thus, the line bundle corresponding to the sum of these four points is just the pullback of $\mathcal{O}_{\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)}(1, 1)$ to C_{12}; that is, $\mathcal{O}(D_3 + D_4) \cong L_1 \otimes L_2$, which is the desired relation. $\qquad\square$

Using this relation among the line bundles, a computation shows that the four-cycles in the tetrahedron (8) are not commutative. For example, the composition map

$$\tau_{124}^{123} \circ \tau_{134}^{124} \circ \tau_{234}^{134} \circ \tau_{123}^{234} : C_{123} \longrightarrow C_{123}$$

is a nontrivial automorphism, given as a translation by the point

$$P := L_3 \otimes L_1^{-1} = L_2 \otimes L_4^{-1} \in \mathrm{Pic}^0(C_{12}) \cong \mathrm{Pic}^0(C_{123}).$$

The reverse four-cycle is the inverse map and is given by translation by $-P$. Similarly, the other four-cycles are given by translation by the points $L_4 \otimes L_1^{-1}$ and $L_2 \otimes L_1^{-1}$ (up to sign). Because of the relation in (63), these points (with the correct choice of sign) add up to 0 on the Jacobian! This may also be seen directly from the tetrahedron picture, using the facts that each four-cycle decomposes as two consecutive three-cycles and that each three-cycle composed with itself is the identity (by Lemma 6.5).

We summarize these results in the following proposition:

Proposition 6.7. *Given a nondegenerate hypercube $\mathcal{A}$, we have the following statements, for any permutation (i, j, k, l) of $(1, 2, 3, 4)$:*

(i) *The composition map*

$$\alpha_{ijkl} := \tau_{ijk}^{jkl} \circ \tau_{ijl}^{ijk} \circ \tau_{ikl}^{ijl} \circ \tau_{jkl}^{ikl} : C_{jkl} \longrightarrow C_{jkl}$$

is the automorphism of C_{jkl} given by translation by the point

$$P_{ijkl} := M_l \otimes M_j^{-1} \in \mathrm{Pic}^0(C_{jl}) \cong \mathrm{Pic}^0(C_{jkl})$$

where $M_j = (\pi_{jl}^j)^* \mathcal{O}_{\mathbb{P}(V_j^\vee)}(1)$ and $M_l = (\pi_{jl}^l)^* \mathcal{O}_{\mathbb{P}(V_l^\vee)}(1)$ are degree 2 line bundles on C_{jl}.

(ii) *We have $P_{ijkl} = -P_{ilkj}$, as $\alpha_{ijkl} \circ \alpha_{ilkj}$ is the identity map on C_{jkl}.*

(iii) *The points P_{ijkl}, P_{iklj}, and P_{iljk} sum to 0 on the Jacobian of C_{jkl}, so the composition of the automorphisms α_{ijkl}, α_{iklj}, and α_{iljk} in any order is the identity map on C_{jkl}.*

6.2.2. Bijections. Because the geometric constructions of the previous section are entirely G-invariant, we have already seen that the G-orbit of a nondegenerate hypercube gives rise to a genus one curve and four line bundles (with a relation), up to isomorphism. In fact, we may construct a nondegenerate hypercube from such a curve, along with the line bundles, which will prove Theorem 6.4.

Proof of Theorem 6.4. Let C be a genus one curve, and let L_1, L_2, L_3, L_4 be degree 2 line bundles on C as in the statement of the theorem. We first show how to construct a hypercube from this data.

Lemma 6.8. *Given a genus one curve C and three non-isomorphic degree 2 line bundles L_1, L_2, L_3 on C, the multiplication map (i.e., the cup product on cohomology)*

$$\mu_{123} : H^0(C, L_1) \otimes H^0(C, L_2) \otimes H^0(C, L_3) \longrightarrow H^0(C, L_1 \otimes L_2 \otimes L_3)$$

is surjective, and its kernel may be naturally identified with the space of global sections $H^0(C, L_i^{-1} \otimes L_j \otimes L_k)$ for any permutation $\{i, j, k\}$ of $\{1, 2, 3\}$.

Proof. Recall from the proof of Lemma 6.1 that the multiplication map

$$\mu_{ij} : H^0(C, L_i) \otimes H^0(C, L_j) \longrightarrow H^0(C, L_i \otimes L_j)$$

for two such line bundles is an isomorphism, due to the basepoint-free pencil trick. We apply the same trick again here: for any permutation $\{i, j, k\}$ of $\{1, 2, 3\}$, we tensor the sequence $0 \to L_i^{-1} \to H^0(C, L_i) \otimes \mathcal{O}_C \to L_i \to 0$ with $L_j \otimes L_k$ and take cohomology to obtain the exact sequence

$$0 \to H^0(C, L_i^{-1} \otimes L_j \otimes L_k) \to H^0(C, L_i) \otimes H^0(C, L_j \otimes L_k) \to H^0(C, L_i \otimes L_j \otimes L_k)$$
(64) $$\to H^1(C, L_i^{-1} \otimes L_j \otimes L_k) = 0.$$

As the map μ_{123} factors through the isomorphism

$$(\mathrm{id}, \mu_{jk}) : H^0(C, L_i) \otimes H^0(C, L_j) \otimes H^0(C, L_k) \to H^0(C, L_i) \otimes H^0(C, L_j \otimes L_k),$$

the sequence (64) shows that μ_{123} is surjective and its kernel may be naturally identified with $H^0(C, L_i^{-1} \otimes L_j \otimes L_k)$. $\qquad\square$

Given C, L_1, L_2, L_3 as in the lemma, by Riemann-Roch, the kernel of μ_{123} has dimension 2, and we may use the inclusion of this kernel into the domain to specify a hypercube

$$\mathcal{A} \cong \mathrm{Hom}(\ker \mu_{123}, H^0(C, L_1) \otimes H^0(C, L_2) \otimes H^0(C, L_3))$$
$$\in H^0(C, L_1) \otimes H^0(C, L_2) \otimes H^0(C, L_3) \otimes (\ker \mu_{123})^\vee$$

where $V_i = H^0(C, L_i)$ for $1 \leq i \leq 3$ and $V_4 = (\ker \mu_{123})^\vee$. We will show below that the hypercube $\mathcal{A}$ thus constructed is nondegenerate and that the geometric construction from $\mathcal{A}$ gives a tuple isomorphic to the original (C, L_1, L_2, L_3, L_4).

Let C'_{ij} be the image of C via the natural immersion into $\mathbb{P}(H^0(C, L_i)^\vee) \times \mathbb{P}(H^0(C, L_j)^\vee)$. Let C_{ij} be constructed from $\mathcal{A}$ by

$$C_{ij} := \{(w, x) \in \mathbb{P}(V_i^\vee) \times \mathbb{P}(V_j^\vee) : \det(\mathcal{A} \lrcorner (w \otimes x)) = 0\} \subset \mathbb{P}(V_i^\vee) \times \mathbb{P}(V_j^\vee).$$

We will show that these two varieties are the same for all $i \neq j$, but first for *some* $i \neq j$.

Claim 6.9. *For some $1 \leq i \neq j \leq 3$, we have $C_{ij} = C'_{ij}$ as sets.*

Proof. For all $i \neq j$, the inclusion $C'_{ij} \subseteq C_{ij}$ is easy: for each $1 \leq k \leq 3$, let $\{r_{k1}, r_{k2}\}$ be a basis of $H^0(C, L_k)$. Then the definition of $\mathcal{A}$ implies that

$$\mathcal{A} \lrcorner ([r_{i1}(p) : r_{i2}(p)] \otimes [r_{j1}(p) : r_{j2}(p)] \otimes [r_{k1}(p) : r_{k2}(p)]) = 0$$

for all points $p \in C$, so $([r_{i1}(p) : r_{i2}(p)], [r_{j1}(p) : r_{j2}(p)])$ lies in C_{ij}. Since C_{ij} is defined by a bidegree $(2, 2)$ equation f_{ij} in $\mathbb{P}(V_i^\vee) \times \mathbb{P}(V_j^\vee)$, if we show that f_{ij} is nonzero and irreducible, then we find that C_{ij} is a smooth irreducible genus one curve and thus $C_{ij} = C'_{ij}$.

An irreducible bidegree (d_1, d_2) form on $\mathbb{P}^1 \times \mathbb{P}^1$ defines a genus $(d_1 - 1)(d_2 - 1)$ curve. So if f_{ij} is nonzero and factors nontrivially, then no irreducible component can be a smooth irreducible genus one curve. However, since C_{ij} contains the smooth irreducible genus one curve C'_{ij}, the polynomial f_{ij} must be either zero or irreducible for each pair $i \neq j$. If $f_{ij} = 0$ identically, then C_{ij} is all of $\mathbb{P}(V_i^*) \times \mathbb{P}(V_j^*)$. The projection of

$$C_{123} := \{(w, x, y) \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) \times \mathbb{P}(V_3^\vee) : \mathcal{A}(w, x, y, \cdot) = 0\}$$

to any $\mathbb{P}(V_i^\vee) \times \mathbb{P}(V_j^\vee)$ is exactly C_{ij} by definition, and we will show that at least one of these projections is not two-dimensional.

Let f and g be the two tridegree $(1,1,1)$ equations defining C_{123}. Because $\mathcal{A}$ is defined by two linearly independent elements of $\ker \mu_{123}$, we have that f and g are nonzero and not multiples of one another. If $\gcd(f,g) = 1$, then C_{123} is a complete intersection and thus a one-dimensional variety. Otherwise, suppose without loss of generality that $\gcd(f,g)$ has tridegree $(1,1,0)$ or $(1,0,0)$. In either case, the projection to $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$ is still one-dimensional. Therefore, there exists *some* $i \neq j$ such that C_{ij} is not two-dimensional, and thus must be exactly C'_{ij}. $\qquad\square$

Since f_{ij} cuts out a smooth irreducible genus one curve, we have disc f_{ij} is nonzero. Thus, the hypercube $\mathcal{A}$ has nonzero discriminant and is nondegenerate.

As $\operatorname{disc}(\mathcal{A}) \neq 0$, the polynomials f_{kl} do not vanish for any $k \neq l$, and the C_{kl} are smooth irreducible genus one curves. It follows from the proof of Claim 6.9 that all of the C_{kl} are in fact set-theoretically equal to C'_{kl}. Moreover, C_{123} is set-theoretically equal to the image C'_{123} of the embedding of C into the triple product space $\mathbb{P}(H^0(C,L_1)^\vee) \times \mathbb{P}(H^0(C,L_2)^\vee) \times \mathbb{P}(H^0(C,L_3)^\vee)$. Because there is a canonical isomorphism $C'_{123} \to C_{123}$, for $1 \leq i \leq 3$, the pullbacks of $\mathcal{O}_{\mathbb{P}(H^0(C,L_i)^\vee)}(1)$ to C_{123} and then to C are exactly the line bundles L_i.

From a genus one curve and three nonisomorphic degree 2 line bundles on this curve, we have constructed a nondegenerate hypercube. This hypercube, in turn, produces—via the constructions of §6.2.1—an isomorphic curve and the same line bundles. Similarly, by the definitions of these maps, going from G-orbits of nondegenerate hypercubes to quintuples (C, L_1, L_2, L_3, L_4) as in the theorem, and then back to G-orbits of hypercubes, is the identity map. $\qquad\square$

We now rewrite the basic bijection of Theorem 6.4, by describing the geometric data in a slightly different way. This is analogous to the corollary following Theorem 5.1. We simply replace the data of the line bundles L_2, L_3, L_4 by the differences between each of them and L_1, which is a point on $\operatorname{Pic}^0(C) \subset \operatorname{Jac}(C)$. Since the sum of these differences (up to sign) is zero, it suffices to keep track of two such points on the Jacobian of the curve, say $P := L_2 \otimes L_1^{-1}$ and $P' := L_3 \otimes L_2^{-1}$.

Corollary 6.10. *Let V_1, V_2, V_3, V_4 be 2-dimensional K-vector spaces. Then the nondegenerate $\operatorname{GL}(V_1) \times \operatorname{GL}(V_2) \times \operatorname{GL}(V_3) \times \operatorname{GL}(V_4)$-orbits of $V_1 \otimes V_2 \otimes V_3 \otimes V_4$ are in bijection with isomorphism classes of quadruples (C, L, P, P'), where C is a genus one curve over K, L is a degree 2 line bundle on C, and P and P' are distinct nonzero points in $\operatorname{Pic}^0(C)(K)$.*

This also concludes the proof of Theorem 2.1, where we take P'' to represent the difference between L_1 and L_3.

6.2.3. Invariant theory. The $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2) \times \mathrm{SL}(V_3) \times \mathrm{SL}(V_4)$-invariants of an element of $V_1 \otimes V_2 \otimes V_3 \otimes V_4$, for two-dimensional vector spaces V_i, form a polynomial ring generated freely by a_2, a_4, a_4', a_6 of degrees 2, 4, 4, and 6, respectively [Lit89]. Just as in the previous cases considered, these invariants have several interpretations in terms of each orbit's geometric data consisting of a genus one curve C, a degree 2 line bundle L, and nonzero points P, P', and P'' in $\mathrm{Pic}^0(C)(K)$ that sum to 0.

One geometric interpretation of the generators of the invariant ring was discussed in §2.4: the Jacobian of the genus one curve is given by

$$(65) \qquad E : y^2 = x^3 + a_8 x + a_{12},$$

where we have formulas for a_8 and a_{12} in terms of a_2, a_4, a_4', and a_6; then a_2 is the slope of the line on which P, P', P'' lie (on E); (a_4, a_6) are the coordinates for the point P on E; and a_4' is the x-coordinate for P'.

Another interpretation gives a model for the Jacobian elliptic curve with fixed points corresponding to P and P':

Proposition 6.11. *There exists a choice of normalization for the $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2) \times \mathrm{SL}(V_3) \times \mathrm{SL}(V_4)$-invariants δ_2, δ_4, δ_4', δ_6 such that given a nondegenerate tensor in $V_1 \otimes V_2 \otimes V_3 \otimes V_4$ corresponding to (C, L, P, P') as in Corollary 6.10, the Jacobian of C may be given in normal form as*

$$(66) \qquad E : y^2 + \delta_4' y = x^4 + \delta_2 x^3 + \delta_4 x^2 + \delta_6 x$$

with identity point $(0,0)$, and the points P and P' correspond to the two points at infinity when homogenized.

Just as for Proposition 5.5, straightforward proofs of both of these results are computational. In this case, the invariants are very reasonable to work with explicitly, and it is easy to show that the elliptic curve in (66) is isomorphic to the Jacobian of the genus one curves constructed from the hypercube and that the points at infinity give the translations α_{ijk}. An abstract proof of Proposition 6.11, again like in Proposition 5.5, relies on the fact that elliptic curves with two distinct non-identity points may be written in the form (66), so the coefficients δ_2, δ_4, δ_4', δ_6 are relative $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3) \times \mathrm{GL}(V_4)$-invariants of $V_1 \otimes V_2 \otimes V_3 \otimes V_4$.

For any elliptic curve E over K of the form (66), there always exists a G-orbit of V where E is the Jacobian of the associated genus one curve, giving the analogous statement to Corollary 5.7:

Corollary 6.12. *The map from nondegenerate orbits $V(K)/G(K)$ to elliptic curves of the form*

$$E : y^2 + \delta_4' y = x^4 + \delta_2 x^3 + \delta_4 x^2 + \delta_6 x$$

with δ_2, δ_4, δ_4', $\delta_6 \in K$, by taking the Jacobian of the genus one curve associated to the orbit, is surjective.

6.3. Symmetric hypercubes

In this section, we study "symmetrized" hypercubes, as discussed in §2.5–2.8. We show that nondegenerate orbits of the different types of symmetric hypercubes correspond to genus one curves with different numbers of degree 2 line bundles. Nondegeneracy for symmetric hypercubes is determined by the nonvanishing of the same degree 24 discriminant for hypercubes, although this discriminant factors differently in each case.

6.3.1. Doubly symmetric hypercubes. The simplest case is that of doubly symmetric hypercubes, i.e., elements of the representation $V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3 \subset V_1 \otimes V_2 \otimes V_3 \otimes V_3$ of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$, where the V_i are 2-dimensional K-vector spaces. With choices of bases for each vector space, the elements may be viewed as doubly symmetric hypercubes or as 2×2 matrices of binary quadratic forms. Away from characteristic 2, this is the same as the quotient representation $V_1 \otimes V_2 \otimes \mathrm{Sym}^2 V_3$.

Theorem 6.13. *Let V_1, V_2, V_3 be 2-dimensional vector spaces over K. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$-orbits of $V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3$ are in bijection with isomorphism classes of quadruples (C, L_1, L_2, L_3), where C is a genus one curve over K, and L_1, L_2, L_3 are degree 2 line bundles on C satisfying $L_1 \otimes L_2 \cong L_3^{\otimes 2}$ and L_3 not isomorphic to L_1 or L_2.*

Proof. Given a nondegenerate element $\mathcal{A} \in V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3 \subset V_1 \otimes V_2 \otimes V_3 \otimes V_3$, we construct the genus one curve $C \subset \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$ and four degree 2 line bundles L_1, L_2, L_3, L_4 on C in the same way as in §6.2. The symmetry implies that the line bundles L_3 and L_4 may be naturally identified, so we have from before that $L_1 \otimes L_2 \cong L_3^{\otimes 2}$ and L_3 is not isomorphic to L_1 or L_2.

Conversely, given such (C, L_1, L_2, L_3) as in the theorem, we may set $L_4 = L_3$ and use the construction in the proof of Theorem 6.4 to obtain a nondegenerate orbit of a hypercube $\mathcal{A} \in V_1 \otimes V_2 \otimes V_3 \otimes V_4$, where $V_i = H^0(C, L_i)$ for $i = 1, 2, 3$ and V_4 is the dual of the kernel of the multiplication map μ_{123}. From the proof of Theorem 6.4, we see that V_4 is also identified

with $H^0(C, L_4)$, so the spaces V_3 and V_4 are naturally identified, say by $\psi_{43} : V_4 \to V_3$. The maps from $C \cong C_{12} \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee)$ to $\mathbb{P}(V_3^\vee)$ and $\mathbb{P}(V_4^\vee)$ are both given by sections of the same line bundle L_3 and thus identical (after applying the identification ψ_{43}).

Now given a rank one element $B \in V \otimes V$ for a 2-dimensional K-vector space V, if $B(x, \cdot) = 0$ and $B(\cdot, x) = 0$ for some nonzero $x \in V^\vee$, then B is in the subspace $\mathrm{Sym}_2 V$ of $V \otimes V$. Therefore, for any $(x, y) \in C_{12}$, the map $1 \otimes \psi_{43}$ on $V_3 \otimes V_4$ takes $\mathcal{A}(x, y, \cdot, \cdot)$ to an element of $\mathrm{Sym}_2 V_3 \subset V_3 \otimes V_3$. And since C_{12} spans $\mathbb{P}(H^0(C, L_1)^\vee) \times \mathbb{P}(H^0(C, L_2)^\vee)$, the map $1 \otimes 1 \otimes 1 \otimes \psi_{43}$ on $V_1 \otimes V_2 \otimes V_3 \otimes V_4$ sends $\mathcal{A}$ to an element of $V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3 \subset V_1 \otimes V_2 \otimes V_3 \otimes V_3$. □

The two points P and P' referred to in Corollary 6.10 are now related; in particular, we have $P = 2P'$. Therefore, it suffices to keep track of only a single point P', giving the following basis-free formulation of Theorem 2.4:

Corollary 6.14. *Let V_1, V_2, V_3 be 2-dimensional vector spaces over K. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$-orbits of $V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3$ are in bijection with isomorphism classes of quadruples (C, L, P'), where C is a genus one curve over K, and L is a degree 2 line bundle on C, and P' is a nonzero, non-2-torsion point in $\mathrm{Jac}_C^2(K)$.*

The ring of $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2) \times \mathrm{SL}(V_3)$-invariants of $V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3$ is a polynomial ring generated in degrees 2, 4, and 6 [Lit89]. Again, we may find several related geometric interpretations of these invariants.

Recall that there is a choice of rational generators a_2, a_4, a_4', a_6 for the invariant ring of hypercubes such that the Jacobian of the genus one curve is given by (65), where a_8 and a_{12} are given as in (11) and the two points on the Jacobian are $P = (a_4, a_6)$ and $P' = (a_4', a_6')$. For the doubly symmetric hypercube, as we know from Corollary 6.14, because we have $P = 2P'$, we compute that $2a_4' = 9a_2^2 - a_4$. The expressions for a_8, a_{12}, and the discriminant Δ also simplify significantly, when written in terms of a_2, a_4', a_6':

$$a_8 = -3a_4'^2 + 2a_2 a_6',$$
$$a_{12} = 2a_4'^3 - 2a_2 a_4' a_6' + a_6'^2,$$
$$(67) \qquad \Delta = -16a_6'^2(-36a_2^2 a_4'^2 + 108a_4'^3 + 32a_2^3 a_6' - 108a_2 a_4' a_6' + 27a_6'^2).$$

Note that because of the factorization of Δ, the nondegeneracy condition that we require is now actually the nonvanishing of a degree $6 + 12 = 18$ invariant.

A little bit of algebra shows that the Jacobian is isomorphic to the elliptic curve

$$(68) \qquad E : y^2 + 2a_2xy + 2a_6'y = x^3 + (3a_4' - a_2^2)x^2$$

where the point P' is now at $(x, y) = (0, 0)$.

Proposition 6.15. *There is a choice of normalization for the relative invariants b_2, b_4, b_6 for the space of doubly symmetric hypercubes such that given a nondegenerate element of $V_1 \otimes V_2 \otimes Sym_2V_3$ corresponding to (C, L, P') as in Corollary 6.14, the Jacobian of C may be given in generalized Weierstrass form as*

$$(69) \qquad E : y^2 + b_2xy + b_6y = x^3 + b_4x^2$$

with the point P' being $(x, y) = (0, 0)$. Furthermore, the map from nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$-orbits of this representation to elliptic curves of the form (69), given by taking the Jacobian of the associated elliptic curve, is surjective.

6.3.2. Triply symmetric hypercubes. Next, we study the space of triply symmetric hypercubes. We may use the same methods as before to obtain a parametrization of the $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$-orbits of the space $V_1 \otimes \mathrm{Sym}_3 V_2 \subset V_1 \otimes V_2 \otimes V_2 \otimes V_2$, for 2-dimensional K-vector spaces V_1 and V_2. As K does not have characteristic 2 or 3 by assumption, this space is isomorphic to the quotient space $V_1 \otimes \mathrm{Sym}^3 V_2$, and it may also be thought of as pairs of binary cubic forms. The following is a basis-free version of Theorem 2.3:

Theorem 6.16. *Let V_1 and V_2 be 2-dimensional vector spaces over K. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$-orbits of $V_1 \otimes \mathrm{Sym}_3 V_2$ are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve over K, L is a degree 2 line bundle on C, and P is a nonzero 3-torsion point of $\mathrm{Jac}(C)(K)$.*

Proof. From a nondegenerate element of $V_1 \otimes \mathrm{Sym}_3 V_2 \subset V_1 \otimes V_2 \otimes V_2 \otimes V_2$, we obtain a genus one curve C and four line bundles L_1, L_2, L_3, L_4 such that $L_1 \otimes L_2 \cong L_3 \otimes L_4$, just as for the usual hypercube. For ease of exposition, we will sometimes refer to the second and third copies of V_2 as V_3 and V_4, respectively. The symmetry clearly indicates that L_3 and L_4 are isomorphic. While it is tempting to conclude that the symmetry also implies that L_2 is isomorphic to L_3 and L_4, recall that this cannot be so even in the usual

hypercube case! We instead have that the map from the curve C to $\mathbb{P}(V_1^\vee) \times \mathbb{P}(V_2^\vee) \times \mathbb{P}(V_3^\vee)$ is invariant under switching the latter two factors (where $V_2 = V_3$), so there must be an isomorphism $L_2 \otimes L_3 \cong L_1^{\otimes 2}$. Thus, combining these relations and setting $P := L_2 \otimes L_1^{-1}$ as a point on $\mathrm{Jac}(C)$, we have that $3P = 0$. Note that all 3-torsion points are in $\mathrm{Pic}^0(C)(K)$. Therefore, from a nondegenerate triply symmetric hypercube, we obtain a genus one curve, a degree 2 line bundle L_1, and a nonzero 3-torsion point in $\mathrm{Jac}(C)(K)$.

Conversely, given such a triple (C, L, P), we claim that we may construct a triply symmetric hypercube. We may define the line bundles $L_1 = L$, $L_2 = L \otimes P$ and $L_3 = L_4 = L \otimes P \otimes P$, and the usual construction produces a nondegenerate hypercube $\mathcal{A} \in V_1 \otimes V_2 \otimes V_3 \otimes V_4$ from (C, L_1, L_2, L_3, L_4), where $V_1 = H^0(C, L_1)$, $V_2 = H^0(C, L_2)$, $V_3 = H^0(C, L_3)$, and V_4 is dual to the kernel of the multiplication map μ_{123}. By the same argument as in Theorem 6.13, we may choose an appropriate identification of V_3 and V_4 such that $\mathcal{A}$ lies in $V_1 \otimes V_2 \otimes \mathrm{Sym}_2 V_3$; in other words, $\mathcal{A}$ is invariant under the transposition (34) acting on the indices of the vector spaces V_i for $i = 1$, 2, 3, 4.

In fact, we may identify V_2 and V_3 as well. Our $\mathcal{A}$ gives rise again to a genus one curve isomorphic to C, but we may choose different line bundles to reconstruct the hypercube. That is, by focusing on $C \hookrightarrow C_{14} \in \mathbb{P}(V_1^\vee) \times \mathbb{P}(V_4^\vee)$, we have line bundles L_1 and L_4, as before, which are the pullbacks of $\mathcal{O}_{\mathbb{P}(V_1^\vee)}(1)$ and $\mathcal{O}_{\mathbb{P}(V_4^\vee)}(1)$, respectively, to C_{14}. The pullbacks of $\mathcal{O}_{\mathbb{P}(V_2^\vee)}(1)$ and $\mathcal{O}_{\mathbb{P}(V_3^\vee)}(1)$ to C_{14} via ρ_{14}^{124} and ρ_{14}^{134}, respectively, are now both isomorphic to $L_1 \otimes P$. Using the multiplication map μ_{124} to reconstruct the same hypercube $\mathcal{A}$ gives a natural identification of V_2 and V_3 where the maps from C_{14} to $\mathbb{P}(V_2^\vee)$ and to $\mathbb{P}(V_3^\vee)$ are identical. Thus, we obtain an identification of V_2 and V_3 such that the hypercube $\mathcal{A}$ remains invariant under the transposition (23).

Therefore, because $\mathcal{A}$ is fixed under the transpositions (23) and (34), it is a triply symmetric hypercube in $V_1 \otimes \mathrm{Sym}_3 V_2$, as desired. $\qquad\square$

The $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariants for the space $V_1 \otimes \mathrm{Sym}_3 V_2$ form a polynomial ring, generated by two polynomials a_2 and a_6 of degrees 2 and 6, respectively. We may use our understanding of the invariant theory of normal hypercubes and of doubly symmetric hypercubes to explain these invariants geometrically. In particular, the two degree 4 invariants for hypercubes (and the one for doubly symmetric hypercubes) are now just $a_2^2/3$. Substituting this relation into (67) then gives that the Jacobian of the associated genus one curve C has discriminant

$$\Delta = 16(4a_2^3 - 27a_6)a_6^3.$$

Thus, the condition that a triply symmetric hypercube is nondegenerate is given by the nonvanishing of a polynomial of degree $6+6 = 12$. The Jacobian of C may also be written in the form

$$E : y^2 + 2a_2xy + 2a_6y = x^3,$$

where P is the 3-torsion point at $(x, y) = (0, 0)$.

Proposition 6.17. *There is a choice of normalization for the relative invariants b_2 and b_6 for the space of triply symmetric hypercubes such that given a nondegenerate element of $V_1 \otimes \mathrm{Sym}_3 V_2$ corresponding to (C, L, P) as in Theorem 6.16, the Jacobian of C may be given in generalized Weierstrass form as*

(70) $$E : y^2 + b_2xy + b_6y = x^3$$

with the 3-torsion point P being $(x, y) = (0, 0)$. Furthermore, the map from nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2)$-orbits of this representation to elliptic curves of the form (70), given by taking the Jacobian of the associated elliptic curve, is surjective.

6.3.3. Doubly doubly symmetric hypercubes, or bidegree $(2, 2)$ forms again. We now study the subrepresentation $\mathrm{Sym}_2 V_1 \otimes \mathrm{Sym}_2 V_2 \subset V_1 \otimes V_1 \otimes V_2 \otimes V_2$ of $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathbb{G}_m$, where V_1 and V_2 are 2-dimensional K-vector spaces. We call these doubly doubly symmetric hypercubes. Away from characteristic 2, this space is isomorphic to the representation $\mathrm{Sym}^2 V_1 \times \mathrm{Sym}^2 V_2$ of bidegree $(2, 2)$ forms, which we examined in §6.1 with a different interpretation.

Theorem 6.18. *Let V_1 and V_2 be 2-dimensional vector spaces over K. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathbb{G}_m$-orbits of $\mathrm{Sym}_2 V_1 \times \mathrm{Sym}_2 V_2$ are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve over K, L is a degree 2 line bundle on C, and P is a nonzero non-2-torsion point on $\mathrm{Jac}(C)(K)$.*

This statement is a basis-free version of Theorem 2.5. Note that the moduli problem for doubly doubly symmetric hypercubes is identical to that for doubly symmetric hypercubes!

Proof. Starting from an element of $\mathrm{Sym}_2 V_1 \otimes \mathrm{Sym}_2 V_2 \subset V_1 \otimes V_1 \otimes \mathrm{Sym}_2 V_2$, Corollary 6.14 gives the triple (C, L, P) as desired.

Conversely, given such (C, L, P), recall from the proof of Theorem 6.13 that we may construct a hypercube $\mathcal{A} \in U_1 \otimes U_2 \otimes \mathrm{Sym}_2\, U_3$, where $U_i :=$ $H^0(C, L_i)$ for

$$L_1 := L \qquad\qquad L_2 := L \otimes P \otimes P \qquad\qquad L_3 := L \otimes P.$$

From this hypercube $\mathcal{A}$, we may create the usual curves C_{ijk} in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$; for example, we have $C_{123} \subset \mathbb{P}(U_1^\vee) \times \mathbb{P}(U_2^\vee) \times \mathbb{P}(U_3^\vee)$ with L_i the pullback of $\mathcal{O}_{\mathbb{P}(U_i^\vee)}(1)$ to C_{123}. Under the composition

$$C_{123} \to C_{13} \to C_{134} \to C_{34} \to C_{234} \to \mathbb{P}(U_2^\vee),$$

the line bundle $\mathcal{O}_{\mathbb{P}(U_2^\vee)}(1)$ pulled back to C_{123} is isomorphic to L_1 (using the relations of the form in Lemma 6.6). In particular, this gives a natural identification of the vector spaces $U_1 = H^0(C, L_1)$ with U_2! Moreover, the two maps

$$\pi^1_{134} \circ \rho^{134}_{34} : C_{34} \to C_{134} \to \mathbb{P}(U_1^\vee)$$

$$\pi^2_{234} \circ \rho^{234}_{34} : C_{34} \to C_{234} \to \mathbb{P}(U_2^\vee)$$

are the same after the identification of U_1 and U_2. Therefore, there exists a choice of basis for U_1 and for U_2 such that $\mathcal{A}$ is actually invariant when switching the first and second factor; in other words, it is in the orbit of an element in $\mathrm{Sym}_2\, U_1 \otimes \mathrm{Sym}_2\, U_3$. $\qquad\square$

There also exists a straightforward computational proof, by exhibiting a linear transformation in $\mathrm{GL}(V_1)$ taking an element of $V_1 \otimes V_1 \otimes \mathrm{Sym}_2\, V_2$ to an element of $\mathrm{Sym}_2\, V_1 \otimes \mathrm{Sym}_2\, V_2$. This linear transformation has entries that are degree 3 in the coefficients of the original element; its determinant is nonzero for nondegenerate doubly symmetric hypercubes, as it is exactly the degree 6 invariant a'_6 from §6.3.1, which appears as a factor of the discriminant for doubly symmetric hypercubes. If we choose bases $\{u_1, u_2\}$ and $\{v_1, v_2\}$ for V_1 and V_2, respectively, we may represent a doubly symmetric hypercube as

$$(71) \qquad\qquad \sum_{i,j=1}^{2} (r_{ij} v_1^2 + s_{ij} v_1 v_2 + t_{ij} v_2^2) u_i u_j.$$

Then the linear transformation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(V_1)$ with

$$a = -r_{22}s_{21}t_{11} + r_{21}s_{22}t_{11} + r_{22}s_{11}t_{21} - r_{11}s_{22}t_{21} - r_{21}s_{11}t_{22} + r_{11}s_{21}t_{22}$$
$$b = -r_{21}s_{12}t_{11} + r_{12}s_{21}t_{11} + r_{21}s_{11}t_{12} - r_{11}s_{21}t_{12} - r_{12}s_{11}t_{21} + r_{11}s_{12}t_{21}$$
$$c = -r_{22}s_{21}t_{12} + r_{21}s_{22}t_{12} + r_{22}s_{12}t_{21} - r_{12}s_{22}t_{21} - r_{21}s_{12}t_{22} + r_{12}s_{21}t_{22}$$
$$d = -r_{22}s_{12}t_{11} + r_{12}s_{22}t_{11} + r_{22}s_{11}t_{12} - r_{11}s_{22}t_{12} - r_{12}s_{11}t_{22} + r_{11}s_{12}t_{22}$$

will send the doubly symmetric hypercube (71) to a doubly doubly symmetric hypercube.

Note that this moduli interpretation for the orbits is very similar to the one in Corollary 6.3. However, the curve X obtained in that corollary (and the previous Theorem 6.2) has discriminant of degree 12. The curve C here, from Theorem 6.18, has discriminant of degree 24, so they are clearly not the same — but they are closely related. In particular, the curve C is the (generalized) Hessian of the curve X! Here, we define the *Hessian* of a bidegree $(2,2)$ form $f(w_1, w_2, x_1, x_2)$ in $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$ (and by abuse of terminology, the Hessian of the corresponding curve) as the curve cut out by the determinant of the matrix

$$\left(\frac{\partial^2 f}{\partial w_i \partial x_j} \right)_{1 \leq i, j \leq 2}$$

which is also a bidegree $(2,2)$ form on $\mathrm{Sym}^2 V_1 \otimes \mathrm{Sym}^2 V_2$. It is a small computation to check that the genus one curve C is the Hessian of X.

The $\mathrm{SL}(V_1) \times \mathrm{SL}(V_2)$-invariant ring of $\mathrm{Sym}_2 V_1 \times \mathrm{Sym}_2 V_2$ is generated by three invariants δ_2, δ_3, δ_4 of degrees 2, 3, and 4, respectively, as we know from §6.1.2. We may apply our understanding of the invariants in the doubly symmetric hypercube case; in particular, we find that

$$\delta_2 = -\frac{8}{3}a_2, \qquad \delta_3^2 = \frac{4}{27}a_6', \qquad \delta_4 = \frac{64}{9}a_2^2 - 16a_4',$$

where a_2, a_4', and a_6' are the polynomials from §6.3.1. We can substitute these formulas into (68) to obtain a formula for the Jacobian of the curve C arising from an element f of $\mathrm{Sym}_2 V_1 \otimes \mathrm{Sym}_2 V_2$ via Theorem 6.18. Thus, there are rational generators b_2, b_3, b_4 for the invariants such that $\mathrm{Jac}(C)$ may be written in generalized Weierstrass form as

$$(72) \qquad\qquad y^2 + b_2 xy + 6b_3^2 y = x^3 + b_4 x^2,$$

and the point P is at $(x, y) = (0, 0)$. The discriminant of the Jacobian of C factors as a rational multiple of

$$\delta_3^4(-64a_2^2a_4'^2 + 192a_4'^3 + 384a_2^3\delta_3^2 - 1296a_2a_4'\delta_3^2 + 2187\delta_3^4),$$

where the second factor (up to a scalar) is the discriminant of the Jacobian of the genus one curve X cut out by f directly.

A priori, it may not be obvious that any elliptic curve over K with a nonzero non-2-torsion point can be expressed in the form (72). To see this, recall that any such curve can be expressed in the form

$$y^2 + axy + by = x^3 + cx^2$$

where the discriminant is nonzero (and thus $b \neq 0$). We then note that the latter elliptic curve is actually isomorphic to one of the form (72) by taking $b_2 = 6a/b$, $b_4 = 6/b$, and $b_6 = 36c/b^2$.

6.3.4. Quadruply symmetric hypercubes, or binary quartic forms again. The last symmetrization that we study is the case of fully symmetric hypercubes, i.e., elements of $\mathrm{Sym}_4(V) \subset V^{\otimes 4}$ for a 2-dimensional K-vector space V. Since our field K is not of characteristic 2 or 3, this space is isomorphic to the quotient space $\mathrm{Sym}^4 V$ of binary quartic forms. Here, we take the standard $\mathrm{GL}(V)$-action on $\mathrm{Sym}_4(V)$, along with a standard $\mathbb{G}_m$-action by scaling, which is slightly different than the action considered on binary quartic forms in §4.1. The following is a basis-free version of Theorem 2.2:

Theorem 6.19. *For a 2-dimensional K-vector space V, the nondegenerate $\mathrm{GL}(V) \times \mathbb{G}_m$-orbits of $\mathrm{Sym}_4(V)$ are in bijection with isomorphism classes of triples (C, L, P), where C is a genus one curve over K, L is a degree 2 line bundle on C, and P is a nonzero 3-torsion point of $\mathrm{Jac}(C)(K)$.*

This moduli problem is identical to that of triply symmetric hypercubes!

Proof. Given an element of $\mathrm{Sym}_4(V) \subset V \otimes \mathrm{Sym}_3 V$, we may apply Theorem 6.16 to obtain a genus one curve C with a degree 2 line bundle L and a nonzero 3-torsion point P of $\mathrm{Jac}(C)(K)$.

Conversely, given such a triple (C, L, P), we may use Theorem 6.16 to construct a hypercube $\mathcal{A}$ in $U_1 \otimes U_2 \otimes U_3 \otimes U_4$, where $U_1 = H^0(C, L)$ and $U_2 = H^0(C, L \otimes P)$ has a natural identification with U_3 and U_4 such that $\mathcal{A}$ is invariant under permutations of U_2, U_3, and U_4. An almost identical argument to the one in Theorem 6.18 shows that we may in fact identify

U_1 with U_2 and that $\mathcal{A}$ is invariant under switching U_1 and U_2. In other words, the hypercube $\mathcal{A}$ coming from (C, L, P) is in the orbit of a quadruply symmetric hypercube. $\qquad\square$

A simple computational proof, just as for Theorem 6.18, is also possible; we only need to specify an element of $\mathrm{GL}(V)$ that acts on a given nondegenerate element of $V \otimes \mathrm{Sym}_3(V)$ (via the first factor only) to produce an element of $\mathrm{Sym}_4(V)$. With a choice of basis $\{v_1, v_2\}$ for V, we may represent an element of $V \otimes \mathrm{Sym}_3 V$ as

$$(73) \qquad \sum_{i=1}^{2} v_i \otimes (r_i v_1^3 + s_i v_1^2 v_2 + t_i v_1 v_2^2 + u_i v_2^3).$$

Then applying the linear transformation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(V)$, with

$$a = -s_2^2 t_1 + s_1 s_2 t_2 + r_2 t_1 t_2 - r_1 t_2^2 - r_2 s_1 u_2 + r_1 s_2 u_2$$
$$b = s_1 s_2 t_1 - r_2 t_1^2 - s_1^2 t_2 + r_1 t_1 t_2 + r_2 s_1 u_1 - r_1 s_2 u_1$$
$$c = s_2 t_1 t_2 - s_1 t_2^2 - s_2^2 u_1 + r_2 t_2 u_1 + s_1 s_2 u_2 - r_2 t_1 u_2$$
$$d = -s_2 t_1^2 + s_1 t_1 t_2 + s_1 s_2 u_1 - r_1 t_2 u_1 - s_1^2 u_2 + r_1 t_1 u_2,$$

to the first factor of V, gives a quadruply symmetric hypercube. The determinant of this transformation is just the degree 6 invariant a_6 for triply symmetric hypercubes (from §6.3.2), and since it is a factor of the discriminant, it is nonzero for nondegenerate hypercubes.

Just as for the triply symmetric Rubik's cubes and the doubly doubly symmetric hypercubes, this parametrization of binary quartic forms is related to the other "dual" parametrization for the same space, namely the one described in §4.1. In Theorem 4.1, the genus one curve X arising from a binary quartic form has discriminant of degree 6. Here, in Theorem 6.19, we produce a genus one curve C whose discriminant has degree 24. But these two curves X and C are again related by the Hessian construction, i.e., C is the Hessian of X! More precisely, let $q(w_1, w_2)$ be a binary quartic form in $\mathrm{Sym}^4 V$. Then the *Hessian* of q (or of the genus one curve X given as $y^2 = q(w_1, w_2)$) is the binary quartic

$$H(q)(w_1, w_2) := \mathrm{disc}\left(\frac{\partial^3 q}{\partial w_i \partial w_j \partial w_k} \right)_{1 \le i, j, k \le 2},$$

i.e., the discriminant of the three-dimensional matrix of triple derivatives. (Recall from §2.1 that the discriminant is the unique polynomial invariant

of a $2 \times 2 \times 2$ cube.) By abuse of terminology, we also say that the genus one curve C associated to $H(q)$ is the Hessian of q and of X. This curve C is the one obtained from Theorem 6.19. In particular, we obtain a proof of the following:

Corollary 6.20. *Given a binary quartic form q of $\mathrm{Sym}^4 V$, where V is a 2-dimensional K-vector space, let $H(q)$ denote the Hessian binary quartic form. Then the Jacobian of the genus one curve given by the equation $y^2 = H(q)$ has a nonzero 3-torsion point defined over K.*

Recall from §4.1 that the $\mathrm{SL}(V)$-invariants of $\mathrm{Sym}^4 V$ are generated by two invariants I and J of degrees 2 and 3, respectively. These invariants appear in the coefficients for the Jacobian of the curve C arising from an element $\mathcal{A} \in \mathrm{Sym}_4(V)$ via Theorem 6.19. In particular, because the space $\mathrm{Sym}_4(V)$ is contained in both $V \otimes \mathrm{Sym}_3 V$ and $\mathrm{Sym}_2 V \otimes \mathrm{Sym}_2 V$, we may use the geometric interpretations of the invariants of triply symmetric hypercubes and of doubly doubly symmetric hypercubes to easily understand the invariants in this case! The Jacobian of C is isomorphic to

(74) $$E : y^2 + 2a_2 xy + 216 a_3^2 y = x^3,$$

where a_2 is defined as for hypercubes and a_3 is the primitive integral degree 3 invariant generator. In terms of the invariants I and J, because $\mathcal{A}$ viewed as a binary quartic form has coefficients with factors of 4 and 6, the polynomials $I(\mathcal{A})$ and $J(\mathcal{A})$ are not primitive: $I(\mathcal{A}) = -4a_2$ and $J(\mathcal{A}) = -432 a_3$. The discriminant of the Jacobian (74) factors as a rational multiple of

$$a_3^6 (a_2^3 + 729 a_3^2),$$

and the latter factor is just the discriminant of the Jacobian of Z (or of $\mathcal{A}$ as a binary quartic form).

Finally, just as before, we observe that any elliptic curve over K with a nonzero 3-torsion point defined over K can be expressed in the form (74). Namely, if we have an elliptic curve of the form $y^2 + axy + by = x^3$ with nonzero discriminant (implying $b \neq 0$), then setting $a_2 = 108a/b$ and $a_3 = 216/b$ gives an isomorphic elliptic curve of the form (74).

6.4. Hermitian cubes

In this section, we discuss spaces $\mathscr{C}$, sometimes called "Freudenthal algebras," or "Freudenthal triple systems," that have a quartic norm form, originally introduced in [Fre]. These vector spaces are related to the space of

$2 \times 2 \times 2$ cubes—that is, the tensor space $V_1 \otimes V_2 \otimes V_3$ where V_i is a two-dimensional vector space over K—in the same way that the spaces of Hermitian matrices over composition algebras are related to the usual matrix algebras. Our goal here, then, is to "triply Hermitianize" the space of $2 \times 2 \times 2$ cubes with respect to a cubic algebra.

The natural cubic algebras to use are cubic Jordan algebras J. In fact, this process works for any cubic Jordan algebra with a nondegenerate trace form (see §5.3.1 for general constructions of such cubic Jordan algebras). Some of the properties and formulas we use below for Hermitian cubes are explained in more detail in [Kru07] and also rely on ideas from [Fau72, Cle03].

Analogously to §5.3, we describe spaces $\mathscr{C}$ of Hermitian $2 \times 2 \times 2$ cubical matrices and their properties, including a norm form, a trace form, an adjoint map, and a notion of rank. We then are interested in the rank one loci of such spaces and their moduli descriptions. We use such moduli interpretations to obtain vector bundles on varieties mapping to these rank one loci. This allows us in §6.5 to uniformly study representations of the form $V \otimes \mathscr{C}$, where V is a K-vector space of dimension 2, in terms of genus one curves.

6.4.1. Definitions and invariants.

Definition 6.21. A *Hermitian cube space* $\mathscr{C}(J)$ over a cubic Jordan algebra J is the K-vector space of quadruples (a, b, c, d), where $a, d \in K$ and $b, c \in J$. We call elements of $\mathscr{C}(J)$ *Hermitian cubes*.

The reason for the name is that we may think of elements of $\mathscr{C}(J)$ as "cubes" of the form
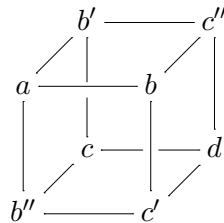
where b' and b'' (respectively, c' and c'') are thought of as formal conjugates of b (resp., c) in isomorphic copies of J. (This viewpoint makes Hermitian cubes analogous to the Hermitian matrices discussed in §5.3.2.) In some cases, the other copies of J may naturally be viewed as embedded in a larger algebra, e.g., if J is a cubic field over K, then the other isomorphic copies may be thought of as the Galois conjugate fields as subfields of the Galois closure of J over K, and b', b'' are the usual Galois conjugates of b.

If J has dimension d over K, then $\mathscr{C}(J)$ is a K-vector space of dimension $2d+2$. Although there is a very weak algebra structure on $\mathscr{C}(J)$, we will not use it in the sequel. We will only use the structure of $\mathscr{C}(J)$ as a representation of a certain reductive group $G_{\mathscr{C}(J)}$, which will be a prehomogeneous vector space with a relative invariant of degree 4. This invariant will be the *norm form* for Hermitian cubes.

Recall that a cubic Jordan algebra J comes equipped with a trace form Tr and a cubic norm form N, as well as their (bi)linearizations (see equation (44) in §5.3.1). We restrict our attention to cubic Jordan algebras for which the trace form Tr is nondegenerate, in which case we obtain a natural adjoint map $\sharp$, as in equation (50). We use these properties of J to construct a *trace form* $\mathrm{Tr}_{\mathscr{C}(J)}$ and quartic norm form $\mathrm{N}_{\mathscr{C}(J)}$ for $\mathscr{C}(J)$, given the basepoint $\varepsilon := (1, 0, 0, 1)$.

For the cubic Jordan algebra of 3×3 Hermitian matrices over a composition algebra A, the cubic norm form is a generalization of the determinant of the matrix; here, we analogously generalize the quartic discriminant of a $2 \times 2 \times 2$ cube, which is the generator of the ring of SL_2^3-invariants for $2 \times 2 \times 2$ cubes.

Definition 6.22. The *discriminant* of a Hermitian cube $A = (a, b, c, d)$ is given by

$$(75) \qquad \mathrm{disc}(A) = (ad - \mathrm{Tr}(b, c))^2 - 4\,\mathrm{Tr}(b^\sharp, c^\sharp) + 4a\,\mathrm{N}(c) + 4d\,\mathrm{N}(b).$$

The *norm form* $\mathrm{N}_{\mathscr{C}(J)}$ is the complete linearization of the discriminant form, so it is a symmetric quadrilinear map

$$\mathrm{N}_{\mathscr{C}(J)} : \mathscr{C}(J) \times \mathscr{C}(J) \times \mathscr{C}(J) \times \mathscr{C}(J) \longrightarrow K$$

with $\mathrm{N}_{\mathscr{C}(J)}(A, A, A, A) = \mathrm{disc}(A)$. The linear *trace form* $\mathrm{Tr}_{\mathscr{C}(J)}$ is defined as

$$\mathrm{Tr}_{\mathscr{C}(J)}(A) := \mathrm{N}_{\mathscr{C}(J)}(A, \varepsilon, \varepsilon, \varepsilon)$$

and there is an alternating bilinear trace form

$$\langle A, A' \rangle = ad' - \mathrm{Tr}(b, c') + \mathrm{Tr}(b', c) - a'd.$$

Since the trace form Tr for the Jordan algebra J is nondegenerate, and hence the bilinear trace form $\langle \cdot, \cdot \rangle$ is nondegenerate, the space $\mathscr{C}(J)$ is self-dual. There is a natural cubic "adjoint" map $\flat$ associated to $\mathscr{C}(J)$:

$$(76) \qquad \flat : \quad \mathscr{C}(J) \longrightarrow \mathscr{C}(J)^\vee \overset{\cong}{\longrightarrow} \mathscr{C}(J)$$
$$A \longmapsto \mathrm{N}_{\mathscr{C}(J)}(A, A, A, \cdot) \longmapsto A^\flat.$$

This map is the analogue of the adjoint map $\sharp$ for cubic Jordan algebras (defined in equation (50)) and satisfies the properties

$$(77) \qquad \mathrm{N}_{\mathscr{C}(J)}(A, A, A, B) = \langle A^\flat, B \rangle \quad \text{and} \quad (A^\flat)^\flat = -\operatorname{disc}(A)^2 A.$$

Explicitly, for a Hermitian cube $A = (a, b, c, d)$, the adjoint $A^\flat = (a^\flat, b^\flat, c^\flat, d^\flat)$ is given by the formulas

$$
(78) \qquad
\begin{aligned}
a^\flat &= a^2 d - a \operatorname{Tr}(b, c) + 2 \operatorname{N}(b) \\
b^\flat &= 2c \times b^\sharp - 2ac^\sharp + (ad - \operatorname{Tr}(b, c))b \\
c^\flat &= -2b \times c^\sharp + 2db^\sharp - (ad - \operatorname{Tr}(b, c))c \\
d^\flat &= -ad^2 + d \operatorname{Tr}(b, c) - 2 \operatorname{N}(c)
\end{aligned}
$$

where $\times$ denotes the bilinearization of $\sharp$ defined in (48). As in the cubic case, by an abuse of notation, the map $\flat$ will sometimes just refer to the first map in (76) from $\mathscr{C}(J)$ to $\mathscr{C}(J)^\vee$.

Example 6.23. If J is the field K itself with cubic norm form $\operatorname{N}(x) = x^3$ for $x \in K$, the space $\mathscr{C}(J)$ is isomorphic to $\operatorname{Sym}^3 K^2$, and the discriminant of a $A = (a, b, c, d)$ is the usual quartic discriminant of a binary cubic form in $\operatorname{Sym}^3 K^2$. That is, if $A = (a, b, c, d)$ represents the binary cubic $aX^3 + 3bX^2Y + 3cXY^2 + dY^3$, then

$$\operatorname{disc}(A) = a^2 d^2 - 3b^2 c^2 - 6abcd + 4ac^3 + 4b^3 d$$

and the adjoint is the binary cubic form covariant given by the determinant of the Jacobian matrix of the cubic and its Hessian, namely

$$A^\flat = (2b^3 - 3abc + a^2 d, b^2 c - 2ac^2 + abd, -bc^2 + 2b^2 d - acd, -2c^3 + 3bcd - ad^2).$$

Example 6.24. If J is the split algebra $K \times K \times K$ with norm form $\operatorname{N}((x_1, x_2, x_3)) = x_1 x_2 x_3$, then $\mathscr{C}(J)$ is isomorphic to $K^2 \otimes K^2 \otimes K^2$, or the space of $2 \times 2 \times 2$ cubes, and the discriminant of the Hermitian cube $A = (a, (b_1, b_2, b_3), (c_1, c_2, c_3), d)$ is the usual quartic discriminant of a $2 \times 2 \times 2$ cube (see [Bha04a, §2.1]):

$$
\begin{aligned}
\operatorname{disc}(A) = {}& a^2 d^2 + b_1^2 c_1^2 + b_2^2 c_2^2 + b_3^2 c_3^2 + 4(ac_1 c_2 c_3 + b_1 b_2 b_3 d) \\
& - 2(ab_1 c_1 d + ab_2 c_2 d + ab_3 c_3 d + b_1 b_2 c_1 c_2 + b_1 b_3 c_1 c_3 + b_2 b_3 c_2 c_3).
\end{aligned}
$$

The adjoint $A^\flat := (a^\flat, (b_1^\flat, b_2^\flat, b_3^\flat), (c_1^\flat, c_2^\flat, c_3^\flat), d^\flat)$ is easy to compute, with coordinates

$$a^\flat = 2b_1b_2b_3 - a(b_1c_1 + b_2c_2 + b_3c_3) + a^2d$$
$$d^\flat = -2c_1c_2c_3 + d(b_1c_1 + b_2c_2 + b_3c_3) - ad^2$$
$$b_i^\flat = (-b_ic_i + b_jc_j + b_kc_k)b_i - 2ac_jc_k + adb_i$$
$$c_i^\flat = -(-b_ic_i + b_jc_j + b_kc_k)c_i + 2db_jb_k - adc_i$$

where $\{i, j, k\} = \{1, 2, 3\}$.

6.4.2. Rank and linear transformations. We may also define an analogue of rank for Hermitian cube spaces that agrees with the natural notion of rank for a tensor space in the simplest cases.

Definition 6.25. A nonzero Hermitian cube $A \in \mathscr{C}(J)$ has *rank one* if it is a scalar multiple of a Hermitian cube of the form

$$(79) \qquad (a, b, c, d) = (\mathrm{N}(\alpha), \alpha^\sharp \bullet \beta, \beta^\sharp \bullet \alpha, \mathrm{N}(\beta))$$

for any $\alpha, \beta \in J$. A Hermitian cube $A \in \mathscr{C}(J)$ has *rank* ≤ 2 if its adjoint $A^\flat$ is 0. It has *rank* ≤ 3 if its discriminant $\mathrm{disc}(A)$ is 0, and A has *rank four* if its discriminant is nonzero. Finally, a Hermitian cube A has *rank zero* if $A = (0, 0, 0, 0)$.

Note that the condition on scalar multiples for rank one cubes is necessary: if $k \in K$ is not in the image of the map N, then $(k, 0, 0, 0)$ is not of the form in (79), but intuitively we would still like this cube to have rank one. With this definition, the rank one (and zero) cubes are, up to K-scaling, given by elements of J^2. More precisely, there is a map

$$J \oplus J \longrightarrow \mathscr{C}(J)$$
$$(\alpha, \beta) \longmapsto (\mathrm{N}(\alpha), \alpha^\sharp \bullet \beta, \beta^\sharp \bullet \alpha, \mathrm{N}(\beta))$$

that descends to a rational map

$$(80) \qquad \tau : \mathbb{P}(J \oplus J) \dashrightarrow \mathbb{P}(\mathscr{C}(J))$$

where $\mathbb{P}(J \oplus J)$ and $\mathbb{P}(\mathscr{C}(J))$ denotes K-lines in the K-vector spaces $J \oplus J$ and $\mathscr{C}(J)$, respectively. Let $X_{\mathscr{C}(J)}$ denote the image of the map τ. Intuitively, the variety $X_{\mathscr{C}(J)}$ is like the projective line over J, with τ being analogous to the embedding of the twisted cubic. (This comparison is not entirely

accurate, of course, since scaling (α, β) by elements of J does not usually fix its image under τ.)

Let $\mathrm{SL}_2(J)$ denote the group of discriminant-preserving K-linear transformations of the space $\mathscr{C}(J)$ (this group is denoted by $\mathrm{Inv}(\mathscr{C}(J))$ in [Kru07]). Some examples include

J	$\mathscr{C}(J)$	$\mathrm{SL}_2(J)$
K	$\mathrm{Sym}^3(2)$	$\mathrm{SL}_2(K)$
K^3	$2 \otimes 2 \otimes 2$	$\mathrm{SL}_2(K)^3$
$\mathscr{H}_3(K)$	$\wedge_0^3(6)$	$\mathrm{Sp}_6(K)$
$\mathscr{H}_3(K \times K)$	$\wedge^3(6)$	$\mathrm{SL}_6(K)$
$\mathscr{H}_3(\mathscr{Q})$	$S^+(32)$	Spin_{12}
$\mathscr{H}_3(\mathscr{O})$	56	E_7

where the last two may also range over different quaternion and octonion algebras over K (and thus are associated with different forms of the corresponding groups).

Thus, the space $\mathscr{C}(J)$ may be thought of as a representation of $\mathrm{SL}_2(J)$. In fact, the variety $X_{\mathscr{C}(J)}$ is the projectivization of the orbit of the highest weight vector of the representation of $\mathrm{SL}_2(J)$ on $\mathscr{C}(J)$, and is isomorphic to the homogeneous space given by this representation! That is, the variety $X_{\mathscr{C}(J)}$ is isomorphic to $\mathrm{SL}_2(J)/P_{\mathscr{C}(J)}$, where $P_{\mathscr{C}(J)}$ is the parabolic subgroup associated to the representation $\mathscr{C}(J)$, and it has a moduli interpretation as a flag variety.

In fact, the rank of all the elements of $\mathscr{C}(J)$ is preserved under the action of $\mathrm{SL}_2(J)$, and over an algebraically closed field, the group $\mathrm{SL}_2(J)$ acts transitively on the set of rank r elements [Kru07, Lemma 21 & Thm 2]. In other words, the space $\mathscr{C}(J)$ is stratified by rank into orbits of $\mathrm{SL}_2(J)$ when K is algebraically closed. Thus, for many computations related to elements in $\mathscr{C}(J)$, they may just be checked on representatives of $\mathscr{C}(J)$ of the appropriate rank; see, e.g., [Kru07, eqs. (58)-(61)] for some simple choices of representatives.[6]

In the case where J is the $\mathscr{H}_3(\mathbb{C} \times \mathbb{C})$ and $X_{\mathscr{C}(J)}$ is the Grassmannian $\mathrm{Gr}(3,6)$, these varieties and some of the geometric constructions in the sequel are studied in Donagi's work [Don77].

Furthermore, in each of the cases in the above table over an algebraically closed field, the secant variety of $X_{\mathscr{C}(J)}$ is the entire space $\mathbb{P}(\mathscr{C}(J))$, and the tangent variety of $X_{\mathscr{C}(J)}$ is the quartic hypersurface $Y_{\mathscr{C}(J)}$ given by the vanishing of the discriminant [Zak93, Chap. III]; that is, $Y_{\mathscr{C}(J)}$ is made up

---

[6]For example, the definition of "rank one" cubes in [Kru07] differs from Definition 6.25, but it is easy to check that they are equivalent by this method.

of the rank ≤ 3 elements of $\mathscr{C}(J)$ (up to K-scaling). In fact, Zak shows (and it is easy to check on representatives of the appropriate ranks):

Lemma 6.26. *Each general point of $\mathbb{P}(\mathscr{C}(J)) \setminus Y_{\mathscr{C}(J)}$ lies on exactly one secant line of $X_{\mathscr{C}(J)}$. Each point of $Y_{\mathscr{C}(J)} \setminus X_{\mathscr{C}(J)}$ lies on exactly one tangent line of $X_{\mathscr{C}(J)}$.*

Therefore, we find that the adjoint map $\flat$ induces a birational map

$$\beta_J : \mathbb{P}(\mathscr{C}(J)) \dashrightarrow \mathbb{P}(\mathscr{C}(J))$$

whose reduced base locus is the variety $X_{\mathscr{C}(J)}$. Under β_J, the quartic hypersurface $Y_{\mathscr{C}(J)}$ is blown down to $X_{\mathscr{C}(J)}$, as the adjoint of rank ≤ 3 elements in $\mathscr{C}(J)$ have rank ≤ 1. By (77), applying β_J twice is the identity away from $Y_{\mathscr{C}(J)}$.

Furthermore, the adjoint map β_J preserves each secant line. This is easy to check by computation, e.g., by showing that the adjoint of the sum of two rank one cubes is in their span. For example, the adjoint of the sum of $A = (1, 0, 0, 0)$ and $B = (\mathrm{N}(\alpha), \alpha^\sharp \bullet \beta, \beta^\sharp \bullet \alpha, \mathrm{N}(\beta))$ is $\mathrm{N}(\beta)A - \mathrm{N}(\beta)B$.

6.5. Triply Hermitian hypercubes

As in §5.4, we would like to study the orbits of a class of "Hermitianized" representations uniformly. Namely, for V a two-dimensional K-vector space and J a cubic Jordan algebra, we study the representation of $\mathrm{GL}(V) \times \mathrm{SL}_2(J)$-orbits on $V \otimes \mathscr{C}(J)$. We find that the orbits correspond to isomorphism classes of genus one curves with degree 2 line bundles, along with bundles related to $X_{\mathscr{C}(J)}$. We consider only nondegenerate elements of the tensor space, which will correspond to smooth curves.

Definition 6.27. An element $\phi \in V \otimes \mathscr{C}(J)$ is called *nondegenerate* if the induced composition map

$$\flat \circ \phi : V^\vee \to \mathscr{C}(J) \to \mathscr{C}(J)^\vee$$

is injective. Note that nondegeneracy implies that the elements in the image of ϕ do not have rank one, and the discriminant of all but four points (over $\overline{K}$, up to multiplicity) in the image of ϕ is nonzero.

The following theorem—a more precise version of Theorem 2.8—states that the orbits of such nondegenerate elements of $V \otimes \mathscr{C}(J)$ are in correspondence with genus one curves with certain vector bundles:

Theorem 6.28. *The nondegenerate* $\mathrm{GL}_2(K) \times \mathrm{SL}_2(J)$*-orbits of* $V \otimes \mathscr{C}(J)$ *are in bijection with isomorphism classes of nondegenerate quadruples* $(C, L, \mathcal{F}, \kappa)$, *where* C *is a genus one curve over* K; L *is a degree* 2 *line bundle on* C; $\mathcal{F} = (E_i)$ *is the flag of vector bundles* E_i *given by pulling back the universal flag via the map* $\kappa : C \to X_{\mathscr{C}(J)}$; *and* $\kappa^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1) \cong L^{\otimes 3}$.

As in §5.4, we will discuss the nondegeneracy condition on quadruples $(C, L, \mathcal{F}, \kappa)$ in the proof. It is again an open condition, so the statement of the theorem may be rephrased as giving a bijection between orbits of $V \otimes \mathscr{C}(J)$ and the K-points of an open substack of the moduli space of $(C, L, \mathcal{F}, \kappa)$ (with the isomorphism from $\kappa^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1)$ to $L^{\otimes 3}$). Again, in many cases, this nondegeneracy condition will be a simple condition on the bundles.

The rest of this subsection contains the proof of Theorem 6.28. First, from a nondegenerate element ϕ in $V \otimes \mathscr{C}(J)$, we explain how to naturally construct the genus one curve and associated data described in Theorem 6.28. The construction will be invariant under the group action. Although many features of this construction are similar to the one described in §5.4, here the curve will not necessarily be immersed in $\mathbb{P}(\mathscr{C}(J))$ but instead have a degree 2 map to a line in $\mathbb{P}(\mathscr{C}(J))$. In addition, the adjoint map plays a different role here and is not logically necessary for describing the genus one curve and other geometric data from the multilinear object. For the remainder of this subsection, we fix the cubic Jordan algebra J and set $X := X_{\mathscr{C}(J)}$ and $Y := Y_{\mathscr{C}(J)}$.

We will work with the Hilbert scheme $\mathcal{H}\mathrm{ilb}_2(X)$ of two points on X. Let $\zeta : \mathcal{Z}^{\mathrm{univ}} \to \mathcal{H}\mathrm{ilb}_2(X)$ denote the universal degree 2 subscheme over $\mathcal{H}\mathrm{ilb}_2(X)$, so there is also a natural map $\epsilon : \mathcal{Z}^{\mathrm{univ}} \to X$. Let $\mathcal{L}^{\mathrm{univ}}$ denote the universal line over $\mathcal{H}\mathrm{ilb}_2(X)$ pulled back from the universal line over the Hilbert scheme $\mathcal{H}\mathrm{ilb}_2(\mathbb{P}(\mathscr{C}(J)))$ of two points in $\mathbb{P}(\mathscr{C}(J))$. That is, to a zero-dimensional degree 2 subscheme in $X \subset \mathbb{P}(\mathscr{C}(J))$, we associate the unique line passing through it; a nonreduced subscheme gives a point and a tangent direction, and thus also a unique line. We then have the diagram

$$(81) \qquad \mathcal{Z}^{\mathrm{univ}} \stackrel{\iota}{\hookrightarrow} \mathcal{L}^{\mathrm{univ}} \stackrel{b}{\longrightarrow} \mathbb{P}(\mathscr{C}(J))$$

with maps ζ down-left and the $\mathbb{P}^1$-bundle down to $\mathcal{H}\mathrm{ilb}_2(X)$.

where the map b on the right comes from the construction of $\mathcal{L}^{\mathrm{univ}}$. A straightforward computation (e.g., as found in [Ver09, §2.1]) gives

$$(82) \qquad \mathcal{L}^{\mathrm{univ}} \cong \mathbb{P}(\zeta_* \epsilon^* \mathcal{O}_X(1)),$$

where $\mathcal{O}_X(1)$ denotes the pullback of $\mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1)$ to $X \subset \mathbb{P}(\mathscr{C}(J))$.

We first give the construction of a genus one curve and the appropriate bundles from an orbit of $V \otimes \mathscr{C}(J)$.

Construction 6.29. Given $\phi \in V \otimes \mathscr{C}(J)$, we view ϕ as a linear map in $\mathrm{Hom}(V^\vee, \mathscr{C}(J))$. Nondegeneracy implies that there is a map

$$\mathbb{P}(\phi) : \mathbb{P}(V^\vee) \longrightarrow \mathbb{P}(\mathscr{C}(J))$$

whose image does not intersect X. Lemma 6.26 implies that the general points of $\mathbb{P}(V^\vee)$ each lie in exactly one secant line. The idea is that the curve will be made up of the "pivot" points of these secant lines and thus be a double cover of $\mathbb{P}(V^\vee)$.

More precisely, because the image of the map $\mathbb{P}(\phi) : \mathbb{P}(V^\vee) \to \mathbb{P}(\mathscr{C}(J))$ is not completely contained in X, the map $\mathbb{P}(\phi)$ lifts uniquely to $\mathcal{L}^{\mathrm{univ}}$ by the valuative criterion, as b is birational. We thus have

(83)

$$
\begin{array}{ccc}
 & & \mathbb{P}(V^\vee) \\
 & \overset{\widetilde{\mathbb{P}(\phi)}}{\nearrow} & \downarrow {\scriptstyle \mathbb{P}(\phi)} \\
\mathcal{Z}^{\mathrm{univ}} \overset{\iota}{\hookrightarrow} \mathcal{L}^{\mathrm{univ}} & \overset{b}{\longrightarrow} & \mathbb{P}(\mathscr{C}(J)) \\
{\scriptstyle \zeta}\searrow \quad \downarrow {\scriptstyle p} & & \\
\mathcal{Hilb}_2(X) & &
\end{array}
$$

If $\widetilde{\mathbb{P}(\phi)}$ factors through a fiber of p, then the image of $\mathbb{P}(\phi)$ would itself be a secant line to X, which contradicts the nondegeneracy assumption. Thus, the composite map $p \circ \widetilde{\mathbb{P}(\phi)}$ is a finite map; because two lines in $\mathbb{P}(\mathscr{C}(J))$ intersect in at most one point, this composite map is actually an isomorphism onto its image in $\mathcal{Hilb}_2(X)$.

Pulling back the bottom left triangle of (83) via $p \circ \widetilde{\mathbb{P}(\phi)} : \mathbb{P}(V^\vee) \to \mathcal{Hilb}_2(X)$, we obtain the diagram

$$
\begin{array}{ccc}
C & \overset{\iota}{\hookrightarrow} & \Sigma \\
 & {\scriptstyle \eta}\searrow & \downarrow {\scriptstyle p} \\
 & & \mathbb{P}(V^\vee)
\end{array}
$$

where Σ is a ruled surface and C is a degree 2 cover of $\mathbb{P}(V^\vee)$.

Recall that $\mathcal{Hilb}_2(X)$ is the blowup of $\mathrm{Sym}^2(X)$ along the diagonal. The 2-to-1 map $C \to \mathbb{P}(V^\vee)$ ramifies exactly where $\mathbb{P}(V^\vee)$ intersects the locus of

fat schemes of $\mathcal{Hilb}_2(X)$, namely the pullback of the diagonal of $\mathrm{Sym}^2(X)$ via the natural birational map $\mathcal{Hilb}_2(X) \dashrightarrow \mathrm{Sym}^2(X)$. This ramification locus is the intersection of $\mathrm{Im}\,(\mathbb{P}(\phi)) \subset \mathbb{P}(\mathscr{C}(J))$ and the tangent variety Y. Since Y is a quartic hypersurface in $\mathbb{P}(\mathscr{C}(J))$, the ramification locus is a zero-dimensional subscheme of degree 4, and by the nondegeneracy assumption, the four points of ramification over $\overline{K}$ are distinct. By Riemann-Hurwitz, the curve C, possibly after normalization, has genus one.

This construction also produces an explicit equation for the curve C, e.g., for $v \in V^\vee$, it is the double cover of $\mathbb{P}(V^\vee)$ given by $y^2 = \mathrm{disc}(\phi(v))$. The bundles on the curve C may also be found immediately from the construction. First, the pullback of $\mathcal{O}_{\mathbb{P}(V^\vee)}(1)$ via the degree 2 map η is the desired degree 2 line bundle L. The map

$$\kappa : C \longrightarrow \mathcal{Z}^{\mathrm{univ}} \xrightarrow{\ \epsilon\ } X \hookrightarrow \mathbb{P}(\mathscr{C}(J))$$

and the moduli interpretation of X as a flag variety in $\mathbb{P}(\mathscr{C}(J))$ together give a flag of bundles $\mathcal{F} = (E_i)$ on the curve C.

Now we establish a relation between the line bundles L and $\kappa^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1)$ on C. It is easiest to describe geometrically. Take a hyperplane H in $\mathbb{P}(\mathscr{C}(J))$ containing the image of $\mathbb{P}(\phi)$ but not its (cubic) image under the adjoint map β_J. Then for any point of C intersecting H, its conjugate (under the map η) also lies on H, since the secant line containing these two conjugate points intersects $\mathrm{Im}\,\mathbb{P}(\phi)$ by the construction of C. Thus, the line bundle $\kappa^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1)$ is a power of L.

To show that this power is 3, recall that the adjoint map β_J preserves secant lines. In particular, for a general point in $\mathbb{P}(\mathscr{C}(J)) \backslash X$, the line spanned by itself and its image under β_J is a secant line of X. Now applying the adjoint map β_J to $\mathrm{Im}\,\mathbb{P}(\phi)$ gives a cubic rational curve in $\mathbb{P}(\mathscr{C}(J))$, i.e., a curve whose intersection with H is degree 3. Therefore, for a general choice of H, there are exactly three secant lines that contain points of $\mathrm{Im}\,\mathbb{P}(\phi)$ and are contained in H; these give rise to exactly three pairs of conjugate points on the curve C contained in H.

As noted earlier, the data of the curve C, the line bundle L, the flag $\mathcal{F}$, and the map κ are all clearly preserved (up to isomorphism) under the action of the group $\mathrm{GL}(V) \times \mathrm{SL}_2(J)$, since each factor acts by linear transformations on its respective projective space.

We have described the map from $\mathrm{GL}(V) \times \mathrm{SL}_2(J)$-orbits of $V \otimes \mathscr{C}(J)$ to isomorphism classes of quadruples $(C, L, \mathcal{F}, \kappa)$. We now describe the reverse map. It will be clear that these two constructions are inverse to one another.

Construction 6.30. The general idea of the reverse map is as follows: starting with the geometric data of $(C, L, \mathcal{F}, \kappa)$, we would like to pick out a linear $\mathbb{P}^1$ in $\mathbb{P}(\mathscr{C}(J))$. For each degree 2 divisor on the curve in the linear series $|L|$, we find the "average" point of the images of its support in X, and all such points together form the desired $\mathbb{P}^1$.

More precisely, given a quadruple $(C, L, \mathcal{F}, \kappa)$ as in the theorem, we have a natural degree 2 map $\eta : C \to \mathbb{P}(H^0(C, L)^\vee) \cong \mathbb{P}^1$. Using the hyperelliptic involution ι on C given by η and the map $\kappa : C \to X$, we obtain the commutative diagram

$$
\begin{array}{ccc}
C & \xrightarrow{(\kappa, \kappa \circ \iota)} & X \times X \\
\eta \downarrow & & \downarrow S_2-\text{quotient} \\
\mathbb{P}(H^0(C, L)^\vee) & \xrightarrow{h'} & \mathrm{Sym}^2(X).
\end{array}
$$

The map h' may be lifted to a map $h : \mathbb{P}(H^0(C, L)^\vee) \to \mathcal{H}ilb_2(X)$, since the image of h' does not lie completely in the diagonal of $\mathrm{Sym}^2(X)$. We thus have the commutative diagram

$$
\begin{array}{ccccc}
C & \longrightarrow & \mathcal{Z}^{\mathrm{univ}} & \longrightarrow & X \times X \\
\eta \downarrow & & \zeta \downarrow & & \downarrow S_2-\text{quotient} \\
\mathbb{P}(H^0(C, L)^\vee) & \xrightarrow{h} & \mathcal{H}ilb_2(X) & \longrightarrow & \mathrm{Sym}^2(X).
\end{array}
$$

By diagram (81), recall that $\mathcal{L}^{\mathrm{univ}}$ is a $\mathbb{P}^1$-bundle over $\mathcal{H}ilb_2(X)$. Define $\Sigma := h^* \mathcal{L}^{\mathrm{univ}}$, so $p : \Sigma \to \mathbb{P}(H^0(C, L)^\vee)$ gives a ruled surface, specifically a $\mathbb{P}^1$-bundle over $\mathbb{P}(H^0(C, L)^\vee)$. In fact, using the relation between L and $\kappa^* \mathcal{O}_X(1)$ and (82), along with the projection formula, we see that

$$
\Sigma = \mathbb{P}(\eta_* \mathcal{O}_C \otimes \mathcal{O}_{\mathbb{P}(H^0(C, L^\vee))}(3)).
$$

We would like to pick out a section $s : \mathbb{P}(H^0(C, L)^\vee) \to \Sigma$ such that the image of the composite $b \circ h \circ s$ is linear in $\mathbb{P}(\mathscr{C}(J))$.

First, we claim there is a unique section $s : \mathbb{P}(H^0(C, L)^\vee) \to \Sigma$ classifying $\eta_* \mathcal{O}_C \otimes \mathcal{O}(3) \to \mathcal{O}(1)$. That is, a cohomology computation shows that there is an exact sequence

$$
0 \to \mathcal{O}(3) \to \eta_* \mathcal{O}_C \otimes \mathcal{O}(3) \to \mathcal{O}(1) \to 0
$$

on $\mathbb{P}(H^0(C,L)^\vee)$, and because $\mathrm{Hom}(\mathcal{O}(3),\mathcal{O}(1))=0$, any such map $\eta_*\mathcal{O}_C \otimes \mathcal{O}(3) \to \mathcal{O}(1)$ is this one, up to scalars.

Therefore, we obtain a map from $\mathbb{P}(H^0(C,L)^\vee)$ to $\mathcal{L}^{\mathrm{univ}}$, and thus to $\mathbb{P}(\mathscr{C}(J))$. The nondegeneracy condition on the geometric data that we require is exactly that the image of this map does not intersect X; it is clear that it is satisfied by the data in Construction 6.29 by assumption.

We now check that this map $\mathbb{P}(H^0(C,L)^\vee) \to \mathbb{P}(\mathscr{C}(J))$ is linear, i.e., the pullback of $\mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1)$ to $\mathbb{P}(H^0(C,L)^\vee)$ from $\mathbb{P}(\mathscr{C}(J))$ (via $b \circ h \circ s$) is isomorphic to $\mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(1)$. Since Σ is a ruled surface, there exists some $a_1, a_2 \in \mathbb{Z}$ such that

$$(84) \qquad (b \circ h)^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1) = \mathcal{O}_p(a_1) \otimes p^* \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(a_2).$$

It is easy to see that $a_1 = 1$ because the fibers of Σ map to lines in $\mathbb{P}(\mathscr{C}(J))$. To compute a_2, we pull back (84) to C via $\iota : C \to \Sigma$:

$$
\begin{aligned}
(85) \qquad \iota^*(b \circ h)^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1) &= \iota^* \mathcal{O}_p(1) \otimes \eta^* \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(a_2) \\
&= \eta^* \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(3) \otimes \eta^* \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(a_2),
\end{aligned}
$$

Since the left-hand side of (85) is just $\eta^* \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(3)$ by the assumed relation, we must have $a_2 = 0$. Thus, we obtain

$$s^*(b \circ h)^* \mathcal{O}_{\mathbb{P}(\mathscr{C}(J))}(1) = s^*(\mathcal{O}_p(1)) = \mathcal{O}_{\mathbb{P}(H^0(C,L)^\vee)}(1),$$

as desired.

6.6. Specializations

Allowing the cubic Jordan algebra J in Theorem 6.28 to vary gives many special cases, as highlighted in Table 1. For certain choices of J, we recover some of the previously considered spaces related to hypercubes and the corresponding parametrization theorems, while for others, we obtain moduli spaces of genus one curves with higher rank vector bundles.

For example, for $J = K \times K \times K$, we recover the case of standard hypercubes from §6.2. In this case, the homogeneous variety $X_{\mathscr{C}(J)}$ is just the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. If we instead let $J = K$, with norm form $\mathrm{N}(x) = x^3$ for an element $x \in K$, then the space $\mathscr{C}(J)$ coincides with the space of triply symmetric hypercubes studied in §6.3.2, and $X_{\mathscr{C}(J)}$ is the twisted cubic in $\mathbb{P}^3$. Also, the space of doubly symmetric hypercubes (see §6.3.1) may be obtained by taking $J = K \times K$, with the norm form

$\mathrm{N}(x_1, x_2) = x_1 x_2^2$ for $(x_1, x_2) \in K \times K$ and $X_{\mathscr{C}(J)}$ the image of $\mathbb{P}^1 \times \mathbb{P}^1$ embedded in $\mathbb{P}^5$ via $\mathcal{O}(1, 2)$.

We describe some of the new moduli problems below. In each case, we also describe more carefully the bijections when the algebra J contains split algebras, e.g., matrix algebras instead of more general central simple algebras. Taking other forms of these algebras then give twisted versions of the geometric data on the genus one curve.

6.6.1. Doubly skew-symmetrized hypercubes.

A new case arises by choosing the cubic Jordan algebra J to be the algebra $K \times \mathrm{Mat}_{2 \times 2}(K)$. We first describe the structure of J and the space of Hermitian cubes $\mathscr{C}(J)$ for this choice of J.

The norm of an element $(x, M) \in K \times \mathrm{Mat}_{2 \times 2}(K)$ is $\mathrm{N}(x, M) = x \det(M)$, and for Springer's construction, we take the basepoint e to be $(1, \mathrm{Id})$. Composition in this algebra is component-wise, with the usual Jordan structure on $\mathrm{Mat}_{2 \times 2}(K)$: for elements $(x_1, M_1), (x_2, M_2) \in K \times \mathrm{Mat}_{2 \times 2}(K)$, we have $(x_1, M_1) \bullet (x_2, M_2) = (x_1 x_2, (M_1 \cdot M_2 + M_2 \cdot M_1)/2)$.

We claim that there is a natural isomorphism between $\mathscr{C}(J)$ and the space $W := K^2 \otimes \wedge^2 K^4$, where the action of $\mathrm{SL}_2(J)$ on $\mathscr{C}(J)$ corresponds to the natural action of $\mathrm{SL}_2(K) \times \mathrm{SL}_4(K)$ on W. We represent elements of W as a pair of 4×4 skew-symmetric matrices. Let $a, b, c, d, b_{ij}, c_{ij} \in K$ for $1 \le i, j \le 2$. Then this isomorphism sends $(a, (b, (b_{ij})), (c, (c_{ij})), d) \in \mathscr{C}(J)$ to the pair

$$\begin{pmatrix} 0 & a & -b_{12} & b_{11} \\ -a & 0 & -b_{22} & b_{21} \\ b_{12} & b_{22} & 0 & c \\ -b_{11} & -b_{21} & -c & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & b & -c_{12} & c_{11} \\ -b & 0 & -c_{22} & c_{21} \\ c_{12} & c_{22} & 0 & d \\ -c_{11} & -c_{21} & -d & 0 \end{pmatrix}$$

in W. It is a slightly tedious but trivial computation to check that the two group actions align.

The homogeneous variety $X_{\mathscr{C}(J)}$ is $\mathbb{P}^1 \times \mathrm{Gr}(2, 4) \hookrightarrow \mathbb{P}^1 \times \mathbb{P}(\wedge^2 K^4) \hookrightarrow \mathbb{P}(W^\vee)$, where the first inclusion is by the Plücker map and the second is the Segre embedding. A map from a scheme T to X thus gives a degree 2 line bundle and a rank 2 vector bundle on T. Theorem 6.28 with this choice of J gives the following moduli description for pairs of Hermitian cubes up to equivalence:

Theorem 6.31. *Let V_1, V_2, and V_3 be K-vector spaces of dimensions 2, 2, and 4, respectively. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$-orbits of $V_1 \otimes V_2 \otimes \wedge^2(V_3)$ are in bijection with isomorphism classes of nondegenerate*

triples (C, L_1, L_2, E), where C is a genus one curve over K, L_1 and L_2 are non isomorphic degree 2 line bundles on C, and E is a rank 2 vector bundle on C with $\det E \cong L_1 \otimes L_2$.

If we record the point $P := L_2 \otimes L_1^{-1}$ instead of the line bundle L_2, we recover Theorem 2.6. Also, we may also replace J with $K \times Q$, for any quaternion algebra Q over K, in which case the homogeneous variety X is a product of $\mathbb{P}^1$ and a twisted form of the Grassmannian $\mathrm{Gr}(2, 4)$.

6.6.2. Triply skew-symmetrized hypercubes. Now let $J = \mathscr{H}_3(K \times K)$, i.e., the space of 3×3 Hermitian matrices over the composition algebra $K \times K$. It is easy to check that J is isomorphic to the space $\mathrm{Mat}_{3\times3}(K)$ of 3×3 matrices over K, with composition given by $(M_1 \cdot M_2 + M_2 \cdot M_1)/2$ for $M_1, M_2 \in \mathrm{Mat}_{3\times3}(K)$.

Then the space $\mathscr{C}(J)$ of Hermitian cubes is isomorphic to $W := \wedge^3 K^6$, with the action of $\mathrm{SL}_2(J)$ matching the natural action of $\mathrm{SL}_6(K)$ on W. We will write down the isomorphism, following [Kru07, Example 19]. Let $a, b_{ij}, c_{ij}, d \in K$ for $1 \le i, j \le 3$. Let $\{e_1, e_2, e_3, f_1, f_2, f_3\}$ be a basis for K^6, and let $e_j^* = e_{j+1} \wedge e_{j+2}$ and $f_j^* = f_{j+1} \wedge f_{j+2}$ in $\wedge^2 K^6$, where the indices are taken cyclically. Then the element $(a, (b_{ij}), (c_{ij}), d)$ is sent to

$$ae_1 \wedge e_2 \wedge e_3 + \sum_{i,j=1}^{3} b_{ij} e_i \wedge f_j^* + \sum_{i,j=1}^{3} c_{ij} f_i \wedge e_j^* + df_1 \wedge f_2 \wedge f_3$$

in $W = \wedge^3 K^6$.

Here, the homogeneous variety $X_{\mathscr{C}(J)}$ is the Grassmannian $\mathrm{Gr}(3, 6)$, which lies in $\mathbb{P}(W^\vee)$ via the Plücker map. Specializing Theorem 6.28 gives the following basis-free version of Theorem 2.7:

Theorem 6.32. *Let V_1 and V_2 be K-vector spaces of dimensions 2 and 6, respectively. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{SL}(V_2)$-orbits of $V_1 \otimes \wedge^3(V_2)$ are in bijection with isomorphism classes of nondegenerate triples (C, L, E), where C is a genus one curve over K, L is a degree 2 line bundle on C, and E is a rank 3 vector bundle on C with $\det E \cong L^{\otimes 3}$.*

6.6.3. Some more exceptional representations. For $J = \mathscr{H}_3(\mathscr{Q})$, where $\mathscr{Q}$ denotes the split quaternion algebra over K (isomorphic to the algebra $\mathrm{Mat}_{2\times2}(K)$), we obtain a more exceptional representation and theorem.

Theorem 6.33. *Let V_1 and V_2 be K-vector spaces of dimensions 2 and 32, respectively, where V_2 is the half-spin representation of Spin_{12}. Let X be the homogeneous space for this action in $\mathbb{P}(V_2^\vee)$. Then nondegenerate $\mathrm{GL}(V_1) \times \mathrm{Spin}_{12}$-orbits of $V_1 \otimes V_2$ are in bijection with the K-points of an open substack of the moduli space of nondegenerate tuples (C, L, κ, ψ), where C is a genus one curve, L is a degree 2 line bundle on C, and κ is a map from C to $X \subset \mathbb{P}(V_2^\vee)$, along with an isomorphism ψ from $L^{\otimes 3}$ to the pullback of $\mathcal{O}_{\mathbb{P}(V_2^\vee)}(1)$ to C via κ.*

In Table 1, we referred to this choice of $X_{\mathscr{C}(J)}$ as the projective line over the cubic algebra J; this is due to our interpretation of $X_{\mathscr{C}(J)}$ as the rank one cubes that are Hermitian over J. In addition, analogous theorems hold when $\mathscr{Q}$ is replaced by a non-split quaternion algebra. Then, the group Spin_{12} is replaced by the appropriate twists.

For $J = \mathscr{H}_3(\mathscr{O})$, where $\mathscr{O}$ denotes the split octonion algebra over K, we have a similar statement.

Theorem 6.34. *Let V_1 and V_2 be K-vector spaces of dimensions 2 and 56, respectively, where V_2 is the miniscule representation of the group E_7. Let X be the homogeneous space for this action in $\mathbb{P}(V_2^\vee)$. Then nondegenerate $\mathrm{GL}(V_1) \times E_7$-orbits of $V_1 \otimes V_2$ are in bijection with the K-points of an open substack of the moduli space of nondegenerate tuples (C, L, κ, ψ), where C is a genus one curve, L is a degree 2 line bundle on C, and κ is a map from C to $X \subset \mathbb{P}(V_2^\vee)$, along with an isomorphism ψ from $L^{\otimes 3}$ to the pullback of $\mathcal{O}_{\mathbb{P}(V_2^\vee)}(1)$ to C via κ.*

Again, taking different octonion algebras over K gives similar theorems, where the split E_7 is replaced by twisted forms of E_7.

7. Connections with exceptional Lie groups and Lie algebras

In this section, we describe two ways in which the coregular representations we have considered in this paper are related to exceptional Lie groups and Lie algebras. These still mysterious connections give hints as to further moduli problems and directions for investigation.

7.1. Vinberg's θ-groups

All of the representations we have considered in this paper are *θ-groups* in the sense of Vinberg [Vin76], when viewed as representations of complex Lie groups. Vinberg's idea was to extend the concept of a Weyl group and a

Cartan subspace to graded Lie algebras. Then the invariants of the representation correspond exactly to the invariants of the Cartan subspace under the action of the Weyl group. Since the Weyl group here is generated by complex reflections, its ring of invariants is free, so the representations obtained in this way are coregular. Moreover, this construction gives a description of the invariants (including their degrees) in terms of the Lie theory.

Let $\mathfrak{g}$ be a $\mathbb{Z}/m\mathbb{Z}$-graded (or $\mathbb{Z}$-graded) Lie algebra for some integer $m \geq 1$ (or respectively, $m = \infty$). Then for m finite, we may write

$$\mathfrak{g} = \mathfrak{g}_0 + \mathfrak{g}_1 + \cdots + \mathfrak{g}_{m-1}$$

with $[\mathfrak{g}_i, \mathfrak{g}_j] \subset \mathfrak{g}_{i+j}$ for $i, j \in \mathbb{Z}/m\mathbb{Z}$. To each such graded Lie algebra, one associates an automorphism θ (or, for m infinite, a one-parameter family of such θ) of $\mathfrak{g}$, e.g., for m finite, we have $\theta(x) = \omega^k x$ for $x \in \mathfrak{g}_k$ and $\omega = e^{2\pi i}$.

Given a graded Lie algebra $\mathfrak{g}$, let G be any connected group having $\mathfrak{g}$ as its Lie algebra, and let G_0 be the connected subgroup of G with $\mathfrak{g}_0$ as its Lie algebra. Then a θ-*group* corresponding to $\mathfrak{g}$ is the representation of G_0 on $\mathfrak{g}_1$. (The name "group" makes sense by thinking of G_0 as a subgroup of $\mathrm{GL}(\mathfrak{g}_1)$.)

Vinberg showed that the G_0-invariants of $\mathfrak{g}_1$ form a polynomial ring, and in fact, the elements of $\mathfrak{g}_1$ with the same G_0-invariants comprise a finite number of orbits over $\mathbb{C}$ [Vin76]. Moreover, Kac showed that most such representations arise in this way [Kac80].

These observations give a heuristic reason for looking at these particular representations if we want to find parametrizations of genus one curves with data such as line bundles and points on the Jacobian. The coarse moduli space of such objects is often a weighted projective space, or a generically finite cover thereof, e.g., in many of the cases in this paper, the orbit spaces over $\mathbb{C}$ parametrize elliptic curves in some family determined by the invariants. In contrast, arithmetic objects such as rings and ideal classes, whose coarse moduli spaces are just a finite number of points, are often parametrized by orbits of prehomogeneous vector spaces.

The θ-groups may be read off directly from subdiagrams of Dynkin diagrams or affine Dynkin diagrams [Vin76, Kac80]. For subdiagrams of Dynkin diagrams, the θ-groups are all prehomogeneous vector spaces. All other irreducible θ-groups are listed in [Kac80, Table III]. These are given by removing a single node from the affine Dynkin diagram. We have indicated the affine Dynkin diagram that gives rise to each representation in Table 1. (Note that in Table 1 we only list the semisimple part of the θ-group.) We have $m = 2$ for lines 1–12 of Table 1, $m = 3$ for lines 13–18, $m = 4$ for line 19, and $m = 5$

						$(A_1,2)$
					$(\mathbb{G}_m,1)$	$(A_2,3)$
				$(\mu_3,1)$	$(A_1,3)$	$(G_2,7)$
			$(\mu_2^2,1)$	$(\mathbb{G}_m^2,2)$	$(A_1^3,4)$	$(D_4,8)$
		$(\mu_2^2,2)$	$(A_1,5)$	$(A_2,8)$	$(C_3,14)$	$(F_4,26)$
	$(\mu_3,1)$	$(\mathbb{G}_m^2,3)$	$(A_2,6)$	$(A_2^2,9)$	$(A_5,15)$	$(E_6,27)$
$(\mathbb{G}_m,2)$	$(A_1,4)$	$(A_1^3,8)$	$(C_3,14)$	$(A_5,20)$	$(D_6,32)$	$(E_7,56)$

Table 2: Deligne and Gross's Magic Triangle of group representations

for line 20. Thus the value of m corresponds to the degree of the associated line bundles in the geometric data!

The connection between these moduli problems and Vinberg theory, especially in the case $m = 2$, is investigated in the beautiful work of Thorne [Tho12]. It is an interesting question as to how Thorne's representation-theoretic constructions of families of curves when $m = 2$, obtained via Vinberg theory and the deformation theory of simple singularities, are related to our more direct geometric constructions of these families.

7.2. The Magic Triangle of Deligne and Gross

In [DG02], Deligne and Gross observed that many of the remarkable properties of the adjoint representations of the groups in the exceptional series

$$(86) \qquad 1 \subset A_1 \subset A_2 \subset G_2 \subset D_4 \subset F_4 \subset E_6 \subset E_7 \subset E_8$$

(as observed in [Del96]) persist for certain other natural sequences of representations. Namely, for each pair $H \subset K$ of distinct subgroups in (86), we may consider the centralizer $Z(H, K)$ of H in K. In this way, we obtain a triangle of subgroups of E_8, as shown in Table 2, where the rows are indexed by $H = E_7, \ldots, A_1$ from top to bottom, and the columns are indexed by $K = A_1, \ldots, E_7$ from left to right, and where we have ignored all semidirect products with, and quotients by, finite groups. Deligne and Gross show that each of the groups in this triangle is naturally equipped with a certain *preferred* representation of that group, obtained from the action of $Z(H, K) \times H$ on $\mathrm{Lie}(K)$ (see [DG02] for details). In Table 2, we have included also the dimensions of these preferred representations. Note that the

groups in the bottom right 4×4 square in Table 2 correspond to the entries of "Freudenthal's Magic Square" of Lie algebras [Fre].

If one takes the last row of representations $(Z(H, K), V)$, where $H = A_1$, and considers instead $(Z(H, K) \times H, V \otimes 2)$, one obtains many of the representations that we used in Sections 2 and 6 to understand degree 2 line bundles on genus one curves. Similarly, if one takes the second-to-last row of representations $(Z(H, K), V)$, where $H = A_2$, and considers instead $(Z(H, K) \times H, V \otimes 3)$, one obtains many of the representations that we used in Sections 3 and 5 to understand degree 3 line bundles on genus one curves.

As with §7.1, we suspect that much more lies behind this connection.

References

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985.

[AKM+01] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, and Alexander R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90** (2001), no. 2, 304–315.

[ARVT05] Michael Artin, Fernando Rodriguez-Villegas, and John Tate, *On the Jacobians of plane cubics*, Adv. Math. **198** (2005), no. 1, 366–382. MR2183258 (2006h:14043)

[BE82] David A. Buchsbaum and David Eisenbud, *Gorenstein ideals of height* 3, Seminar D. Eisenbud/B. Singh/W. Vogel, Vol. 2, Teubner-Texte zur Math., vol. 48, Teubner, Leipzig, 1982, pp. 30–48.

[BH12] Manjul Bhargava and Wei Ho, *On the average sizes of Selmer groups in families of elliptic curves*, preprint, 2012.

[Bha] Manjul Bhargava, *Higher composition laws. V. The parametrization of quaternionic and octonionic rings and modules*, in preparation.

[Bha04a] _____, *Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) **159** (2004), no. 1, 217–250.

[Bha04b] _____, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886.

[Bha04c] _____, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360.

[Bha05] _____, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[Bha08] _____, *Higher composition laws. IV. The parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), no. 1, 53–94.

[Bha10] _____, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), no. 3, 1559–1591.

[BK11] Anita Buckley and Tomaž Košir, *Plane curves as Pfaffians*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **10** (2011), no. 2, 363–388.

[BS13a] Manjul Bhargava and Arul Shankar, *The average number of elements in the 4-Selmer groups of elliptic curves is 7*, 2013, http://arxiv.org/abs/1312.7333.

[BS13b] _____, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, 2013, http://arxiv.org/abs/1312.7859.

[BS15a] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242.

[BS15b] _____, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[CF09] John Cremona and Tom A. Fisher, *On the equivalence of binary quartics*, Journal of Symbolic Computation **44** (2009), 673–682.

[CFO+08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155.

[CFS10]   John E. Cremona, Tom A. Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4** (2010), no. 6, 763–820.

[Cle03]   Jean-Louis Clerc, *Special prehomogeneous vector spaces associated to F_4, E_6, E_7, E_8 and simple Jordan algebras of rank 3*, J. Algebra **264** (2003), no. 1, 98–128.

[Cre99]   J. E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64–94 (electronic).

[CS03]   John H. Conway and Derek A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A K Peters Ltd., Natick, MA, 2003.

[Del96]   Pierre Deligne, *La série exceptionnelle de groupes de Lie*, C. R. Acad. Sci. Paris Sér. I Math. **322** (1996), no. 4, 321–326. MR1378507 (96m:22012)

[Dem73]   Michel Demazure, *Invariants symétriques entiers des groupes de Weyl et torsion*, Invent. Math. **21** (1973), 287–301. MR0342522 (49 #7268)

[DG02]   Pierre Deligne and Benedict H. Gross, *On the exceptional series, and its descendants*, C. R. Math. Acad. Sci. Paris **335** (2002), no. 11, 877–881.

[Dol12]   Igor Dolgachev, *Classical algebraic geometry: A modern view*, Cambridge University Press, 2012.

[Don77]   Ron Y. Donagi, *On the geometry of Grassmannians*, Duke Math. J. **44** (1977), no. 4, 795–837. MR0572991 (58 #28012)

[ESB89]   Lawrence Ein and Nicholas Shepherd-Barron, *Some special Cremona transformations*, Amer. J. Math. **111** (1989), no. 5, 783–800.

[Fau72]   John R. Faulkner, *A geometry for E_7*, Trans. Amer. Math. Soc. **167** (1972), 49–58.

[Fis]   Tom Fisher, *Genus one curves defined by Pfaffians*, preprint.

[Fis06]   ———, *Testing equivalence of ternary cubics*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 333–345.

[Fis08]   ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR2448246 (2009j:11087)

[Fis10]   _____, *Pfaffian presentations of elliptic normal curves*, Trans. Amer. Math. Soc. **362** (2010), no. 5, 2525–2540.

[Fre]   Hans Freudenthal, *Beziehungen der $\mathfrak{E}_7$ und $\mathfrak{E}_8$ zur Oktavenebene,* I-XI, Nederl. Akad. Wetensch. Proc. Ser. A, **57** (1954), 218-230, 363-368, **58** (1955), 151-157, 277-285, **62** (1959), 165-179, 180-191, 192- 201, 447-465, 466-474, **66** (1963), 457-471, 472-487.

[Ful97]   William Fulton, *Young tableaux*, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997, With applications to representation theory and geometry.

[Gau01]   Carl Friedrich Gauss, *Disquisitiones arithmeticae*, 1801.

[Ho09]   Wei Ho, *Orbit parametrizations of curves*, PhD dissertation, Princeton University, August 2009.

[Jac68]   Nathan Jacobson, *Structure and representations of Jordan algebras*, American Mathematical Society Colloquium Publications, Vol. XXXIX, American Mathematical Society, Providence, R.I., 1968.

[Kac80]   V. G. Kac, *Some remarks on nilpotent orbits*, J. Algebra **64** (1980), no. 1, 190–213.

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits.

[Kru07]   Sergei Krutelevich, *Jordan algebras, exceptional groups, and Bhargava composition*, J. Algebra **314** (2007), no. 2, 924–977.

[Lit89]   Peter Littelmann, *Koreguläre und äquidimensionale Darstellungen*, J. Algebra **123** (1989), no. 1, 193–222.

[LVdV84]   R. Lazarsfeld and A. Van de Ven, *Topics in the geometry of projective space*, DMV Seminar, vol. 4, Birkhäuser Verlag, Basel, 1984, Recent work of F. L. Zak, With an addendum by Zak.

[McC04]   Kevin McCrimmon, *A taste of Jordan algebras*, Universitext, Springer-Verlag, New York, 2004.

[MSS96]   J. R. Merriman, S. Siksek, and N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. **77** (1996), no. 4, 385–404.

[Mum66]   D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354. MR0204427 (34 #4269)

[Mum70]   David Mumford, *Varieties defined by quadratic equations*, Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970, pp. 29–100.

[Ng95]   Kok Onn Ng, *The classification of* $(3, 3, 3)$ *trilinear forms*, J. Reine Angew. Math. **468** (1995), 49–75.

[O'N02]   Catherine O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), no. 2, 329–339.

[SBG$^+$95] Helmut Salzmann, Dieter Betten, Theo Grundhöfer, Hermann Hähl, Rainer Löwen, and Markus Stroppel, *Compact projective planes*, de Gruyter Expositions in Mathematics, vol. 21, Walter de Gruyter & Co., Berlin, 1995, With an introduction to octonion geometry.

[Stu09]   Bernd Sturmfels, *Open problems in algebraic statistics*, Emerging applications of algebraic geometry, IMA Vol. Math. Appl., vol. 149, Springer, New York, 2009, pp. 351–363.

[Tho12]   Jack Thorne, *The arithmetic of simple singularities*, Ph.D. thesis, Harvard University, 2012.

[Ver09]   Peter Vermeire, *Singularities of the secant variety*, J. Pure Appl. Algebra **213** (2009), no. 6, 1129–1132. MR2498802 (2010b:14108)

[Vin76]   È. B. Vinberg, *The Weyl group of a graded Lie algebra*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 3, 488–526, 709.

[WY92]   David J. Wright and Akihiko Yukie, *Prehomogeneous vector spaces and field extensions*, Invent. Math. **110** (1992), no. 2, 283–314.

[Zak85]   F. L. Zak, *Severi varieties*, Mat. Sb. (N.S.) **126(168)** (1985), no. 1, 115–132, 144.

[Zak93]   ———, *Tangents and secants of algebraic varieties*, Translations of Mathematical Monographs, vol. 127, American Mathematical Society, Providence, RI, 1993, Translated from the Russian manuscript by the author.

Manjul Bhargava
Department of Mathematics
Princeton University
Princeton, NJ 08544
USA
E-mail address: bhargava@math.princeton.edu

Wei Ho
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA
E-mail address: weiho@umich.edu